METHODS FOR THE SOLUTION OF CIPHERS

PUBLICATIONS, 15-22 INCL.

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
Riverbank--Geneva, Ill.

William F. Friedman
Washington
1948

Gift of
Riverbank Laboratories

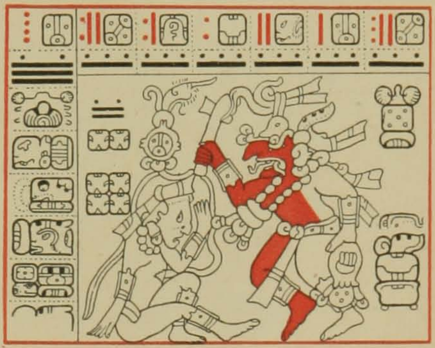
Note -
All these papers were written by me
except No. 19 (Transposition Ciphers) which
was written in collaboration with
Capt. Lenox R. Lohr; and No. 21, which
was written in collaboration with
Elizebeth Smith Friedman, my wife.
W. F. F.

Umol-huun tah-tiyal

William Frederick

yetel

Elizebeth Smith Friedman



Lay ca-huunil kubenbil tech same.
This our book we entrusted you a while-ago.
Ti manaan apaclam-tz'a lo toon
It not-being you-return-give it us,
Epahal ca-baat tumen ah-men.
Is-being-sharpened our-axe by the expert.

A Method of Reconstructing the Primary Alphabet

From a Single One of the Series of Secondary Alphabets

Publication No. 15

RIVERBANK LABORATORIES
DEPARMTENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1917

A Method of Reconstructing the Primary Alphabet from a Single One of the Series of Secondary Alphabets

In a modified Vigenere table, that is, one in which a key-word followed by the rest of the unused letters of the alphabet is employed instead of the straight direct alphabet, it is possible to derive a series of twenty-five mixed alphabets. We will designate the "master-key" alphabet, that is, the one containing the key-word and on which the table is based, as the *PRIMARY ALPHABET*, and the alphabets resulting from the table as the *SECONDARY ALPHABETS.*

The following is an example of such a table and its method of use, employing the key-word "Stenography."

S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z
T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S
E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T
N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E
O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N
G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O
R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G
A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R
P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A
H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P
Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H
B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y
C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B
D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C
F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D
I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F
J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I
K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J
L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K
M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L
Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M
U	V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q
V	W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U
W	X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V
X	Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W
Z	S	T	E	N	O	G	R	A	P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X

To encipher the words "General Pershing has" etc., using the key-word CARGO, in accordance with the well-known original Vigenere method, viz.: finding at the top the key letter, at the left side the text letter, and taking the letter at the intersection of the vertical and horizontal columns as the cipher-letter, we have:*

Key letter.....	C A R G O	C A R G O	C A R G O	C A R
Plain text......	G E N E R	A L P E R	S H I N G	H A S
Cipher.........	K H H A Y	M Z F A Y	C J U P H	U F R

Now for each different key letter in the encipherment of a message a different one of the series of the twenty-five alphabets is employed; e. g., in the case of the above key-word CARGO, in the C alphabet, T is enciphered by D, E is enciphered by F, G by K, etc.; the next key letter being A, T is enciphered by P, E by H, N by Y, etc.

Considering the primary alphabet as partaking of the nature of a disk or wheel, each line of the table, consisting of exactly the same sequence of letters, is a repetition of the preceding line, removed one place to the left. It is therefore possible to produce every one of the secondary alphabets by the use of two strips of paper upon which the same primary alphabet appears, sliding one beneath the other, one place at a time, thus producing consecutively the twenty-five secondary alphabets. For example, using the same primary alphabet as above, placed on two strips of cross-section paper and sliding S of the lower strip one space to the left, we have:**

```
  S T E N O G R A P H Y B C D F I J K L M Q U V W X Z
S T E N O G R A P H Y B C D F I J K L M Q U V W X Z
```

Considering the lower strip to represent the plain text, the entire Z secondary alphabet of the table can be produced from the above relative positions of the sliding alphabets, and is as follows, for enciphering:

(1)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	R	Y	B	C	T	D	O	P	F	I	J	K	L	E	N	A	M	G	Z	S	Q	U	V	W	H	X

For deciphering, however, this alphabet would be written thus:

(2)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	P	C	D	F	N	I	R	Y	J	K	L	M	Q	O	G	H	U	A	T	E	V	W	X	Z	B	S

Given this secondary alphabet it is possible to recover the primary by the following method:

Write the numerical sequence from 1 to 26, using, preferably, cross-section paper so as to have the spaces between the letters the same. Starting with the letter A, which equals P, place P under the space No. 1; under space No. 2, place the equivalent of P, which is H; under space No. 3 place the equivalent of H, which is Y; under space No. 4, place the equivalent of Y, which is B, etc. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
P	H	Y	B																						

*It is possible, of course, to use a square table in several other ways, but whatever the method, any cipher message enciphered by the use of a key-word and square table, may be deciphered by a multi-alphabet system, and therefore the present principles of finding the primary alphabet are applicable to all.

**In actual practice one of the alphabets on the sliding strips should be double in length in order to secure coincidence of plain text and cipher-equivalent letters no matter where set.

This procedure results in the reconstruction of the primary alphabet, thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
P	H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A

In working out this example we placed the equivalent of each letter right next to the letter itself as each was determined in order. This was because the cipher letters and the plain text letters were but one space removed from each other in the sliding strips when the Z secondary alphabet is used. In other words, the alphabets were one place removed from each other. If they had been removed two places from each other, then we should have every time to leave *ONE* space between a letter and its equivalent; when three places removed, then *two* spaces should have to be left; when four places removed, *three* spaces, etc., in short, when *n* places removed, then *n — 1* spaces should be left. Thus, given the enciphering alphabet as follows:

(3) A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
G N Y B S C N A D F I J K T E R L O X Z M Q U V P W

and the resulting deciphering alphabet:

(4) A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
H D F I O J A B K L M Q U G R Y V P E N W X Z S C T

to find the primary alphabet, place the equivalent of A, which is H, in space No. 1; then place the equivalent of H, which is B, one space removed from H, that is, in space No. 3; place the equivalent of B, which is D, in space No. 5, etc. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
H		B		D		I		K		M		U		W		Z		T		N		G		A	

When we have reached the point G equals A, we find that our determined sequence begins to repeat itself, since A equals H. To continue the procedure, we assume that a sequence such as FG, JK, PQ, VWXYZ is not interrupted by the key-word in the primary alphabet. We then experiment on this basis by placing, for example in the case above, the letter J in the space No. 8 and continue as before, placing the equivalent of J, which is L, in space No. 10, etc. Thus the primary alphabet is again reproduced completely.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
H	Y	B	C	D	F	I	J	K	L	M	Q	U	V	W	X	Z	S	T	E	N	O	G	R	A	P

It follows then that to recover the primary alphabet from any one of the secondary alphabets, it will be necessary to leave as many spaces between each cipher letter of the secondary alphabet and its equivalent plain text letter, as the number of places the primary alphabets have been removed from each other. In other words, if *n* represents the number of places the primary alphabets were shifted, then in recovering the primary from any secondary alphabet, the primary alphabet will appear when the equivalent of each letter of that particular secondary alphabet has been put in the *n+1* place from the letter itself. Reduced to the form of an equation:

If n = the number of places the primary alphabet has been shifted;
Then n − 1 = the number of spaces which should be left between each letter of a secondary alphabet and its equivalent;
Or n + 1 = the number of the place into which is put the equivalent of any letter, counting from that letter.

Now in actual practice two things are true with respect to the above: (1) no secondary alphabet will carry in itself any indication whatever as to its position in the table, that is, the number of spaces the primary alphabets have been shifted (with one exception to be discussed later); (2) hardly ever will any secondary alphabet be complete except in deciphering a very long message. In practice, therefore, the recovery of a primary alphabet will not be so simple as in the above cases, but will necessitate considerable experiment, for which the following two principles may serve as guiding points:

(1) A sequence of determined letters must be either a pronounceable combination, thus being a part of the key-word; or,

(2) A sequence of determined letters must follow the normal straight alphabetical sequence interrupted by those letters which have been incorporated in the key-word. That is, a sequence such as GHKLN is entirely possible and indicates that I, J and M are present in the key-word, while the sequence such as HGKNL is impossible and indicates that we have not left the proper number of spaces between letters and their equivalents.

In order to illustrate the above points we will work out an example. Given the deciphering alphabet:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
N T U V P W X J F Y Z D K Q C A B O G R L I S H M E

The tabulated results are as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1st trial..............	N	Q	B																							
2nd trial..............	N		Q		B		T																			
3rd trial..............	N	D		Q	V		B			T			R			O			C			U			L	
4th trial..............	N		U		Q				B				T				R				O				C	
5th trial..............	N					Q					B					T					R					
6th trial..............	N				O		Q				C		B				U		T				L		R	
7th trial..............	N		R					Q		O					B		C					T				
8th trial..............	N						R		Q						O		B						C		T	
9th trial..............	N	T	C	D						Q	R	U	V						B	O	L	I				

At the ninth trial we are beginning to see a possible portion of a key-word, together with two other normal sequences save for interruptions. A continuation of this leads to the completion of the primary alphabet which is as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	T	C	D	F	G	J	K	P	Q	R	U	V	W	X	Y	Z	A	B	O	L	I	S	H	M	E

and the key-word is ABOLISHMENT.

It is possible to reconstruct completely by the exercise of some ingenuity a primary alphabet from a partial secondary in which as many as ten or twelve letters are missing. Given the following partial deciphering alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	R		P	A	M	O		U	S	B	F	H	G		T	I		E		D			L	N	

the following letters are missing: C J K Q W X Y Z. The first thing to do is to find the longest sequence of equivalents, which in this case begins with Q. Going through all the steps as before, we get no good results until we have left about 19 or 20 spaces between letters and equivalents, when the sequence in the primary alphabet begins to assume a nearly normal appearance. At 20 spaces interval the sequence of some of the letters is such as to make us certain that we are on the right track at last.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1st trial.............	Q	I	U	D	P	T																				
10th trial.............	Q				D						I				P						U				T	
18th trial.............	Q		D								U		T						I		P					
20th trial.............	Q	T					P					D					U					I				

This is as far as we can get with our first unbroken sequence. Our next longest sequence of equivalents begins with J. Now if in the primary alphabet the sequence JK is unbroken, then J would follow I in the last of the above trials and the letters determined from this start should agree with those already placed.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Q	T	V				P	A				D	E				U	S				I	J			

The next longest sequence of equivalents begins with W, and we will assume that the VW sequence is unbroken in the primary alphabet, which means that we should place W after V in the tentative primary alphabet.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Q	T	V	W			P	A		H		D	E		M		U	S		F		I	J		L	

The next sequence of equivalents begins with X, which we will place after W.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Q	T	V	W	X		P	A		H		D	E		M	O	U	S		F	G	I	J		L	N

The remaining letters are easily placed and the whole sequence is now completed.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Q	T	V	W	X	Z	P	A	C	H	Y	D	E	R	M	O	U	S	B	F	G	I	J	K	L	N

The key-word is PACHYDERMOUS.

Sometimes a continuance of the sequence may be found by going backward instead of forward. Many possibilities will suggest themselves to the ingenious decipherer.

One and only one of the series of twenty-five secondary alphabets carries with it a number which indicates its position in the table, viz., the 13th, which is what may be called a RECIPROCAL alphabet, in which for example plain text letter A equals R and plain text letter R equals A. In working out the primary alphabet from this particular secondary alphabet, it is necessary to assume parts of unbroken sequences such as BC, FG, JK, PQ, VWXYZ, and remove their equivalents 13 spaces right from the start, since in a table such as is being discussed the 13th secondary alphabet is *always* a reciprocal alphabet. The following is an example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N		G		T					O	M	R		A		X	D	L	U	E	S	H	I	P		

The first step would be to fill in as many of the missing values as possible. If J is O, then O is J; if V is H, then H is V, etc. The alphabet, as nearly complete from the values given as possible, is as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N		G	Q	T		C	V	W	O	M	R	K	A	J	X	D	L	U	E	S	H	I	P		

We first assume that the UVWXYZ sequence is unbroken and what is probably a portion of the key-word, SHIP, are 13 spaces apart. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
							S	H	I	P		F	G	J						U	V	W	X	Y	Z

If our key-word ends in SHIP and if B is not a part of it, then B would be likely to follow P, and 13 spaces in advance would bring Y as its equivalent, which is very good. The only unfilled letters are Z and F. Placing F next to B brings Z in proper position. After F may come G, which would give C as the first letter of the key-word; after G must come J, which gives O as the second letter of the key-word, since H and I are already a part of the key-word. Thus, step by step the whole primary alphabet is reconstructed.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
C	O	M	R	A	D	E	S	H	I	P	B	F	G	J	K	L	N	Q	T	U	V	W	X	Y	Z

It has been shown repeatedly that the method of enciphering by means of the Vigenere table, the so-called "Chiffre indeschiffrable," is easily attacked by the ordinary principles and rules of deciphering. The above method of recovering or reconstructing the primary alphabet is an addition to deciphering methods which will not only save months of labor, but will also furnish a means whereby enemy messages may be deciphered exactly as rapidly as by the intended recipient himself.

Solve the following examples:

(1)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
	Q	M	T	A	Z	S	C	U	X	L	I	W	P	Y	N	E	B	D	R	F	V	G	H	J	K	O	English

(2)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	English
		P	R	U	Y	C	K	X	W	H	S	E	A	T	D	F		I		B	Q	L	V	M	N	O	

(3)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	German
	J	Z		M	O	A	N		E	R	L	Q	U	K	S	T	B	P		Y	V	C	I		G	H	

(4)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	French
	G	A		C	F		L		N	P		S	T	V	U		Y			B	H	O	R	I	D	E	

(5)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Spanish
	U		T	M	P	E		I	R		A	N	L			O	S	B	Y	D		G		Q			

Methods for The Solution of Running-Key Ciphers

Publication No. 16

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Four Hundred copies of this publication were printed of which this is

No. 271

RIVERBANK
LABORATORIES

GENEVA
ILLINOIS

TABLE OF CONTENTS

METHODS FOR THE SOLUTION OF RUNNING-KEY CIPHERS

RUNNING-KEY CIPHER is the name applied to that system of enciphering which necessitates the use of a book or document, identical copies of which are in possession of the correspondents. The letters of the book text are used as successive key letters in conjunction with any system which will produce a series of twenty-six different alphabets, one for each different letter of the ordinary alphabet of which the running-key text is composed. The possibility of the decipherment of a message or of messages enciphered by such a system has long been considered questionable. As a matter of fact, such a cipher may nearly always be solved; and the solution of a series of messages enciphered by the same running-key is very simple. In order to demonstrate how easy the solution of a series of messages in the same running-key actually is, the following example is given and the underlying principles will follow later.

(1) Solution of a series of messages enciphered by the same running-key and a Vigénère Table (two sliding direct alphabets).

MESSAGES

1.	VBEKT	CLPXZ	VNHQB	VEYIN	IWZSI
2.	SAXTC	DKLTR	YEFWW	NMAEE	KZMZQ
3.	ZNKNI	UNUFV	PNTPW	IXKXQ	WSVRX
4.	HJHAL	CNZEE	KMRQI	QOHRE	IFKCS
5.	OEMPP	ZXYCW	PRRGI	ZTNIF	BSWSX
6.	ORKVT	ZTUIS	VMOGM	FMYSA	EVXKT
7.	GUKHT	BXSEE	KBVJA	UXSPU	NWIRJ
8.	RREHC	OMAET	ROASW	FBAMQ	NLMZQ
9.	BRXKP	OKNIJ	BPCOG	BYNEU	MSWYX
10.	FRLLV	JXHQD	BNVWQ	BGTYU	TTIGJ

Take the first three vertical columns of cipher letters and "set" them in horizontal lines on sliding direct alphabets, thus:

TABLE 1.

Column 1 Cipher letters VSZHOOGRBF	Column 2 Cipher letters BANJERURRR	Column 3 Cipher letters EXKHMKKEXL
WTAIPPHSCG	CBOKFSVSSS	FYLINLLFYM
XUBJQQITDH	DCPLGTWTTT	GZMJOMMGZN
YVCKRRJUEI	EDQMHUXUUU	HANKPNNHAO
ZWDLSSKVFJ	FERNIVYVVV	IBOLQOOIBP
AXEMTTLWGK	GFSOJWZWWW	JCPMRPPJCQ
BYFNUUMXHL	HGTPKXAXXX	KDQNSQQKDR
CZGOVVNYIM	IHUQLYBYYY	LEROTRRLES
DAHPWWOZJN	JIVRMZCZZZ	Key letter T
EBIQXXPAKO	KJWSNADAAA	
FCJRYYQBLP	LKXTOBEBBB	
GDKSZZRCMQ	MLYUPCFCCC	
HELTAASDNR	NMZVQDGDDD	
Key letter O	ONAWREHEEE	
	Key letter N	

Now combine the horizontal row of letters representing the plain-text equivalents of the first column of cipher letters with those representing the second and third columns and the results are as follows:

	1	2	3
Key:	O	N	T
1.	H	O	L
2.	E	N	E
3.	L	A	R
4.	T	W	O
5.	A	R	T
6.	A	E	R
7.	S	H	R
8.	D	E	L
9.	N	E	E
10.	R	E	S

Repeat the preceding process for the succeeding columns:

TABLE 2.

Column 4 Cipher letters	Column 5 Cipher letters	Column 6 Cipher letters
KTNAPVHHKL	TCILPTTCPV	CDUCZZBOOJ
LUOBQWIILM	UDJMQUUDQW	DEVDAACPPK
MVPCRXJJMN	VEKNRVVERX	EFWEBBDQQL
NWQDSYKKNO	WFLOSWWFSY	FGXFCCERRM
OXRETZLLOP	XGMPTXXGTZ	GHYGDDFSSN
PYSFUAMMPQ	YHNQUYYHUA	HIZHEEGTTO
QZTGVBNNQR	ZIORVZZIVB	IJAIFFHUUP
RAUHWCOORS	AJPSWAAJWC	JKBJGGIVVQ
SBVIXDPPST	BKQTXBBKXD	KLCKHHJWWR
TCWJYEQQTU	CLRUYCCLYE	LMDLIIKXXS
UDXKZFRRUV	DMSVZDDMZF	MNEMJJLYYT
VEYLAGSSVW	ENTWAEENAG	NOFNKKMZZU
WFZMBHTTWX	FOUXBFFOBH	OPGOLLNAAV
ZGANCIUUXY	GPVYCGGPCI	Key letter O
YHBODJVVYZ	HQWZDHHQDJ	
ZICPEKWWZA	IRXAEIIREK	
AJDQFLXXAB	JSYBFJJSFL	
BKERGMYYBC	KTZCGKKTGM	
CLFSHNZZCD	LUADHLLUHN	
DMGTIOAADE	MVBEIMMVIO	
Key letter H	NWCFJNNWJP	
	OXDGKOOXKQ	
	PYEHLPPYLR	
	Key letter E	

Add the equivalents to what has already been determined:

	123456
Key:	ONTHEO
1.	HOLDPO
2.	ENEMYP
3.	LARGEG
4.	TWOTHO
5.	ARTILL
6.	AEROPL
7.	SHRAPN
8.	DELAYA
9.	NEEDLA
10.	RESERV

There is no doubt that the messages can now be solved completely. Only such time is needed as it takes to produce, by the foregoing almost automatic method, the equivalents for each vertical column of cipher letters. The messages and key read:

Key:	ONTHE	OTHER	HANDI	NTHEC	ASEOF
1.	HOLDP	OSITI	ONUNT	ILREL	IEVED
2.	ENEMY	PREPA	RESTO	ATTAC	KHILL
3.	LARGE	GUNBE	INGMO	VEDTO	WARDS
4.	TWOTH	OUSAN	DMENA	DVANC	INGON
5.	ARTIL	LERYF	IREDA	MAGED	BASES
6.	AEROP	LANEB	OMBDE	STROY	EDTWO
7.	SHRAP	NELAN	DBIGS	HELLS	NEEDE
8.	DELAY	ATTAC	KONPO	SITIO	NTILL
9.	NEEDL	ARGES	UPPLY	OFGAS	MASKS
10.	RESER	VEAMM	UNITI	ONMUS	TBESE

Now how was this simple solution of an "undecipherable" system achieved, and what are the principles involved?

To illustrate, return to the series of messages just deciphered, which were enciphered by a Vigénère Table, shown in the accompanying Figure 1. Each column of cipher letters is the result of the encipherment of all the plain-text letters in that column by the same key letter. Therefore, all the cipher letters in one column are an equal distance removed from their respective plain-text letters. That is, the series of plain-text letters HELTAASDNR (Column 1 of the example) with the key letter O and the Vigénère Table give the cipher equivalents VSZHOOGRBF, cipher letters being taken at the intersection of the column determined by the key letter with the horizontal line determined by the plain-text letter. (See page 12). The same result will be obtained, but by a longer process, explained below, which is known as "running down."

The statement made above—namely, that all the cipher letters in one column are an equal distance removed from their respective plain-text letters—means then, that if, when the key letter is O, the cipher equivalent of plain-text letter H in this example is V, that is, fourteen letters removed from H in a direct alphabet, then the cipher equivalent of plain-text letter E is likewise fourteen letters removed from E, giving the cipher letter S; text L giving Z, etc. In fact, all the cipher equivalents of this column of letters may be found by writing the series of plain-text letters in a horizontal line and then continuing beneath each letter the direct alphabet. Thus:

	HELTAASDNR
1.	IFMUBBTEOS
2.	JGNVCCUFPT
3.	KHOWDDVGQU
4.	LIPXEEWHRV
5.	MJQYFFXISW
6.	NKRZGGYJTX
7.	OLSAHHZKUY
8.	PMTBIIALVZ
9.	QNUCJJBMWA
10.	ROVDKKCNXB
11.	SPWELLDOYC
12.	TQXFMMEPZD
13.	URYGNNFQAE
14.	VSZHOOGRBF

Fig. 1.

VIGÉNÈRE TABLE.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

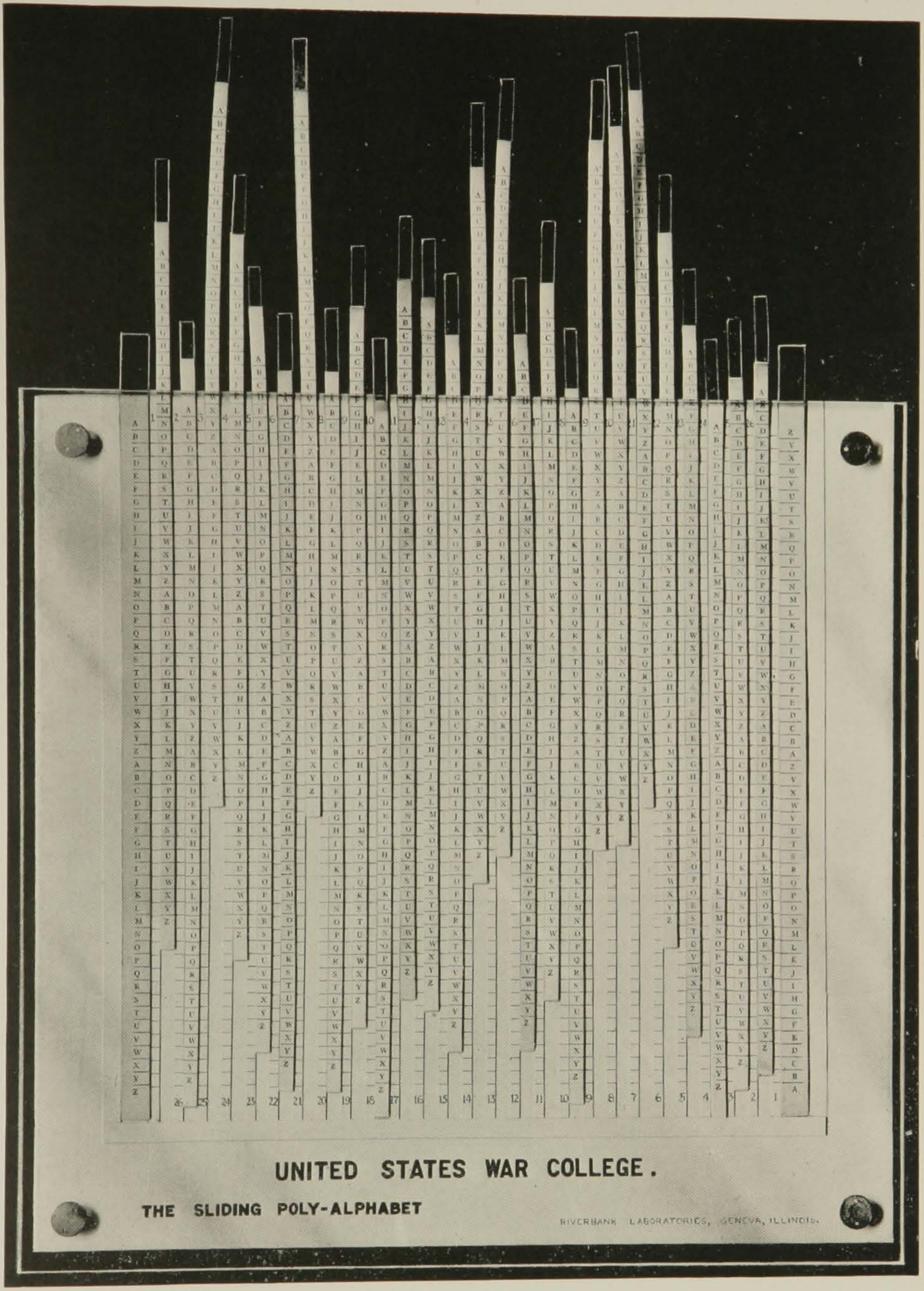
On the other hand, given the cipher letters, the plain-text equivalents may be found either by reversing the process or by continuing the same process; for, if the direct alphabet ending with Z is continued by repeating the alphabet, or if it is printed in circular form on a revolving disk, it may be regarded as a continuous, circulating series of letters, and it therefore follows that if H leads to V, then V will lead to H. This process of continuing the sequence of a series of letters constituting an alphabet, which is known as "running down," may be greatly facilitated by the use of the devices shown in Plate 1. The Sliding Poly-Alphabet, A, consists of a series of twenty-six direct alphabets printed upon cardboard strips which are mounted upon celluloid; the strips are all movable, running either in grooves or on tracks, the two pieces of plate glass provided with set-screws at the corners holding the strips firmly, yet loosely enough so that they easily slide up and down. There is in addition a direct alphabet at the extreme left, and a reversed at the extreme right. The sliding strips bear upon their reverse sides other alphabets, i. e., reversed, French or Spanish, etc. Now when a line of cipher text is "set" at the top, that is, when the sliding strips are moved so that a given number (up to twenty-six) of cipher-text letters are brought into one horizontal line, the successive horizontal lines of equivalents, called *generatrices*, are indicated automatically, and thus a vast amount of writing is eliminated. In an alphabet containing twenty-six letters, there are twenty-five generatrices, the twenty-sixth generatrix becoming identical with the letters at the starting point. The second device, the Poly-alphabet Wheel, B, the idea for which the Riverbank Laboratories is indebted to Lieutenant P. H. Burdick, produces the same results. It makes use of a revolving rubber stamp containing the letters of the direct alphabet equally spaced on the perimeter of the wheel. In order to "run down" a series of cipher letters it is only necessary to start each column with the cipher letter which is to be "run down." The letters all being equidistant from each other, the successive letters all appear upon horizontal lines, or in other words, the successive generatrices are printed. This method possesses some advantageous features which the other does not, the most important being, first, that the apparatus is much smaller and can be carried about easily; secondly, that once a group of cipher letters is "run down" the results are permanently indicated and may be referred to or re-examined at any future time; and thirdly, since the letters are all movable, they may be arranged in accordance with any mixed alphabet sequence.

The third device, the Poly-alphabet Roller, C, makes use of a series of ten endless rubber belts containing the letters of the direct alphabet equally spaced. These belts fit snugly upon the drum, but may be moved with reference to each other so as to contain ten cipher letters in one line. The device is then inked and rolled upon a sheet of paper.

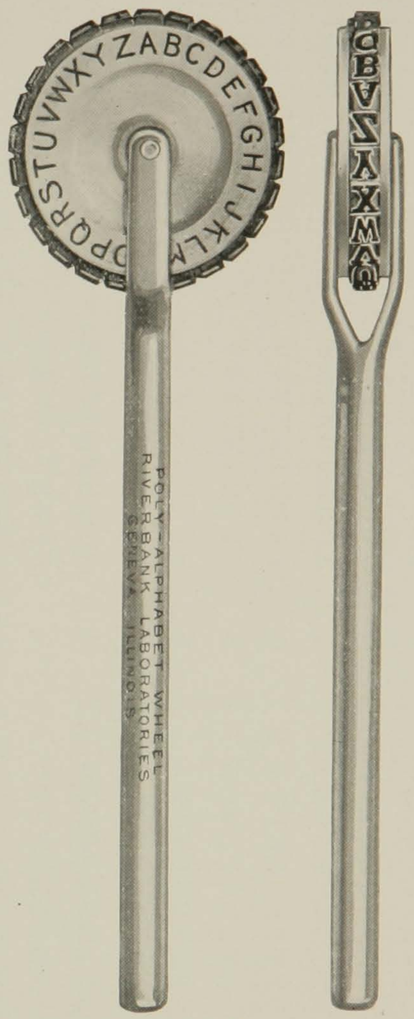
From the above it follows that since all the letters of the first column have been enciphered by the same key letter, and are hence an equal distance removed from their respective plain-text letters, that the process of "running down" should produce one generatrix which will contain all of the plain-text equivalents for the cipher letters of this column. Hence, if the correct generatrix can be found for each column of the above series of messages, then the plain-text equivalents for each column and the decipherment of all the messages are at hand. The problem thus resolves itself into the selection of the correct generatrix from among all the generatrices of each column. Since English text consists largely of the letters ETOANIRSHD, the generatrix sought in the case of each column will be the one which contains the greatest number or best assortment of these high-frequency letters.

The "running down" process in the case of the first three columns in the series of messages above gave the following generatrices:

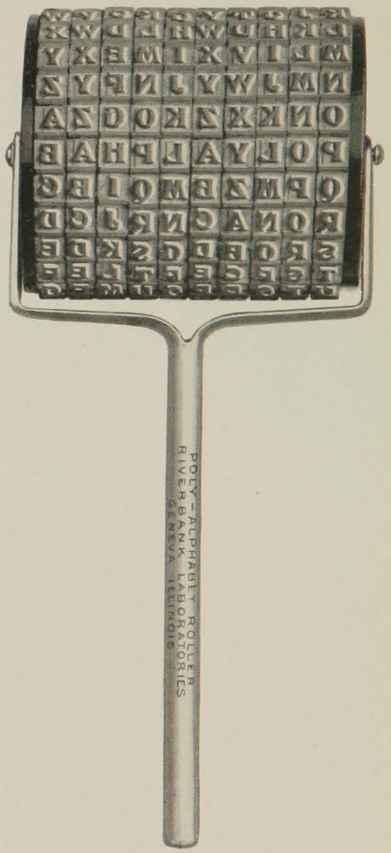
PLATE 1


UNITED STATES WAR COLLEGE.
THE SLIDING POLY-ALPHABET
RIVERBANK LABORATORIES, GENEVA, ILLINOIS.

A


ABCDEFGHIJKLMNOPQRSTUVWXYZ
POLY-ALPHABET WHEEL
RIVERBANK LABORATORIES
GENEVA ILLINOIS

B


POLY-ALPHABET ROLLER
RIVERBANK LABORATORIES
GENEVA ILLINOIS

C

TABLE 3.

GENERATRICES OF

Genera-trix	Column 1 Cipher letters VSZHOOGRBF	Genera-trix	Column 2 Cipher letters BANJERURRR	Genera-trix	Column 3 Cipher letters EXKHMKKEXL
1	WTAIPPHSCG	1	CBOKFSVSSS	1	FYLINLLFYM
2	XUBJQQITDH	2	DCPLGTWTTT	2	GZMJOMMGZN
3	YVCKRRJUEI	3	EDQMHUXUUU	3	HANKPNNHAO
4	ZWDLSSKVFJ	4	FERNIVYVVV	4	IBOLQOOIBP
5	AXEMTTLWGK	5	GFSOJWZWWW	5	JCPMRPPJCQ
6	BYFNUUMXHL	6	HGTPKXAXXX	6	KDQNSQQKDR
7	CZGOVVNYIM	7	IHUQLYBYYY	7	LEROTRRLES
8	DAHPWWOZJN	8	JIVRMZCZZZ	8	MFSPUSSMFT
9	EBIQXXPAKO	9	KJWSNADAAA	9	NGTQVTTNGU
10	FCJRYYQBLP	10	LKXTOBEBBB	10	OHURWUUOHV
11	GDKSZZRCMQ	11	MLYUPCFCCC	11	PIVSXVVPIW
12	HELTAASDNR	12	NMZVQDGDDD	12	QJWTYWWQJX
13	IFMUBBTEOS	13	ONAWREHEEE	13	RKXUZXXRKY
14	JGNVCCUFPT	14	POBXSFIFFF	14	SLYVAYYSLZ
15	KHOWDDVGQU	15	QPCYTGJGGG	15	TMZWBZZTMA
16	LIPXEEWHRV	16	RQDZUHKHHH	16	UNAXCAAUNB
17	MJQYFFXISW	17	SREAVILIII	17	VOBYDBBVOC
18	NKRZGGYJTX	18	TSFBWJMJJJ	18	WPCZECCWPD
19	OLSAHHZKUY	19	UTGCXKNKKK	19	XQDAFDDXQE
20	PMTBIIALVZ	20	VUHDYLOLLL	20	YREBGEEYRF
21	QNUCJJBMWA	21	WVIEZMPMMM	21	ZSFCHFFZSG
22	ROVDKKCNXB	22	XWJFANQNNN	22	ATGDIGGATH
23	SPWELLDOYC	23	YXKGBOROOO	23	BUHEJHHBUI
24	TQXFMMEPZD	24	ZYLHCPSPPP	24	CVIFKIICVJ
25	URYGNNFQAE	25	AZMIDQTQQQ	25	DWJGLJJDWK

It was necessary then to select from among these twenty-five generatrices for each column the correct generatrix. The generatrices which contain the greatest number of high-frequency letters, and therefore the most likely, are given in Table 4.

TABLE 4.

MOST PROBABLE GENERATRICES OF

Generatrix	Column 1 Cipher letters VSZHOOGRBF	Generatrix	Column 2 Cipher letters BANJERURRR	Generatrix	Column 3 Cipher letters EXKHMKKEXL
1	WTAIPPHSCG	9	KJWSNADAAA	3	HANKPNNHAO
12	HELTAASDNR	13	ONAWREHEEE	7	LEROTRRLES
13	IFMUBBTEOS	17	SREAVILIII	16	UNAXCAAUNB
20	PMTBIIALVZ	23	YXKGBOROOO	20	YREBGEEYRF

The letters in the generatrix which is to be chosen from among the possibilities of the first column generatrices, must be joined to the letters in the generatrix to be chosen from among the possibilities of the second column generatrices; those of the second generatrix must be joined to those of the third, etc. Experiment is necessary to find the generatrices which will give the highest number of good combinations, remembering that these combinations must be the beginnings of words.* Not much delay will be experienced in finding that the 12th generatrix of the first column, the 13th of the second, together with the 7th of the third give the combinations already quoted on page 3, and repeated below:

	1	2	3
1.	H	O	L
2.	E	N	E
3.	L	A	R
4.	T	W	O
5.	A	R	T
6.	A	E	R
7.	S	H	R
8.	D	E	L
9.	N	E	E
10.	R	E	S

*With respect to the correct generatrix of the first column, it should be borne in mind that, since the order of frequency of initial letters differs considerably from that of the interior of words, it will often happen that a generatrix containing a high percentage of E, A or O is not the correct one. The order of frequency of initial letters given by Hitt is T, O, A, W (B, C) (S, D). See: Hitt, Parker A., Manual for the Solution of Military Ciphers, 1916, p. 9.

As a further check the key letters in the case of these three columns are sought. There are three ways of finding the key letters. The first is by reference to a Vigénère Table; the second is by the use of two sliding direct alphabets; the third is by the use of the Sliding Poly-Alphabet referred to on Page 7, or some similar device, by a method described below; and in all three cases a little experiment is necessary to determine which method of enciphering was used. There are eight different ways of using a Vigénère Table, but only three of them are encountered frequently enough to warrant mention, though the principles discussed in this booklet apply to all.

(1) The original Vigénère method, taking the cipher letter at the intersection of the vertical column determined by the key letter and the horizontal line determined by the plain-text letter in the first column on the left. Ex. Key M, plain-text S; cipher E.

(2) Proceeding down the key-letter column to the plain-text letter and following the horizontal line thus determined to the extreme left (the method first used by Beaufort). Ex. Key M, plain-text S; cipher G.

(3) Finding the plain-text letter in the first horizontal line, proceeding down the column thus determined to the row containing the key letter, thence out to the extreme left (another method devised by Beaufort). Ex. Plain-text S, key M, cipher U. This method gives exactly the same results as the sliding of a direct alphabet against a reversed, the principle used in the U. S. Army Disk, and will be discussed under section (2) on page 16.

Now all the alphabets resulting from the application of method (1) or (2) to the Vigénère Table may be produced more quickly by the use of two sliding direct alphabets. In the case of these two examples, the sliding alphabets would be in the position indicated below:

Beaufort, or Method (2) Key M; plain-text S; cipher G

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWYZ
            ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Vigénère, or Method (1) Key M; plain-text S; cipher E

A good way of remembering these methods without having to refer to the table is this: Consider the letter A which is set opposite the key letter; when this letter A and the plain-text letter are both on the same strip, it is Method (1), the Vigénère; when this letter A and the plain-text letter are on opposite strips, it is Method (2), the Beaufort.

Applying these principles to the problem in hand in order to find the key letters, consider the first three letters of any of the messages and their corresponding cipher letters; for example, the first message: $\begin{matrix}\text{H O L}\\ \text{V B E}\end{matrix}$. Reference to the diagram directly above will show that if plain-text letter H equals cipher letter V, the key letter is O in case Method (1) was used in enciphering; or the key letter is M, if Method (2) was used. Setting the alphabets again, so that plain-text letter O equals B, the key letter is N in case either Method (1) or (2) was used. Setting the alphabets once more, so that plain-text letter L equals E, the key letter is T in case Method (1) was used, or H in case Method (2) was used. Putting together the results of these three experiments, Method (2) gives MNH as the start of the key, which is obviously impossible, while Method (1) gives ONT, which is not only possible but suggests what the beginning of the key really is. It is concluded, therefore, that Method (1) was used in the encipherment of these messages.

When method (1) of enciphering has been used the Sliding Poly-Alphabet will give the key letter if a *reversed* alphabet is set so that A on the latter is set against the cipher letter, the correct key letter being found opposite the horizontal line containing the plain-text equivalents; if method (2) of enciphering was used, the device will give the key letter if a *direct* alphabet is set so that A on the latter is set against the cipher letter, the correct key letter being found opposite the horizontal line containing the plain-text equivalents. Showing the first column of letters for the above ten messages enciphered by both methods, this may be graphically represented thus:

TABLE 5.

METHOD (1)		METHOD (2)	
Key letter	Cipher letters	Key letter	Cipher letters
A	V S Z H O O G R B F	A	T Q X F M M E P Z D
Z	W T A I P P H S C G	B	U R Y G N N F Q A E
Y	X U B J Q Q I T D H	C	V S Z H O O G R B F
X	Y V C K R R J U E I	D	W T A I P P H S C G
W	Z W D L S S K V F J	E	X U B J Q Q I T D H
V	A X E M T T L W G K	F	Y V C K R R J U E I
U	B Y F N U U M X H L	G	Z W D L S S K V F J
T	C Z G O V V N Y I M	H	A X E M T T L W G K
S	D A H P W W O Z J N	I	B Y F N U U M X H L
R	E B I Q X X P A K O	J	C Z G O V V N Y I M
Q	F C J R Y Y Q B L P	K	D A H P W W O Z J N
P	G D K S Z Z R C M Q	L	E B I Q X X P A K O
O	H E L T A A S D N R	M	F C J R Y Y Q B L P
		N	G D K S Z Z R C M Q
		O	H E L T A A S D N R

The same procedure as was followed in the finding of the correct generatrix for columns 1, 2 and 3, is followed with respect to columns 4, 5 and 6, and the new key letters determined are HEO, making the running-key read ON THE O. As a matter of fact, in the actual solution, the correct generatrices for columns 4 and 5 were found by guessing that the running-key was ON THE, having as a start the three key letters ON T, as determined above. That is, assuming the key letter to be H, the cipher letters of the fourth column were at once converted to their plain-text equivalents, without a search for a generatrix having the greatest number of high-frequency letters; the cipher letters of the fifth column were likewise converted by the key letter E, to their correct equivalents.

In this manner, once the method of enciphering has been determined, the decipherment and the determination of key proceed together, one leading to progress in the other, until the complete solution has been secured.

The solution of a Running-Key Cipher by the above process is not limited to the cases where there are many messages, but is possible wherever there are two or more messages, provided only that they are enciphered by the same key. For example, let us take the following three messages, also enciphered by the Vigénère Table:

```
1.   EJVVQ   YMWTM   POWAV   UKZQG   AVERL
2.   VWUXD   UUOCW   MRWQA   BBNSG   KFIPD
3.   TFABD   YKAEM   ILRKB   WFHKT   BYOVL
```

The generatrices of the first six columns are as shown in Table 6 on page 15:

Those generatrices which are the most probable have been underlined in the table. One naturally begins by trying to join the letters of the most promising generatrix of column 1, with those of any promising generatrix of columns 2 and 3, and if good combinations result, the key letters are sought. Here are a few of these experiments:

Col. 1	Col. 2	Col. 1	Col. 2	Col. 1	Col. 2	Col. 1	Col. 2	Col. 1	Col. 2
Gen. 9	Gen. 8	Gen. 9	Gen. 9	Gen. 9	Gen. 12	Gen. 9	Gen. 21	Gen. 9	Gen. 25
N	R	N	S	N	V	N	E	N	I
E	E	E	F	E	I	E	R	E	V
C	N	C	O	C	R	C	A	C	E

Of these first attempts, only the last two give anything possible. The key letters for these combinations are sought. If the messages were enciphered by method (1) the key letters are RF, for the first, and RB, for the second of these good combinations; if by method (2), JV and JZ, respectively. All of these are impossible, therefore these combinations are rejected and the next most promising generatrix in column 1 is selected for a fresh start, and a similar procedure followed. Impossible key letters will always cause incorrect assumptions to be rejected.

TABLE 6.

Key if enciphered by Method		GENERATRICES OF						
(1)	(2)	Genera-trix	Col. 1	Col. 2	Col. 3	Col. 4	Col. 5	Col. 6
A	A		EVT	JWF	VUA	VXB	QDD	YUY
Z	B	1	FWU	KXG	WVB	WYC	REE	ZVZ
Y	C	2	GXV	LYH	XWC	XZD	SFF	AWA
X	D	3	HYW	MZI	YXD	YAE	TGG	BXB
W	E	4	IZX	NAJ	ZYE	ZBF	UHH	CYC
V	F	5	JAY	OBK	AZF	ACG	VII	DZD
U	G	6	KBZ	PCL	BAG	BDH	WJJ	EAE
T	H	7	LCA	QDM	CBH	CEI	XKK	
S	I	8	MDB	REN	DCI	DFJ	YLL	
R	J	9	NEC	SFO	EDJ	EGK	ZMM	
Q	K	10	OFD	TGP	FEK	FHL	ANN	
P	L	11	PGE	UHQ	GFL	GIM	BOO	
O	M	12	QHF	VIR	HGM	HJN	CPP	
N	N	13	RIG	WJS	IHN	IKO	DQQ	
M	O	14	SJH	XKT	JIO	JLP	ERR	
L	P	15	TKI	YLU	KJP	KMQ		
K	Q	16	ULJ	ZMV	LKQ	LNR		
J	R	17	VMK	ANW	MLR	MOS		
I	S	18	WNL	BOX	NMS	NPT		
H	T	19	XOM	CPY	ONT	OQU		
G	U	20	YPN	DQZ	POU	PRV		
F	V	21	ZQO	ERA	QPV	QSW		
E	W	22	ARP	FSB	RQW	RTX		
D	X	23	BSQ	GTC	SRX	SUY		
C	Y	24	CTR	HUD	TSY	TVZ		
B	Z	25	DUS	IVE	UTZ	UWA		

This entire process in actual practice takes much less time than the description of it, for it is chiefly one of inspection. Hence, one after another, the possible combinations in these messages are tried and rejected, bearing in mind the frequency of initial letters as compared with that of letters of general text (see footnote, p. 11). Finally, generatrix 11 of column 1, giving the letters PGE is tried. At a glance it is seen that these letters will make possible syllables when joined to generatrix 8 of column 2. Thus: PR, GE, EN; key letters PS, or LI. The latter only is possible, hence the conclusion that if the correct generatrices have really been found, the messages were enciphered by Method (2). Now a search is made in column 3 for a generatrix, letters of which will combine with the PR, GE and EN combinations. Only one generatrix, 19, will do so, giving as a result, PRO, GEN, ENT, with key letters LIT. Again, in column 4, generatrix 3 gives PROY, BENA, ENTE, with key letters LITD. Rejecting this, generatrix 7 is tried. Here the combinations are more probable—PROC, GENE, ENTI, with key LITH. At once the words LITHIA, LITHIUM and LITHOGRAPHY suggest themselves as possible first words of the key. On trial of the generatrix opposite the letter I of Method (2) in column 5, the resulting letters are YLL, which are altogether improbable when joined to the preceding—PROC-Y, GENE-L, ENTI-L; hence LITHIUM or LITHIA are found impossible. Returning then to the combinations of text letters, the word GENERAL is suggested as the first word in the second message. The generatrix of column 5 which will give an R in the second place is 14, key letter O. Now the text reads PROCE, GENER, ENTIR, key LITHO. LITHOGRAPHY for the key is thus corroborated. This checks with the assumption of GENERAL and gives for the first and third messages PROCEED and ENTIREB. From now on the solution is only a matter of a few minutes, the messages and key checking the assumptions made from one or the other.

Hence, it is seen how this system of deciphering a Running-Key Cipher is applicable even to as few as two or three messages, the only difficulty being that of the time needed to try out the larger number of probable generatrices, which necessarily increase in occurrence as the number of messages decreases. Even that difficulty, however, applies only to the first two or three columns.

(2) Solution of a series of messages enciphered by the same running-key and a direct alphabet sliding against a reversed (U. S. Army Disk).

The sliding of a direct alphabet against a reversed will produce a series of twenty-six reciprocal alphabets. By a reciprocal alphabet is meant one in which, if for example Y equals E, then E equals Y; or if X equals D, then D equals X. With the key letter D, the word GENERAL would be enciphered by XZQZMDS. Graphically represented, the two sliding alphabets would be in this position:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
    ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Unlike the case of two direct alphabets, the "running down" process will neither produce the cipher equivalents given above for the word GENERAL, nor will it result in the production of the plain-text equivalents from these cipher letters. But if the cipher letters are first converted into their reversed alphabet equivalents on a direct alphabet set against a reversed at any point, then the "running down" process will result in the production of the plain-text equivalents. The above example, where A of the direct alphabet is set against Z of the reversed in securing the reversed alphabet equivalents, may serve as an illustration:

Plain–text letters:	GENERAL
Cipher letters:	XZQZMDS
Reversed alphabet equivalents:	CAJANWH
Generatrix 1 :	DBKBOXI
2 :	ECLCPYJ
3 :	FDMDQZK
4 :	GENERAL

Therefore, before applying the principles presented above for the solution of a Running-Key Cipher enciphered by a Vigénère Table (or two sliding direct alphabets), to a message enciphered by a direct alphabet sliding against a reversed alphabet (U. S. Army Disk), it will be necessary to convert each column of cipher letters into their reversed alphabet equivalents before "running down" to select the proper generatrices. From there on the process is the same. As stated above, the reversed alphabet equivalents may be found by setting a direct alphabet against a reversed at any point; but in order to find, by means of the Poly-Alphabet, the key letter applying to a column, A should be set to Z, in which case when Z of a direct alphabet is set opposite the reversed alphabet equivalents, the correct key letter will be found opposite the correct generatrix. This is illustrated in the solution of the series of messages which follows.

The solution of the six messages given below, enciphered by the U. S. Army Disk and by the same running-key, follows:

1.	DXYCK	BQHLX	BUCYM	MAUMA	GECXN	JSPAS
2.	RQYNL	BCTZF	KJCAA	SDUUR	BUTGZ	WPWVS
3.	AKZBV	JFOXX	UEGEX	REDNW	YOBGI	MSVWC
4.	ZXOLA	YFWBE	GLVYE	PKSBW	ABZUO	LEZVA
5.	BKERJ	RCFAZ	KJNZE	VTUUN	UKMWN	RHAEU
6.	AGPLK	BGZRJ	HSTNO	FYLHT	XQHHR	BSUPZ

TABLE 7.

GENERATRICES OF

Key letters	Genatrix	Column 1	Column 2	Column 3
		Cipher letters	Cipher letters	Cipher letters
		DRAZBA	XQKXKG	YYZOEP
		Equivalents	Equivalents	Equivalents
Z		WIZAYZ	CJPCPT	BBALVK
A	1	XJABZA	DKQDQU	CCBMWL
B	2	YKBCAB	ELRERV	DDCNXM
C	3	ZLCDBC	FMSFSW	EEDOYN
D	4	AMDECD	GNTGTX	FFEPZO
E	5	BNEFDE	HOUHUY	GGFQAP
F	6	COFGEF	IPVIVZ	HHGRBQ
G	7	DPGHFG	JQWJWA	IIHSCR
H	8	EQHIGH	KRXKXB	JJITDS
I	9	FRIJHI	LSYLYC	KKJUET
J	10	GSJKIJ	MTZMZD	LLKVFU
K	11	HTKLJK	NUANAE	MMLWGV
L	12	IULMKL	OVBOBF	NNMXHW
M	13	JVMNLM	PWCPCG	OONYIX
N	14	KWNOMN	QXDQDH	PPOZJY
O	15	LXOPNO	RYEREI	QQPAKZ
P	16	MYPQOP	SZFSFJ	RRQBLA
Q	17	NZQRPQ	TAGTGK	SSRCMB
R	18	OARSQR	UBHUHL	TTSDNC
S	19	PBSTRS	VCIVIM	UUTEOD
T	20	QCTUST	WDJWJN	VVUFPE
U	21	RDUVTU	XEKXKO	WWVGQF
V	22	SEVWUV	YFLYLP	XXWHRG
W	23	TFWXVW	ZGMZMQ	YYXISH
X	24	UGXYWX	AHNANR	ZZYJTI
Y	25	VHYZXY	BIOBOS	AAZKUJ

The union of generatrices 19, 15 and 13 of columns 1, 2 and 3, respectively, is found to give the best combinations with the key-letters SOM:

Column		1	2	3
Key		S	O	M
Message	1:	P	R	O
	2:	B	Y	O
	3:	S	E	N
	4:	T	R	Y
	5:	R	E	I
	6:	S	I	X

Note that the correct generatrix for Column 1, consisting of the letters PBSTRS, conforms closely with the requirements of frequency of initial letters. (See footnote to page 11). In fact, the correct generatrix was chosen on the first attempt.

The messages and key when solved are as follows:

Key	SOMEO	FTHEL	OWGRA	DEFUE	LSHAV	EAHIG
1.	PROCE	EDATO	NCETO	RELIE	FOFDI	VISIO
2.	BYORD	EROFG	ENERA	LBLAN	KYOUW	ILLNO
3.	SENDT	WOTHO	USAND	MACHI	NEGUN	SIMME
4.	TRYTO	HOLDH	ILLTW	OUNTI	LRIGH	TWING
5.	REINF	ORCEM	ENTSW	ILLAR	RIVEI	NTHEM
6.	SIXTE	ENINC	HENEM	YGUNL	OCATE	DINTH

(3) Solution of a series of messages enciphered by the same running-key and a mixed alphabet sliding against (A) a direct alphabet, or (B) a reversed alphabet.

(A) When a mixed alphabet and a direct alphabet are used it is necessary to convert the cipher letters into their direct alphabet or mixed alphabet equivalents before "running down" or "setting" on the Sliding Poly-Alphabet. For example, given the mixed alphabet CRYPTOGAMSBDEFHIJKLNQUVWXZ the word HOW enciphered by the key letter L would be written PBL, as shown graphically*:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
    CRYPTOGAMSBDEFHIJKLNQUVWXZ
           ↑
```

If the direct alphabet equivalents of PBL are found by setting the mixed alphabet thus:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
CRYPTOGAMSBDEFHIJKLNQUVWXZ
   ‾      ‾        ‾
```

*The most frequently encountered mixed alphabets are those employing a key word followed by the rest of the unused letters of the alphabet. The key word should be long, should contain as many of the vowels as possible, and should break up the normal sequence of letters in the alphabet as much as possible. Such an alphabet is called a "Key-word Alphabet."

where it is found that P of the mixed alphabet equals D of the direct, B equals K, and L equals S, the "setting" of these equivalents or "running down" will now produce the plain-text letters.

Plain-text letters:		HOW
Cipher-Letters:		PBL
Direct alphabet equivalents:		DKS
Generatrix:	1.	ELT
	2.	FMU
	3.	GNV
	4.	HOW

The same word HOW may be enciphered in another way, using the same alphabets and the same key letter L, for the plain-text letters may be sought on the mixed alphabet, and their cipher equivalents on the direct. In this case the cipher letters would be SJB. Instead of converting these cipher letters into their direct alphabet equivalents, as above, it is now necessary to convert them into their mixed alphabet equivalents. They are found to be LSR. Now the "running down" of these letters according to a direct alphabet sequence will not produce the plain-text equivalents, but if they are "run down" *according to the given mixed-alphabet sequence*, the plain-text letters will reappear. Thus:

Plain-text letters:		HOW
Cipher letters:		SJB
Mixed-alphabet equivalents:		LSR
Mixed alphabet generatrix:	1.	NBY
	2.	QDP
	3.	UET
	4.	VFO
	5.	WHG
	6.	XIA
	7.	ZJM
	8.	CKS
	9.	RLB
	10.	YND
	11.	PQE
	12.	TUF
	13.	OVH
	14.	GWI
	15.	AXJ
	16.	MZK
	17.	SCL
	18.	BRN
	19.	DYQ
	20.	EPU
	21.	FTV
	22.	HOW

Returning now to the decipherment of a series of messages enciphered on this system, the columns of cipher letters must be converted first into either their direct alphabet equivalents or their mixed alphabet equivalents depending upon the method of encipherment, as discussed above.

(B) What was said under (A) of this section applies also to the case where a mixed alphabet is sliding against a reversed alphabet. Only one conversion is necessary, viz., the conversion of cipher letters to their reversed alphabet equivalents, or to their mixed alphabet equivalents, depending upon the method of encipherment, and the subsequent procedure is the same as in (A).

4. Solution of a series of messages enciphered by the same running-key and two identical mixed alphabets sliding against each other (Modified Vigénère Table).*

The only difference in the case of this system as compared with that using an ordinary Vigénère Table is that instead of "running down" the letters of each column according to the direct alphabetical sequence, it is necessary to "run down" according to the sequence of the mixed alphabet. No conversion into equivalents before "running down" is necessary in this case. The Poly-alphabet Wheel could be used to good advantage here, since it can be arranged to print any mixed alphabet sequence. In the absence of such a device, this work must be done by hand, unless there is sufficient need to have such mixed alphabets printed.

5. Solution of a single message enciphered by a running-key and (A) a direct alphabet sliding against a reversed (U. S. Army Disk), or (B) two direct sliding alphabets (Vigénère Table).

Here again the methods are based upon the very frequent occurrence of the letters ETOANIRSHD in English text. Since E is the most frequently used letter in English, the combination E over E, that is, key-letter E to encipher plain-text letter E, will be the most frequent. The combination T over E, or E over T, will occur next in frequency. Below, the combinations will be represented in this form: $\begin{array}{c}X\\ \underline{\underline{Y}}\\ Z\end{array}$, where X is the key letter; Y, the plain-text letter; and Z, the resultant cipher letter.

(A) A direct alphabet sliding against a reversed (the U. S. Army Disk).

I. All the high frequency combinations and their resultant cipher letters may be compressed into a small table which will serve in finding a breaking point in the key-text or the plain-text, the one being as important as the other in the process of decipherment.

*In an ordinary Vigénère Table the direct alphabet forms the basis of the table, and, as stated before, all of the alphabets of a Vigénère Table may be produced by two sliding strips containing the direct alphabet. In a Modified Vigénère Table, a mixed alphabet forms the basis of the table, and this mixed alphabet, designated as the *Primary Alphabet* usually consists of a keyword (see footnote to Page 19) followed by the rest of the unused letters of the alphabet. The table, aside from this feature, is constructed and used exactly the same as an ordinary Vigénère Table. All of the secondary alphabets may be produced by two sliding strips containing the primary alphabet. The first letter of the lower strip becomes the equivalent of A on the direct alphabet in setting for the required key letter. See page 29.

TABLE 8.

	Key letter											
Text letter	E	T	O	A	N	I	R	S	H	D	L	C
E	A	P	K	W	J	E	N	O	D	Z	H	Y
T	L	A	V	H	U	P	Y	Z	O	K	S	J
O	Q	F	A	M	Z	U	D	E	T	P	X	O
A	E	T	O	A	N	I	R	S	H	D	L	C
N	R	G	B	N	A	V	E	F	U	Q	Y	P
I	W	L	G	S	F	A	J	K	Z	V	D	U
R	N	C	X	J	W	R	A	B	Q	M	U	L
S	M	B	W	I	V	Q	Z	A	P	L	T	K
H	X	M	H	T	G	B	K	L	A	W	E	V
D	B	Q	L	X	K	F	O	P	E	A	I	Z
L	T	I	D	P	C	X	G	H	W	S	A	R
C	C	R	M	Y	L	G	P	Q	F	B	J	A

By this table is shown, for example, that the cipher letter E may represent any of the following combinations $\frac{E}{A}, \frac{I}{E}, \frac{R}{N}, \frac{S}{O}, \frac{H}{D}, \frac{L}{H}.$ It is also clear that when the key letter and plain-text letter coincide, the cipher letter will be A; or stated conversely, the cipher letter A always indicates a coincidence of key and plain-text letters. Furthermore, it is evident that the cipher letter may represent letters other than those indicated in the table. For example:

$$\begin{array}{c}T\\ \hline P\\ \hline\hline E\end{array}\quad \begin{array}{c}Q\\ \hline M\\ \hline\hline E\end{array}\quad \begin{array}{c}V\\ \hline R\\ \hline\hline E\end{array}\ \text{etc.}$$

The same would be the case for any other cipher letter. But since English words are composed of the letters ETOANIRSHDLC to the extent of approximately 85%, the remaining letters of the alphabet being used relatively infrequently as compared with them, the decipherer will be able to recognize the skeletons of words, despite the occasional incorrect letters, which represent the encipherment of infrequent combinations, the identities of which will manifest themselves as the decipherment proceeds.

An illustration of this method of solving a single message is as follows:

MESSAGE.

LOWNH ZKNIC JB (etc.)

The first step is to assume that the key-text and plain-text consist solely of the letters ETOANIRSHDLC, and accordingly the equivalents of the cipher letters as given in the table on page 22, are set down in the manner shown below, maintaining the relative positions of key and plain-text letters for easy reference:

Cipher text		LOWNH	ZKNIC	JB
Possible Key Letters	1a	ESAR		
	2a	TOE		
	3a	DH		
	4a	SR		
	5a	O		
Possible Plain text Letters	1b	TEEE		
	2b	IAI		
	3b	ST		
	4b	HD		
	5b	D		

The first words of the key and the plain-text stand out very plainly: THE and ITI. The latter leads to the trial of IT IS for the plain-text, which gives for the key-text THE F. Now F can be followed by a vowel or by the consonants L or R only. A trial of THE FL gives IT IS E, which is possible. FL can be followed by a vowel only, and they are tried one after the other. The results are as follows:

Key-text	Plain-text	Possible words of plain-text
THE FLA	IT IS EB	EBB, EBENEZER, EBONY, EBU...
THE FLE	IT IS EF	EFF. . . . . . several words.
THE FLI	IT IS EJ	EJACULAT. . . . . .
THE FLO	IT IS EP	EPIPHYTE, EPHRAIM.
THE FLU	IT IS EV	EV. . . . . . several words.
THE FLY	IT IS EZ	EZRA

All of these possibilities are tested one by one. For example, the first possibility: Key, THE FLA, giving plain-text IT IS EB is systematically exhausted in an attempt to continue either the key or the plain-text:

Cipher text	LOWNH	ZKNI	
If the plain-text is	ITISE	BB	
then the key-text is	THEFL	AL,	which is impossible.
If the plain-text is	ITISE	BE	
then the key-text is	THEFL	AO,	which is impossible.
If the plain text is	ITISE	BONY	
then the key-text is	THEFI	AYAG,	which is impossible.

Thus, the possible key-text THE FLA has been exhausted, and the decipherer proceeds to THE FLE, THE FLI, etc. If none of these give good results, it becomes evident that THE FL is not correct, and THE FR is tried next. This may not produce results either, whereupon the vowel combinations with F must be tried. There is no need to go through the whole process, which takes longer to describe than to perform. It will be found that the key-text THE FU gives IT IS N as the plain-text. The words which this new letter suggests immediately are NECESSARY, NOW, NOT, NEITHER, etc. A quick trial of these possibilities is made and it is found that the plain-text IT IS NOT gives for the key-text THE FUND, and the way is now clear for further progress, for the latter suggests THE FUNDAMENTAL, a long sequence, giving for the plain-text IT IS NOT NECESSA, clearly the word NECESSARY.

By this method of checking key against plain-text, and vice versa, the complete decipherment may be accomplished. Often technical matter is used as the running-key text, and in such a case a familiarity with the terminology or nomenclature is a great aid. The hardest part of the task is accomplished, once the start has been made, since the first few letters will often determine the context of both key and plain-text, and both furnish clues to progress in the solution. It may be necessary to proceed into the interior of a message before a breaking point is found. This method of seeking for a continuance of either key or plain-text applies in the solution of any single running-key message by whatever system is used.

II. Another form of table, not based upon the actual tabulation of frequency of combinations normally occurring in English text is shown on page 25 (Table No. 9). Here all of the high frequency letters ETOANIRSHD are distinguished from the others by being in bold faced type. For example, the cipher letter L (at the top of the table) represents the encipherment of plain-text letters T by key letter E; or it may represent the combination $\frac{I}{T}$, or $\frac{D}{O}$, etc.

The same kind of table can be made for the Vigénère square, employing the original Vigénère system or the Beaufort system of enciphering.

III. A short-cut to the preceding method may be found by assuming that common words such as THE, AND, etc., occur in the key, as they very probably would in a message of some length. Test the text for the presence of one of the words, beginning at the very first letter and proceeding letter by letter until a good place is found; that is, one giving a good combination in the equivalent plain-text. This short-cut applied to the message above would at once confirm the suspected presence of such a word as THE, and would show that the plain-text began with IT I. Thus:

If the key is THE
and the cipher-text is LOW
then the plain-text is ITI

giving at once the start of the message.

The plain-text may be assumed to contain a THE or an AND in the same way. Or if the presence of a word is fairly certain or suspected, a thorough test for it will show whether it is present or not.

TABLE 9.

Cipher-letter

Key-letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Key-letter
E	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	**H**	G	F	E
T	**T**	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	T
O	**O**	**N**	M	L	K	J	**I**	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	O
A	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	**H**	G	F	**E**	**D**	C	B	A
N	**N**	M	L	K	J	**I**	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	**O**	N
I	**I**	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	I
R	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	R
S	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	S
H	**H**	G	F	**E**	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	H
D	**D**	C	B	**A**	Z	Y	X	W	V	U	**T**	**S**	**R**	Q	P	**O**	**N**	M	L	K	J	**I**	**H**	G	F	**E**	D
L	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
U	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
C	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
M	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
P	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
F	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
Y	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
W	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
G	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
B	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
V	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
K	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
J	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
Z	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
Q	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Cipher-letter

IV. An improvement over the preceding three methods makes use of sliding strips. It is possible to find the order of frequency of the combinations which result in the production of the same cipher letter by merely multiplying the frequencies of the letters concerned in each combination and then tabulating the combinations in accordance with these products. These products remain constant of course, regardless of the kind of alphabets used (the text remaining the same in nature) but the resultant cipher letters change with the alphabets used, and hence the tabulations would change accordingly.

A. A direct alphabet sliding against a reversed (the U. S. Army Disk).

The following table contains all the combinations which result in the production of the cipher letter P, for example, when a direct alphabet is sliding against a reversed.

Combinations resulting in cipher letter P, arranged alphabetically.

Key-letter:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plain-text:	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

In order to find the relative frequency of the combination $\frac{A}{L}$ as compared with $\frac{B}{M}$ it is only necessary to multiply the frequency of single letter A by that of L and compare the product with that resulting from the multiplication of the frequency of B by the frequency of M*. Thus, the frequency of any combination giving P may be found, and these combinations are then arranged according to their products. Thus, for this same cipher-letter, the results are as follows:

Combinations resulting in cipher letter P, arranged in order of frequency:

Key-letter:	T	I	H	D	A	E	S	C	R	P	N	G	W	U	L	B	X	J	V	O	K	Y	M	F	Q	Z
Plain-text:	E	T	S	O	L	P	D	N	C	A	Y	R	H	F	W	M	I	U	G	Z	V	J	X	Q	B	K

The same data is secured for every letter of the alphabet, and is arranged as shown in Table 10, page 27. All the combinations which result in the production of the same cipher letter are in the same column. In each combination, the upper letter is the key-letter. The columns in this table are then cut apart, and mounted upon sliding sticks. These slides are then used in the following manner:

Given a cipher message:

TOFFA NBPEW KYMOO (etc.)

the slides labeled T, O, F and A are selected for experiment. Slides T and O are set directly opposite each other so that the first combination on the T strip coincides with the first one on the O strip. Since the high frequency combinations are at the top of the slides all those near the top are examined to see if there is present any good combination which might possibly be the start of the message. No combinations are found of sufficient probability to justify further experiment. The O strip is then moved up one space and the resulting series of combinations is examined again. The best combination is $\frac{I\ F}{P\ R}$ which suggests the word PROCEED for the plain-text. A quick trial of this possibility shows that it is correct,

*The data given by Hitt for English Literary Text were used in these calculations.

TABLE 10.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	O	T	H	E	T	T	A	I	N	O	E	E	E	S	T	E	E	A	T	N	O	A	E	R	N
E	**N**	**R**	**E**	**A**	**O**	**N**	**T**	**A**	**E**	**E**	**T**	**S**	**R**	**E**	**E**	**O**	**N**	**I**	**A**	**T**	**T**	**E**	**H**	**T**	**O**
T	E	E	R	I	N	O	H	A	A	E	T	A	R	O	I	H	R	S	A	I	I	E	O	C	D
T	**D**	**C**	**O**	**E**	**I**	**I**	**A**	**S**	**R**	**U**	**I**	**O**	**E**	**A**	**T**	**R**	**A**	**A**	**H**	**O**	**N**	**I**	**R**	**E**	**E**
A	T	N	D	S	S	N	O	M	R	R	S	T	A	H	H	I	I	E	H	H	N	O	A	L	S
A	**S**	**L**	**A**	**O**	**N**	**H**	**H**	**E**	**I**	**H**	**H**	**H**	**N**	**T**	**S**	**S**	**R**	**M**	**O**	**N**	**S**	**S**	**D**	**N**	**T**
O	I	C	O	R	I	E	L	T	C	S	O	D	N	R	D	U	T	L	E	Y	D	N	L	A	H
O	**H**	**A**	**L**	**N**	**D**	**Y**	**E**	**L**	**T**	**I**	**D**	**R**	**A**	**D**	**O**	**E**	**C**	**T**	**L**	**E**	**I**	**R**	**O**	**C**	**I**
N	S	O	L	H	R	A	T	E	O	D	L	M	H	A	A	T	F	W	M	O	M	D	I	M	R
N	**R**	**M**	**I**	**D**	**M**	**U**	**M**	**W**	**F**	**T**	**A**	**A**	**U**	**M**	**L**	**D**	**O**	**E**	**T**	**U**	**R**	**H**	**L**	**O**	**S**
I	F	G	E	L	H	U	S	L	E	N	P	O	U	C	E	D	V	D	L	U	C	H	B	E	E
I	**E**	**E**	**B**	**H**	**C**	**O**	**L**	**D**	**V**	**D**	**E**	**C**	**H**	**O**	**P**	**N**	**E**	**L**	**S**	**A**	**H**	**L**	**E**	**G**	**F**
R	U	U	U	M	M	R	U	N	D	C	D	U	G	I	S	S	D	F	N	L	H	I	R	S	T
R	**T**	**S**	**R**	**I**	**H**	**L**	**N**	**F**	**U**	**S**	**S**	**I**	**T**	**U**	**D**	**C**	**M**	**N**	**U**	**R**	**M**	**M**	**U**	**U**	**U**
H	N	A	I	T	Y	I	P	B	H	Y	N	F	T	T	C	O	U	T	I	C	T	P	F	Y	M
H	**M**	**Y**	**F**	**P**	**T**	**C**	**I**	**T**	**Y**	**O**	**C**	**T**	**G**	**F**	**N**	**Y**	**D**	**B**	**P**	**I**	**Y**	**T**	**I**	**A**	**N**
S	P	P	W	A	F	S	Y	O	M	I	C	R	B	F	R	Y	Y	G	R	M	A	W	T	N	O
S	**O**	**N**	**T**	**W**	**A**	**M**	**R**	**G**	**D**	**Y**	**R**	**F**	**O**	**R**	**C**	**I**	**H**	**O**	**Y**	**S**	**F**	**A**	**W**	**P**	**P**
D	B	R	S	W	W	K	N	P	L	B	A	N	F	B	P	R	C	H	G	E	R	S	P	P	A
D	**A**	**P**	**P**	**S**	**R**	**E**	**G**	**H**	**C**	**R**	**P**	**B**	**S**	**N**	**A**	**B**	**L**	**P**	**N**	**K**	**W**	**W**	**S**	**R**	**B**
L	D	H	N	O	A	G	I	W	U	M	Y	I	O	W	N	C	L	O	B	A	V	K	K	F	C
L	**C**	**F**	**K**	**K**	**V**	**A**	**B**	**O**	**L**	**C**	**N**	**W**	**B**	**I**	**Y**	**M**	**U**	**W**	**I**	**G**	**A**	**O**	**N**	**H**	**D**
C	M	I	F	P	D	Y	V	C	W	K	R	S	S	G	G	A	N	M	O	S	Y	L	C	G	L
C	**L**	**G**	**C**	**L**	**Y**	**S**	**O**	**U**	**N**	**A**	**G**	**G**	**F**	**S**	**R**	**K**	**W**	**U**	**V**	**Y**	**D**	**P**	**F**	**I**	**M**
M	H	V	G	V	J	H	R	U	B	L	H	P	L	D	W	B	S	U	K	B	E	R	D	T	G
M	**G**	**T**	**D**	**R**	**E**	**B**	**K**	**M**	**S**	**B**	**W**	**D**	**Y**	**P**	**H**	**L**	**B**	**C**	**R**	**H**	**J**	**V**	**G**	**V**	**H**
U	C	F	K	C	U	L	D	V	T	W	F	H	Y	M	U	M	K	N	F	F	P	U	H	D	B
U	**B**	**D**	**H**	**Y**	**P**	**F**	**W**	**N**	**K**	**M**	**U**	**V**	**L**	**Y**	**F**	**W**	**T**	**V**	**M**	**L**	**U**	**Y**	**K**	**F**	**C**
F	L	K	P	Y	L	C	M	S	J	T	W	Y	I	V	L	J	A	K	W	G	G	Y	M	I	K
F	**K**	**I**	**M**	**U**	**G**	**W**	**F**	**K**	**A**	**J**	**L**	**M**	**V**	**H**	**W**	**T**	**J**	**S**	**D**	**M**	**L**	**C**	**P**	**K**	**L**
P	J	D	V	G	O	M	B	D	Y	P	M	G	V	U	B	F	P	V	U	W	J	C	S	B	I
P	**I**	**B**	**S**	**C**	**J**	**G**	**U**	**V**	**P**	**F**	**B**	**U**	**I**	**G**	**M**	**P**	**Y**	**D**	**B**	**C**	**O**	**G**	**V**	**D**	**J**
Y	G	W	B	N	B	J	F	R	F	V	I	B	C	P	X	L	G	J	D	D	B	J	Y	U	F
Y	**F**	**U**	**Y**	**J**	**W**	**D**	**Y**	**J**	**W**	**L**	**X**	**P**	**P**	**B**	**I**	**V**	**P**	**R**	**K**	**J**	**G**	**N**	**B**	**W**	**G**
B	V	J	A	F	G	V	K	G	P	U	G	K	P	Y	J	K	J	C	Y	P	W	B	V	H	U
B	**U**	**H**	**X**	**B**	**B**	**P**	**D**	**Y**	**G**	**K**	**V**	**Y**	**C**	**K**	**U**	**U**	**S**	**K**	**F**	**V**	**B**	**F**	**Y**	**J**	**V**
G	W	M	Y	X	K	X	E	K	S	G	U	W	J	K	V	W	M	Y	X	R	F	T	X	K	V
G	**V**	**K**	**V**	**T**	**F**	**R**	**X**	**C**	**J**	**W**	**J**	**K**	**W**	**W**	**G**	**G**	**V**	**G**	**E**	**X**	**K**	**X**	**A**	**M**	**W**
W	A	Y	M	K	P	B	C	Z	V	F	Z	Q	W	E	O	V	W	R	P	V	K	G	J	W	Z
W	**Z**	**W**	**J**	**G**	**K**	**V**	**V**	**R**	**M**	**V**	**O**	**E**	**J**	**Q**	**Z**	**F**	**F**	**Z**	**W**	**B**	**P**	**K**	**M**	**Y**	**A**
K	R	L	T	J	E	Z	W	H	X	X	J	Z	M	N	K	N	O	Z	V	T	Z	F	Q	J	Q
K	**Q**	**J**	**Q**	**F**	**Z**	**T**	**P**	**Z**	**O**	**N**	**Y**	**N**	**Z**	**Z**	**V**	**X**	**X**	**H**	**C**	**Z**	**E**	**J**	**T**	**L**	**R**
V	K	Q	X	D	X	D	J	J	K	H	V	X	Z	L	Y	X	B	B	C	J	S	Z	G	O	J
V	**J**	**O**	**U**	**Z**	**S**	**X**	**C**	**B**	**B**	**X**	**K**	**L**	**M**	**X**	**J**	**H**	**K**	**J**	**J**	**P**	**X**	**D**	**J**	**Q**	**K**
J	Y	S	J	B	C	P	Z	Q	I	A	X	L	D	Z	M	Q	Z	I	S	X	X	X	U	Q	X
J	**X**	**Q**	**G**	**X**	**X**	**J**	**S**	**I**	**Z**	**Q**	**M**	**Z**	**Q**	**L**	**X**	**A**	**I**	**Q**	**Z**	**D**	**C**	**B**	**X**	**S**	**Y**
Z	X	X	Q	Q	Z	F	X	F	Q	Z	Q	V	Q	J	F	P	H	P	Z	Z	U	M	N	V	W
Z	**W**	**V**	**N**	**M**	**U**	**Z**	**Q**	**X**	**H**	**P**	**F**	**J**	**D**	**V**	**Q**	**Z**	**Q**	**X**	**G**	**F**	**Z**	**Q**	**Q**	**X**	**X**
X	Z	B	C	U	Q	W	G	X	G	Q	B	C	K	Q	Q	G	X	X	J	Q	L	Q	Z	Z	Y
X	**Y**	**Z**	**Z**	**Q**	**L**	**Q**	**Z**	**P**	**X**	**G**	**Q**	**Q**	**X**	**C**	**B**	**Q**	**G**	**F**	**Q**	**W**	**Q**	**U**	**C**	**B**	**Z**
Q	Q	Z	Z	Z	V	Q	Q	Y	Z	J	K	J	X	X	Z	Z	Q	Q	Q	K	Q	V	W	X	P
Q	**P**	**X**	**W**	**V**	**Q**	**K**	**J**	**Q**	**Q**	**Z**	**Z**	**X**	**K**	**J**	**K**	**J**	**Z**	**Y**	**X**	**Q**	**V**	**Z**	**Z**	**Z**	**Q**
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

for the corresponding portion of the key-text is IF THERE. The plain-text and the key-text stop simultaneously but the words IS and ARE suggest themselves for trial for a continuance of the key. The key IF THERE IS gives PROCEED TO. Here again the plain-text and the key-text stop simultaneously and after a hasty trial of the words which suggest themselves for a continuance of the key-text, such as ANY, SOME, etc., without results, recourse is had once more to the sliding strips, selecting the W, K and Y strips. After a little experiment, the combination $\frac{\text{NOJ}}{\text{REL}}$ is found, which suggests the plain-text word RELIEF. This gives NO JUST for the corresponding portion of the key-text. Each time the key and the plain-text stop together, and the context has failed to suggest the correct word, recourse is had to the sliding strips. The process is very rapid and takes much less time to do than to explain.

B. Tables similar to this one, for use with messages enciphered by a Vigénère Table may be made, and used in exactly the same manner. The table applying to the Beaufort method would be different from that applying to the Vigénère method.

The Riverbank Laboratories is indebted to Lieutenant Paul H. Burdick for the original suggestion involving the sliding strip idea. Lieut. Burdick's strips contained the same combinations but arranged only alphabetically. It is believed that our modification of his original scheme improves the system considerably and makes the solution of a single running key message involving direct or reversed alphabets a very simple and easy matter.

(6) Solution of a single message enciphered by a known mixed alphabet sliding against a direct alphabet, or a reversed alphabet.

As long as a mixed alphabet concerned is known, it is only necessary to compile a table similar to table 10, applying to the conditions resulting from the sliding of the particular alphabets concerned. The procedure from there on is exactly the same, and the solution of a single message may be secured with the same ease as is the case when the direct or the reversed alphabet is used.

(7) Solution of a single message enciphered by a known mixed alphabet sliding against the same mixed alphabet (Modified Vigénère Table).

What was said under section (6) applies here also.

Up to this point only those cases involving direct, reversed or known mixed alphabets have been considered.

The Vigénère Table is only one form of a square or quadricular table, as it is sometimes called. The direct alphabet forms the basis of the square, or the alphabet upon which all the sub-alphabets are based. These sub-alphabets are all direct alphabets or reversed alphabets, and the correct determination of a single letter in any one of them solves that whole alphabet to which it belongs. But if a mixed alphabet is substituted for the direct alphabet, and the table is constructed as before, all of the sub-alphabets are mixed alphabets, and form a series of interrelated mixed alphabets. The correct determination of a single letter in any one of these alphabets gives no clue to the value of any other letter in the same alphabet or any other one of the interrelated series of alphabets. Such a table is known as a Modified Vigénère Table; the alphabet upon which it is based is called a Primary Alphabet; and the series of sub-alphabets are called Secondary Alphabets. The whole is called a Primary Alphabet System. The Primary Alphabet is most often a Key-Word Alphabet: i. e., it is an alphabet which begins with a key-word and is followed by the rest of the unused letters of the alphabet. Its popularity is due to the ease with which such an alphabet may be written or communicated, without the necessity of writing or remembering the entire alphabet. The remaining pages will deal with the methods of recovering unknown primary alphabets from running-key messages, and of solving a series of running-key messages involving unknown primary alphabets.

Before anything can be done with such cases it is necessary to determine first, whether Method (1) or Method (2) of enciphering was applied, and second, what the initial letter of the Primary Alphabet is. In order to show how this is done, it is necessary to consider some fundamental features of a quadricular table, of which the ordinary Vigénère Table is an example. In finding the cipher equivalents on the basis of a Vigénère Table, by the use of two sliding direct alphabets, A of one strip, say the lower one, is set under the key letter designated on the other strip, the upper one. If the cipher letter is to be taken according to Method (1), the Vigénère method, the plain-text letter is sought on the lower strip and the cipher letter on the upper strip. If the cipher letter is to be taken according to Method (2), the Beaufort Method, the plain-text letter is sought on the upper strip, and the cipher letter on the lower strip. In both cases, the first letter of the alphabet upon which the table is based, the letter A, is set opposite the key letter. In the case of a Modified Vigénère Table, the first letter of the alphabet upon which the table is based, the Primary Alphabet, is set under the designated key letter in the upper strip. When Method (1) is to be used for enciphering, the plain-text letter is sought upon the lower strip and the cipher letter is taken from the upper strip. When Method (2) is to be used, with the same setting, the plain-text letter is sought upon the upper strip, and the cipher letter is taken from the lower strip. A concrete example will make this clear, and is given below:

```
TREBIZONDACFGHJKLMPQSUVWXYTREBIZONDACFGHJKLMPQSUVWXY
  TREBIZONDACFGHJKLMPQSUVWXY
```

Method (1) Key E; plain-text C; cipher G. Or $\frac{E}{C} \rightarrow G$

Method (2) Key E; plain-text C; cipher D. Or $\frac{E}{C} \rightarrow D$

Now consider the reciprocal relations of these two examples, viz., key C, plain-text E. The two strips are now in this position:

```
T R E B I Z O N D A C F G H J K L M P Q S U V W X Y T R E B I Z O N D A C F G H J K L M P Q S U V W X Y
                    T R E B I Z O N D A C F G H J K L M P Q S U V W X Y
```

Method (1) Key C; plain-text E; cipher G. Or $\frac{C}{E} \rightarrow G$

Method (2) Key C; plain-text E; cipher P. Or $\frac{C}{E} \rightarrow P$

In the case of Method (1) the reciprocal relation gives exactly the same result, and this will hold true in all cases. Therefore, stated generally, when Method (1) is used, $\frac{X}{Y} \rightarrow Z$ and $\frac{Y}{X} \rightarrow Z$, where X, Y and Z stand for any letters. But in the case of Method (2) the reciprocal relation does not give the same result. However, if the two sliding strips be placed in the following position:

```
T R E B I Z O N D A C F G H J K L M P Q S U V W X Y T R E B I Z O N D A C F G H J K L M P Q S U V W X Y
                T R E B I Z O N D A C F G H J K L M P Q S U V W X Y
```

it will be seen that by Method (2) Key D, with plain-text C, the cipher letter is E. Stated generally, when Method (2) is used, $\frac{X}{Y} \rightarrow Z$ and $\frac{Z}{Y} \rightarrow X$.

The second important principle deals with the three elements concerned in enciphering: (1) the key letter, (2) the plain-text letter, and (3) the cipher letter. In the example above, when the key letter is E, the plain-text letter T is enciphered by E when Method (1) is used. That is, the cipher letter and the key letter are identical, and the plain-text letter which is enciphered is the first letter of the primary alphabet. In the same example, when Method (2) is used, and when the key letter is E, the plain-text letter E, is enciphered by T. That is, the key letter and the plain-text letter are identical and the cipher letter is the first letter of the primary alphabet. Stated graphically these relations are as follows:

TABLE 11.

If there are at least two different sets of combinations where

(Case 1) Cipher letter = key letter, both sets involving the same plain-text letter, then Method (1) is indicated, and the plain-text letter is the first letter of the primary alphabet.

(Case 2) Cipher letter = key letter, both sets involving different plain-text letters, then Method (2) is indicated. The first letter of the Primary alphabet remains unknown.

(Case 3) Key letter = plain-text letter, both sets giving the same cipher letter, then Method (2) is indicated, and the cipher letter is the first letter of the primary alphabet.

TABLE 11—Continued.

(Case 4) Key letter = plain-text letter, both sets giving different cipher letters, then Method (1) is indicated. The first letter of the primary alphabet remains unknown.

(Case 5) Cipher letter = plain-text letter, both sets involving the same key-letter, then either Method (1) or (2) is indicated. The key letter is the first letter of the primary alphabet.

It follows as a corollary that when the key letter coincides with the first letter of the primary alphabet, all the cipher letters are enciphered by themselves; accordingly when the key letter for any column has been found to be identical with the first letter of the primary alphabet, regardless of whether Method (1) or (2) had been used, the plain-text values may be inserted at once, being the same as the cipher letters. And vice versa, in any column where it has been found that a single cipher letter represents the same plain-text letter as itself, all the other plain-text letters in the same column may be written at once, and the key letter is the first letter of the primary alphabet.

Application of these principles will now be made in the problems which follow.

(8) Recovery of a mixed alphabet given (A) the running-key, the plain-text and the cipher-text; (B) the plain-text and the cipher-text.

(A) It may easily happen that a message or a series of messages in a Running-Key Cipher has been captured or secured by other means. If, as has been known to occur often, the transcription of the cipher-text accompanies the messages, together with the key-text, it becomes necessary to find the mixed alphabet which was used, in order to facilitate the decipherment of other messages which may be intercepted. The following methods are presented simply to point out a few guiding principles for the recovery of the mixed alphabet used, for it may be accomplished by several methods, all subject to the ingenuity of the decipherer.

Given the following series of messages with their decipherment and key:

	Key-text	SEEKI	NGFOR	THESE	THING	SHEEX	CEEDED
1.	Plain-text	GASAT	TACKS	AREMA	KINGO	URPOS	ITIONS
	Cipher-text	GIEXH	KRJSR	FOUMI	YXMYX	UOCBX	BONVDD
2.	Plain-text	REPEA	TLAST	ORDER	REGAR	DINGM	OVEMEN
	Cipher-text	RUCQG	KQQOP	JOGEW	PKWJI	DXDJH	DXUUUW
3.	Plain-text	STOPI	NTERF	ERENC	EOFSH	IPMEN	TSJUST
	Cipher-text	SOBMJ	RVHCT	OOUNL	OYVNC	IJRUT	NEMJEQ
4.	Plain-text	PREPA	RETOM	OVEYO	URMEN	BYDAY	LIGHTA
	Cipher-text	PWUMG	UJRMD	JNUYB	BOSDY	BFGIV	INJPOM
5.	Plain-text	WHATI	SCAUS	INGIN	TERRU	PTION	OFWIRE
	Cipher-text	WKIYJ	NKQFR	HZJID	GKEUM	PWNBT	DHYRWG

The first step is to find the first letter of the Primary Alphabet and the method of encipherment. (See explanation on page 30). In columns 1, 14 and 21 it is seen that the cipher letters and the plain-text letters coincide. This comes under Case 5 above. The first letter of the primary alphabet is therefore S, but either Method (1) or (2) is indicated. In colum 3, the first message, key letter E and cipher letter E coincide, plain-text letter is S; in column 6, the fifth message, key letter N and cipher letter N coincide, plain-text letter is S. These two different sets of combinations both involving the same plain-text letter indicate Case 1, which shows that Method (1) was used in enciphering. Next, an alphabet is made showing, for the key letter E, the cipher equivalents of the plain-text letters as given by all the messages. This alphabet gives, if it has a sufficient number of values, all the data necessary for the recovery of the primary alphabet. In the above series of messages the alphabet of cipher equivalents for the key letter E, is as follows:

Cipher	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plain-text		O	P	N	S		D	F	A	G	H	C	J	I	T		K	M			E		R			

The plain-text equivalent K for the cipher letter Q was secured from the reciprocal relation $\frac{K}{E}$, the fourth letter in message number 2. (See Page 30).

From this single partial secondary alphabet it is possible to reconstruct completely the whole primary alphabet by a method given in a previous publication.† At an interval of 24 spaces forward, or 1 space back, the sequence WRMJGDNIA gives sufficient of the primary alphabet to reconstruct it completely. It is SPECULATIONBDFGHJKMQRVWXYZ.

This method, however, requires that there be a considerable number of equivalents in the secondary alphabet chosen for reconstructing the primary; and in a single message, or in only a few short messages enciphered by the same alphabet but with different running-keys, this is impossible. For such cases, another method, more difficult, is given below:

MESSAGE.

```
                  *            *
Key-text,     INALM  OSTEV  ERYWO  RKARE  FOUND
Plain-text,   RELIA  BLEIN  FORMA  TIONS  TATES
Cipher-text,  AACOA  PZWRX  KCFWD  XPDLV  ODJAA

                         *         *
Key-text,     REPET  ITION  SOFSO  MEOFT  HECHI
Plain-text,   THATD  IPLOM  ATICR  ELATI  ONSAR
Cipher-text,  XPVWL  NCOHN  XIHRC  EYDOU  UARSA

                       *
Key-text,     EFSTA  TEMEN  TSTHO  UGHIN  DIFFE
Plain-text,   EABOU  TTOBE  SEVER  EDONA  CCOUN
Cipher-text,  LQEIM  HWOFA  FVKPC  XUUEO  WDTGA
```

†See Publication No. 15 of Riverbank Laboratories: A Method of Reconstructing the Primary Alphabet from a Single One of the Series of Secondary Alphabets, 1917.

Construct direct alphabets giving the cipher equivalents for the key letters E, T, O and A.†

	Cipher	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Key letters	E	N				M	B					F	E				H		I				S	T	U	L		Plain-text letters
	T			P			S		T	O	U	V	D			F						I		E	R			
	O			R	A				O	T						M	B				F	H						
	A	M		L	O									U		N		F		H			P		S			

With the data thus secured, experimenting with two sliding strips of cross-section paper follows: The first letter in the primary alphabet, M, and the method of enciphering, the Vigenére, are found by the same method as above, the cases indicated by an asterisk placing them under cases 1 and 5; accordingly M is set down on both strips in the first space. It is important to remember that as each new letter is determined it must be set down at once on both strips.

It may be stated that wherever in a secondary alphabet a normal sequence of two, three or four cipher letters is above a normal sequence of plain-text equivalents, it usually but not always indicates that these letters do not form a part of the key word in the primary alphabet. For example, in the first of the series of secondary alphabets given above, where E is the key letter, the sequence VWX of the cipher letters has for its equivalent the sequence STU of the plain-text. This indicates that in the primary alphabet both of the sequences STU and VWX are unbroken. Since these two sequences are adjacent they can be combined and made into one sequence STUVWX. The fact that L of the plain-text equals Y of the cipher indicates at once that both L and Y are in the key word part of the primary alphabet, since it has been found that the sequence VWX is unbroken, and if Y were not in the key word part, its plain-text equivalent would have to be V and not L. Since Y is in the key word part, it is probable that Z is not and we may therefore set down on our sliding strips the sequence STUVWXZ in positions 20, 21, 22, 23, 24, 25, 26 as shown graphically:

```
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
M                                                        S  T  U  V  W  X  Z  M                                                        S  T  U  V  W  X  Z
M                                                        S  T  U  V  W  X  Z
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

Now the key letter E secondary alphabet gives VWX as the cipher equivalents of STU, respectively and E as the cipher equivalent of M. Now the position of M has been determined: it is the first letter in the alphabet. Therefore, when STU are placed under VWX, M should be under E. This means that E must go into the fourth position, and is placed accordingly on both strips. The table shows that cipher L is the equivalent of plain-text E; the latter having just been fixed for position 4, the position of L is thus

†This table includes the values given by the reciprocal relations (see page 30).

indicated as number 7. The table shows that cipher Y is the equivalent of plain-text L; the latter having just been fixed for position 7, the position of Y is thus indicated as number 10. The primary alphabet is then as follows:

```
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
M        E        L        Y                             S  T  U  V  W  X  Z  M        E        L        Y                             S  T  U  V  W  X  Z
         M        E        L        Y                             S  T  U  V  W  X  Z
         1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

It would be possible to secure further values from the E alphabet by assuming the position of certain letters, and checking up the assumptions from the relations given, but a surer way is to proceed to some other alphabet. The T secondary alphabet has many values and the position of T is already fixed in the primary alphabet; therefore, this alphabet is next exhausted for new values. From it, by the same process as above, the following positions and values are secured:

```
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
M  I     E  R     L  O     Y        D  F  H  J  K        S  T  U  V  W  X  Z  M  I     E  R     L  O     Y        D  F  H  J  K        S  T  U  V  W  X  Z
                                                            M  I     E  R     L  O     Y        D  F  H  J  K        S  T  U  V  W  X  Z
                                                            1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The values given by the O secondary alphabet add the following letters to those already determined:

```
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
M  I     E  R     L  O     Y     C  D  F  H  J  K        S  T  U  V  W  X  Z  M  I     E  R     L  O     Y     C  D  F  H  J  K        S  T  U  V  W  X  Z
                     M  I     E  R     L  O     Y     C  D  F  H  J  K        S  T  U  V  W  X  Z
                     1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The values given by the A secondary alphabet add the following letters:

```
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
M  I  N  E  R  A  L  O     Y     C  D  F  H  J  K  P  Q  S  T  U  V  W  X  Z  M  I  N  E  R  A  L  O     Y     C  D  F  H  J  K  P  Q  S  T  U  V  W  X  Z
               M  I  N  E  R  A  L  O     Y     C  D  F  H  J  K  P  Q  S  T  U  V  W  X  Z
               1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The key word in the primary alphabet stands out very plainly now as MINERALOGY. The rest of the primary alphabet may now be filled out and further checking may be done directly with the cipher message itself.

(B) The running-text is not absolutely necessary to the recovery of the primary alphabet. Return to the five messages on page 31, and note that the cipher letter U occurs most frequently as the cipher letter of plain-text letter E by key letter E. It follows that in any column where E is enciphered by U, the key letter is E. From this it follows that two or more columns possessing a single combination of cipher letter and plain-text letter in common are the results of encipherment by the same key letter, and the cipher equivalents of plain-text letters may be compiled from all of these columns under one secondary alphabet. It is clear then that the secondary alphabet E, given in connection with these messages could have been compiled without a knowledge of the running-key text. From there on the process of recovering the primary alphabet is followed just as in the original example on page 32.

In case only one message is at hand, the procedure is modified somewhat by the assumption of additional key letters, such as T, O, A. Then the method given on pages 33 and 34 is applied.

9. Solution of a series of messages when the running-key text is known; the plain-text and the mixed alphabet unknown.

MESSAGES.

Key:	THERE	PRESE	NTATI	VESOF	THETH	REEGR	EATPO	WERSW	ILLME	ETDEC	EMBER
1 –	DLXFP	BRQWL	UVAIB	UEYPX	PCWLA	RQJFT	LTDPH	YLDJT	RXYCW	JTPHB	JMZGF
2 –	LAWJW	QHGSQ	OEGFR	FIWZU	DPJAN	RKWEN	HTVAP	RYPSU	FGTMP	QZVJF	ETJMD
3 –	DLQFM	WSRWQ	LLHQW	MWCRU	VHIMH	GOEEF	PTVYF	LVRPW	QPQNL	PZVVF	YMMQS
4 –	KYIBQ	ARJYW	XHFIC	EUOFN	JRQMY	GWJBK	LTVNW	GJPIW	BJSWI	IDCOU	LSFLK
5 –	LAWRI	NJHYE	UBONH	IJELK	LKOEP	KVHVZ	LSQIH	GOHFJ	PJYCW	GHDJD	JRSOG
6 –	DLVBF	VRQWL	UDSVC	WYWTF	ZYPDM	RJVNZ	GOZPH	YKEWN	UUGEL	UQMLD	PNBHX
7 –	LHAPO	APNJE	EHNFH	CWUDQ	QVYQX	PNETK	IEEAD	TOKSC	HYVBP	WNVJF	ESRXH
8 –	LAWXW	VTQRL	KLIZH	IWHEJ	KYVSP	JQYFG	WRNSB	RIPXC	CVQIV	HIPRB	RISAG
9 –	ZYOGE	QPLUQ	ZQNLC	UQRRK	IVPQM	PHUFM	YEKNO	TQPGW	PUIXJ	VIDOW	WYJPM
10 –	LYOKO	PJWXL	ZMEDO	WKZTW	JMQQX	LBQJB	OGHHL	NJYOZ	DIVYQ	YQIME	NWNWF

All columns enciphered by the same key letter are encipherments by means of one particular alphabet. For example, note the various columns enciphered by key letter E. It is clear that plain-text letter E would be enciphered by the same cipher letter every time it occurred in any of the key letter E columns. It follows, therefore, that a frequency table of cipher letters combining all of the key letter E columns would be nothing but a single mixed substitution alphabet, and given a sufficient number of such columns, the frequency table would enable one to assign values to cipher letters on the basis of frequency alone. From this it follows that a problem such as the above resolves itself into a series of inter-related mixed alphabet problems (inter-related since they are all dependent upon one primary alphabet). It is necessary therefore to make frequency tables for the most frequently recurring key letter columns and then to attempt substitution of values on the basis of such tables. Skeletons of words will manifest themselves in the cipher-text, and it should be possible to decipher a sufficient amount to enable the decipherer to apply the principles elucidated above for the recovery of a primary alphabet. Once this is done, even partially, sufficient of the decipherment can be accomplished finally to reconstruct completely the primary alphabet. The solution of the messages would then be at hand.

Frequency tables are therefore made for the key letters which show any repetitions, such as E. T. R, etc. These tables follow:

	Key-letter E.		Key-letter T.		Key-letter R.		Key-letter H.		Key-letter A.		Key-letter I.
A	||	A	|	A		A	||||	A	|	A	
B	|	B	|	B	|||	B		B		B	||
C		C		C		C	|	C		C	||||
D		D	卌 ||||	D	||	D		D		D	|
E	卌 |||	E	|||	E	|	E		E	|||	E	
F	|	F	||	F	卌	F		F	|	F	|
G	||||	G		G	卌 |	G		G	||	G	
H	卌 ||	H	|||	H	|||	H	|||	H	|	H	||||
I	卌 |||	I	卌	I		I		I	|	I	
J	卌 卌 卌	J	||	J	||||	J		J		J	
K	|||	K	|||	K	卌 |	K	|	K		K	
L	卌 卌 ||||	L	卌 卌	L	|	L	|||	L		L	
M	|||	M	|||	M	||	M	|||	M		M	
N	|||	N	|||	N	|	N	|	N	||	N	
O	卌 卌 ||	O		O		O		O	||	O	|
P	卌 ||||	P	|	P	卌 ||||	P	|||	P		P	||
Q	卌 卌 卌 |||	Q	卌 ||||	Q		Q		Q		Q	|
R	|||	R		R	卌 |||	R	|	R	|	R	||
S		S	|	S	||	S		S	||	S	
T		T	|	T	||	T		T	||||	T	
U	|||	U		U		U		U		U	|
V	卌 |||	V	卌 |	V		V	||	V		V	
W	卌 卌 卌 ||||	W		W		W		W		W	|
X	||	X		X	||	X	||	X		X	
Y	卌 ||	Y		Y	|	Y	卌 |	Y		Y	
Z		Z	卌 |	Z	||	Z		Z		Z	

	Key-letter P.		Key-letter W.		Key-letter L.		Key-letter O.		Key-letter S.		Key-letter M.
A	𝍷𝍷𝍷𝍷	A		A		A		A		A	
B	𝍷	B		B		B	𝍷	B		B	𝍷
C		C	𝍷𝍷	C		C		C	𝍷	C	𝍷𝍷
D		D		D		D	𝍷𝍷	D		D	
E		E		E		E	𝍷	E	𝍷	E	𝍷
F		F		F		F	𝍷𝍷	F	𝍷	F	
G		G	𝍷𝍷	G	𝍷𝍷	G		G	𝍷	G	
H	𝍷	H		H		H	𝍷𝍷𝍷	H	𝍷	H	
I	𝍷	I		I	𝍷𝍷	I		I	𝍷	I	𝍷𝍷
J		J	𝍷	J	𝍷𝍷	J		J	𝍷𝍷	J	
K		K		K		K		K		K	
L		L	𝍷	L		L	𝍷𝍷	L		L	
M		M		M		M		M		M	𝍷𝍷𝍷
N	𝍷𝍷𝍷	N	𝍷𝍷	N		N		N		N	𝍷𝍷
O		O		O		O	𝍷	O	𝍷𝍷	O	
P	𝍷𝍷𝍷	P		P	𝍷	P	𝍷𝍷	P	𝍷	P	
Q	𝍷𝍷	Q		Q	𝍷𝍷	Q		Q		Q	
R		R	𝍷𝍷	R		R	𝍷𝍷	R	𝍷𝍷	R	𝍷
S	𝍷	S		S	𝍷	S		S	𝍷𝍷𝍷	S	𝍷𝍷
T		T	𝍷𝍷𝍷	T	𝍷	T	𝍷𝍷	T		T	𝍷
U		U	𝍷	U	𝍷𝍷	U		U	𝍷𝍷	U	
V	𝍷𝍷	V		V	𝍷𝍷𝍷	V		V		V	
W	𝍷	W	𝍷𝍷𝍷	W		W	𝍷	W	𝍸 𝍷	W	𝍷𝍷
X		X		X	𝍷	X		X	𝍷𝍷	X	𝍷
Y	𝍷	Y	𝍷𝍷	Y	𝍷𝍷𝍷	Y		Y	𝍷𝍷𝍷	Y	𝍷𝍷
Z		Z	𝍷	Z		Z	𝍷	Z	𝍷	Z	

Note particularly the frequency table for key letter A, which closely approximates the normal. This leads to the assumption that the cipher letters here really represent the plain-text letters, and that hence the key letter coincides with the first letter of the primary alphabet, and the latter would therefore be A (see page 30). In any column therefore in which key letter and cipher letter coincide, the plain-text letter may be written at once as A. Also, the plain-text equivalents for key letter A columns are the cipher letters, and hence two whole columns may be completely substituted at once.

The frequency table of the key letter E columns shows that W probably represents E, Q probably represents T, and L probably represents O or N. The value of cipher letter E is A, in accordance with the preceding paragraph.

The frequency table of the key letter T columns shows that D, L or Q may represent E. But in the preceding table it was found that $\frac{E}{T}$ probably gives Q, wherefore, $\frac{T}{E}$ should give Q (see page 30). Therefore Q is assumed to represent E. This leaves L or D for T. The digraph LA occurs four times under the key letters TH and the trigraph LAW occurs three times under the key letters THE. Since W has already been assumed to be E in the E columns, LAW could very well represent THE, which makes L equal T in the T columns, and A equal H in the H columns.

The frequency table of the key letter R columns shows that P is very probably E. Now $\frac{R}{E}$ equals P, therefore $\frac{E}{R}$ equals P; hence in key letter E columns R is substituted for P.

In the key letter H columns, Y is evidently E; from this relation the value of Y in the key letter E columns becomes H. ($\frac{H}{E} \rightarrow$ Y; hence $\frac{E}{H} \rightarrow$ Y).

In the eighth message, group 6, QY equals TH; in the G frequency table, F is good for E; hence QYD is assumed to be THE. This gives F equals G in key letter E alphabet. The results of all these steps are shown in the accompanying figure 2.

This is about as far as substitution from frequency tables alone will allow. Further progress must be made by guessing words. In the sixth message, the sixth group begins RJ equals AN. Referring to the frequency table of the key letter E columns it is seen that V may well represent D. Furthermore, in the sequence VW, which would probably be unbroken in the primary alphabet, D would be likely to precede E. Note now that the sequence VWXY equals DE-H, and that F has been found to equal G, and therefore X could not equal G, and from this it follows that VWXY would equal DEFH. This gives the new value X equals F in the key letter E columns.

In the first message only a little imagination is necessary to guess that the first word is INFORMATION given— —F—R—AT—$\overset{O}{\underset{N}{—}}$. Moreover, the values fit very well for L to equal IN, and for RQWLU to equal ATION, of which there is a repetition in the sixth message, in the same location.

Figure 2.

```
Key:  T H E R E   P R E S E   N T A T I   V E S O F   T H E T H   R E E G R   E A T P O   W E R S W   I L L M E   E T D E C   E M B E R

 1—   D L X F P   B R Q W L   U V A I B   U E Y P X   P C W L A   R Q J F T   L T D P H   Y L D J T   R X Y C W   J T P H B   J M Z G F
          F   R     A T   O       A         A             E T H   A T   E     O T   A       O                 E   N A         N A
                          N                                                   N               N

 2—   L A W J W   Q H G S Q   O E G F R   F I W Z U   D P J A N   R K W E N   H T V A P   R Y P S U   F G T M P   Q Z V J F   E T J M D
      T H E   E         A T       G                       N       A     E       T           H E A           A R   T     N     A

 3—   D L Q F M   W S R W Q   L L H Q W   M W C R U   V H I M H   G O E E F   P T V Y F   L V R P W   Q P Q N L   P Z V V F   Y M M Q S
          T               T     T H E       E           A     A       A       R T           D A   A           O   R     D     H A
                                                                                                              N

 4—   K Y I B Q   A R J Y W   X H F I C   E U O F N   J R Q M Y   G W J B K   L T V N W   G J P I W   B J S W I   I D C O U   L S F L K
                    A N   E       F                       T         E         O T           N E   A                           O
                                                                              N

 5—   L A W R I   N J H Y E   U B O N H   I J E L K   L K O E P   K V H V Z   L S Q I H   G O H F J   P J Y C W   G H D J D   J R S O G
      T H E A           A A       O           N       T             D         O S E                           E         N     N
                                                                              N

 6—   D L V B F   V R Q W L   U D S V C   W Y W T F   Z Y P D M   R J V N Z   G O Z P H   Y K E W N   U U G E L   U Q M L D   P N B H X
          D   G     A T   O       S         H     A       R       A N D         O   A                         O     E   O     R     A
                          N                                                                                   N

 7—   L H A P O   A P N J E   E H N F H   C W U D Q   Q V Y Q X   P N E T K   I E E A D   T O K S C   H Y V B P   W N V J F   E S R X H
      T A   E       E     A       N         E         E   H           A         E               A           R   E     N     A     F

 8—   L A W X W   V T Q R L   K L I Z H   I W H E J   K Y V S P   J Q Y F G   W R N S B   R I P X C   C V Q I V   H I P R B   R I S A G
      T H E   E       T   O     T L         E             D         T H E     E R             E               D
                          A

 9—   Z Y O G E   Q P L U Q   Z Q N L C   U Q R R K   I V P Q M   P H U F M   Y E K N O   T Q P G W   P U I X J   V I D O W   W Y J P M
              A     E     T     E N T       T             R           E       H E     A     T E   A           N   D           E     R

10—   L Y O K O   P J W X L   Z M E D O   W K Z T W   J M Q Q X   L B Q J B   O G H H L   N J Y O Z   D I V Y Q   Y Q I M E   N W N W F
      T           A   E   O       E                       T           T         G         N                   T     H E
                          N
```

Furthermore, the word ending in ATION in the sixth message may now be completed, since the following values are given:

```
DLVBFVRQWLU
IND G ATION
```

Obviously, the word is INDIGNATION.

The decipherment thus far has now produced sufficient values to warrant an attempt at reconstructing the primary alphabet. Applying all the principles illustrated in the preceding sections, a little experimenting will produce new values, which in turn enable further progress in decipherment and recovery of the alphabet to be made. The mixed alphabet is AGINCOURTBDEFHJKLMPQSVWXYZ. The deciphered messages read as follows:

Key: THERE	PRESE	NTATI	VESOF	THETH	REEGR	EATPO	WERSW	ILLME	ETDEC	EMBER
1 – INFOR	MATIO	NHASR	EACHE	DMETH	ATNEG	OTIAT	IONSF	ORTHE	NATIO	NALLO
2 – THERE	GULAT	INGCO	MMISS	IONPL	ACEDW	ITHTH	EHEAD	DEPAR	TMENT	AMOUN
3 – INTOU	CHWIT	HTHES	WEDIS	HAMBA	SSADO	RTHUR	SDAYA	MINFO	RMEDT	HATTH
4 – REMIT	TANCE	SOFSI	LVERM	USTBE	SENTT	OTHEM	ONETA	RYCOM	MISSI	ONNOT
5 – THEAM	ERICA	NGOVE	RNMEN	TISNO	TDISP	OSEDT	OSUPP	LYTHE	LOANU	NLESS
6 – INDIG	NATIO	NISHI	GHINA	MERIC	ANDIP	LOMAT	ICCIR	CLESO	VEROU	RFAIL
7 – TAKES	TEPSA	TONCE	BEFOR	ETHED	EPART	MENTO	FSTAT	ETOPR	EVENT	ANYFU
8 – THELE	NGTHO	FTIME	REQUI	REDFO	RTHES	ERVIC	EMENT	IONED	ISTWO	WEEKS
9 – MESSA	GEOFT	WENTI	ETHIN	STREC	EIVED	HEREA	FTERA	LLFUN	DSASP	ERORD
10 – TESTS	ARENO	WBEIN	GCOND	UCTED	BYTHI	SGOVE	RNMEN	TFORT	HEPUR	POSEO

(10) Solution of a series of messages with no knowledge of key, alphabets, or text.

All of the preceding principles have been elucidated step by step to prepare the way for the solution of a series of messages without the possession of any information whatsover.

In the section immediately preceding, the only knowledge possessed by the decipherer was that concerning the running-key. The advantage of possessing this information was that it enabled the decipherer to compile his frequency tables with the assurance that he was combining columns of cipher letters enciphered by the same alphabet. The next step is to find principles which will enable him to combine the correct columns of cipher letters without a knowledge of the key letters. Frequency tables of columns enciphered by the same key will tend to resemble each other in the distribution of cipher letters. Then, if individual frequency tables of the successive columns of cipher letters are made, a careful comparison of them will show that certain tables resemble certain others to such an extent that they may be assumed to have been enciphered by the same key-letter. When two, three, or four single frequency tables are combined, the high letters E, T, O and A may be found, and these values substituted throughout the messages in the columns concerned. Or it may be possible to compile the frequency tables applying to two or three different key letters, in which case adjoining columns will aid in corroborating the assumed values. Consider, for example, the single frequency tables applying to columns three, five, eight and ten in the problem given in the preceding section, made in the following form, for compactness and easy comparison.

```
Col. 3.  X  W  Q  I  V  A  O            Col. 5.  P  W  M  Q  I  F  O  E
            |||               ||                    ||              ||

Col. 8.  Q  G  R  J  H  N  L  W         Col. 10.  L    Q    W    E
         |||                                      ||||  |||       ||
```

Note that the high letters stand out and make even these fragmentary tables resemble each other. These of course were enciphered by the same key letter, E.

It is necessary then, to compare carefully all the frequency tables applying to all the columns of a series of messages, and to combine those which are similar.

The precedure from that point is exactly the same as in the section explained above. It will necessitate considerable more experimenting, but given time, the solution of a series of messages enciphered by the same running-key may be accomplished without knowledge of key, text or alphabets.

(11) It is clear that in a single message involving a multiple alphabet system of say five alphabets, the successive groups of five letters may be regarded as a series of messages in the same running-key, each message but five letters in length, the first message joining in sense with the second, the second with the third, etc. Hence the solution of such a message where a Vigénère Table, or the U. S. Army Disk has been used, or where the Primary Alphabet is known, may be solved by means of the Poly-Alphabet without the compilation of any frequency tables whatever. Suppose that the process of "factoring" has shown the message to involve five alphabets. The first ten cipher letters of the first alphabet are "set" on a Poly-Alphabet. The plain-text equivalents of the high-frequency generatrix of the first alphabet letters are to be joined to the plain-text equivalents of the high-frequency generatrix of the second alphabet letters, etc., the procedure is the same as that in the case of the solution of a series of messages in the same running-key. The key letters are sought and the entire message may then be solved.

SUMMARY AND CONCLUSIONS.

In the preceding pages it has been shown that:

(1) The Running-Key Cipher used in connection with any known alphabet or system of alphabets is solvable;

(2) A series of messages in the same key, when the alphabet employed is known may actually be deciphered in less time than it took to encipher the individual messages;

(3) An unknown alphabet may be recovered or reconstructed from a message or a series of messages which carry their decipherment with them;

(4) A series of messages in an unknown alphabet may be deciphered if the running-key is known;

(5) A series of messages may be deciphered in time with no knowledge of the running-key or the alphabets used.

Since among military, naval and diplomatic officers it is the generally accepted assumption that the enemy is in possession of a new cipher system or a new code-book at the moment of or very soon after its inception, the last sections, dealing with those cases where the alphabets used are unknown, may be disregarded. Since, further, the most that may be expected of a field cipher for army use is that it should offer to the decipherment by an interceptor obstacles sufficient to enable the intended recipient to carry out such orders or directions as are contained within the dispatches, it would seem that the safest plan in connection with a Running-Key Cipher is to use only mixed alphabets, which are made up not with the use of a key word, but are made absolutely according to the laws of chance, either by the use of a deck of cards or by random drawing from a box, and which, further, are changed very frequently. There is no doubt but that the Running-Key Cipher is simple and rapid and in these two respects meets the requirements of a cipher for field use. If the precautions outlined above are taken, they would add to these two features the third and most valuable one, namely, safety.

# An Introduction to Methods
for the
Solution of Ciphers

Publication No. 17

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Two Hundred copies of this publication were printed of which this is

No. 121

RIVERBANK
LABORATORIES
GENEVA
ILLINOIS

TABLE OF CONTENTS

AN INTRODUCTION TO METHODS FOR THE SOLUTION OF CIPHERS

ON THE FLEXIBILITY OF MIND NECESSARY IN CIPHER WORK

Deciphering is both a science and an art. It is a science because certain definite laws and principles have been established which pertain to it; it is also an art because of the large part played in it by imagination, skill, and experience. Yet it may be said that in no other science are the rules and principles so little followed and so often broken; and in no other art is the part played by reasoning and logic so great. In no other science, not even excepting the science of language itself, grammar, does that statement, "The exception proves the rule," apply so aptly. Indeed it may be said, and still be within the limits of the truth, that in deciphering, "The rule is the exception."

The reason for this is not hard to see. If one is dealing with a problem in physics, for example, a problem dealing with the temperature, pressure, and volume of a gas, the solution of the problem may be attained directly and with almost absolute accuracy, because the underlying laws are invariable and unchanging in their application. Because of this, the problem resolves itself into a problem in mathematics. From the very nature of mathematics, the results are absolutely predetermined. The data having been given, the solution is reached by a series of definite and unerring steps, subject to no modification whatever, because the results, being dependent upon nothing but the data, are fixed from the start. Each step follows inevitably from the preceding. No imagination is at all necessary; no assumptions need be made, which may prove to be untenable and therefore must be rejected and replaced by others.

Contrast this situation, on the other hand, with that which confronts the decipherer at the very beginning of his attempts to solve a problem. Many times the cipher carries with it not even so much as an indication of the particular language in which it is written. Granted, however, that he knows the language, the foundations of any language are so unstable, so variable, and so uncertain, that no absolutely fixed laws can be made to hold. This does not refer to the innumerable variations in inflection, conjugation, etc., with which every language has to contend, but refers particularly to the very roots from which a language springs—the elementary sounds, the elementary syllables, and the words, phrases, and sentences. There is no rule, and there can be no rule, to determine the sequence of sounds—there can be no law which says that sound "ay," for example, must always be followed by sound "em," or any other sound. There can be no rule which determines how many letters shall compose a syllable, how many syllables shall constitute a word; nor what words shall follow any given word. Indeed, the characteristics which distinguish a good writer or speaker from a poor one, are exactly those which are concerned with the flexibility with which the former employs and manipulates the words, phrases, and sentences. A single idea may be expressed in a multiplicity of ways, all differing markedly from each other. Furthermore, the nature of the text as a whole varies. For example, scientific text differs materially from literary text or military text.

All such conditions affect the raw material with which the decipherer must work—the letters themselves. Therefore, only the most generalized rules can ever apply to deciphering operations; and there can be only a few guiding principles, which the decipherer should always be ready to modify. The most important generalizations, for instance, are those which have been derived from what are known as frequency tables, which will be discussed in detail later. Briefly, a frequency table is a systematized count of the individual letters which make up text passages in any language. For the present, let us simply consider three of the generalizations which follow from these frequency tables for English. According to them, the single letter E, the pair of letters TH, and the group of letters THE are the most frequent. This does not mean that in every piece of text, no matter what length, E will be invariably the most frequent single letter, TH the most frequent pair of letters, or THE the most frequent group of three letters. But it is in endeavoring to apply these generalized principles to the special conditions of the particular problem in hand, that the decipherer makes the assumptions upon which his work rests. If the special conditions of the problem approximate or conform closely to the generalized principles, the solution readily follows. But this is rarely the case, and he is forced to modify, not only his assumptions, but also his methods, and even to discard some of them. It is the facility and ease with which a decipherer is able to modify his methods and discard his assumptions, which differentiates the good decipherer from the poor one. ***Deciphering is not a process for a "one-cylinder mind."***

Likewise the part played by imagination and intuition can hardly be overestimated. The knowledge of the circumstances surrounding the interception of a message, of the correspondents, etc., furnishes a wide field for the exercise of the intuitive powers; and a shrewd "guess" will often result in more progress than a whole day's painstaking labor. This faculty, so essential in deciphering, can be developed and trained. The exercise of the imaginative powers by attempting to assume whole words, given only two or three letters and their positions, will result in the stimulation of all the faculties concerned in the expression of ideas, will thus enlarge the decipherer's vocabulary, and otherwise arouse those qualities of mind which are peculiarly needed in cipher work.

Persistency is absolutely necessary for deciphering. Results are often secured only after seemingly endless experiment, and concentrated effort. It may be said that even after one has a thorough grasp of the underlying principles, patience and perseverance are the key-notes to success. *Yet, too long application soon results in mental exhaustion, and in such a condition little progress can be made. The decipherer will actually save time by ceasing from his labors and attacking the problem afresh later. A few minutes of work by a rested and clear mind is worth as many hours by a brain which is dull from fatigue.*

To summarize then, the qualities upon which success depends in deciphering are interrelated—reasoning from laws must be balanced with facility in modifying those laws; imagination must go hand in hand with discretion; and intuition can never wholly take the place of concentration and perseverance. ***Finally, let it not be forgotten that many times the greatest ally the mind has is that indefinable, intangible something, which we would forever pursue if we could—luck.***

SOME SUGGESTIONS

Standardization of the details of operation in any work is essential if confusion and its consequent loss of time and labor are to be avoided. If a definite method of procedure is adopted and followed consistently, after a time it becomes a habit, and skill and accuracy in using it become second nature.

As a result of considerable experience, not only in the instruction of cipher operators, but also in the successful application of deciphering principles to unknown ciphers, the Department of Ciphers of Riverbank Laboratories has adopted a series of standard methods, close adherence to which, it is believed, will expedite the work materially.

1. PAPER

Do not crowd any work, but at the same time avoid wasting paper. Work sheets SHOULD NOT BE DESTROYED. They form a necessary part of the record pertaining to the solution of the problem. No work is too insignificant to discard, therefore it should be done well from the start. Cross-section paper, with squares ¼ inch in size, is indispensable.

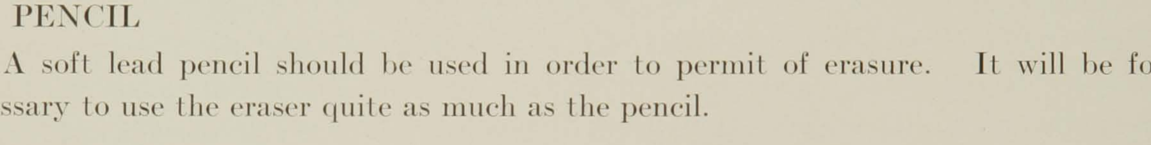
2. PENCIL

A soft lead pencil should be used in order to permit of erasure. It will be found necessary to use the eraser quite as much as the pencil.

3. WRITING

The process of enciphering and deciphering is by no means a ONE-MAN-JOB. Handwriting will have to be read by others. It should be legible and clear. In ordinary writing, a doubtful letter is supplied, or an incorrect one is corrected, from the context; but in cipher writing a single error or questionable letter may throw the writer himself off the track, as well as those who may have to go over his work later. Script letters are rarely used in cipher work. All letters should be "printed"; that is, Roman capitals should be used exclusively.

The following forms of Roman capital letters, and Arabic numerals have been adopted as standard. In a very short time speed and nicety in their use may be achieved. Lower case, or small letters, should never be used in cipher work.



4. SLUGGING

This is the printer's term for the placing upon a piece of work a number which accompanies it until it is completely finished and disposed of in the files. Without it chaos inevitably results, as papers become disarranged, mixed, and lost very easily. Recovery of a lost paper, or the sorting out of mixed sheets is impossible unless a number is put in a conspicuous place upon each and every sheet. All problems, whether practice problems or real ciphers, can and should bear their individual numbers. If every new sheet used on a particular problem is slugged before any other marks are made on it much trouble will be saved. The best place is the upper left-hand corner, using large size Arabic numerals of the style given in Section 3. Placing a heavy circle around it will help make it conspicuous.

5. ERRORS

Cipher messages pass through at least three different operations:

(1) Encipherment
(2) Transmission
(3) Decipherment

In all of these operations the message passes through many hands; each operator concerned is liable to error; each error causes confusion. Due allowance should be made for errors in the work entered upon. An otherwise good assumption should never be rejected because in a single case an impossible combination results. Furthermore, time is wasted which is spent trying to correct an evident error which will in all probability straighten itself out later, when most of the message has been deciphered. All errors found in cipher text should be indicated in some manner. Thus:

```
X T V C B
T H E R E
    -
```

A. Wrong letter.

If in a given alphabet cipher V = R, and the plain-text letter must be E, then write the correct letter, E, and underline it, or use a colored pencil.

```
    ↓          ↓
   ---        ---
1 2 3 3 5     5 2 3 4 5
P N V I D     M O V C I
T H E W R     I T E R S
```

B. Wrong alphabet.

If in a multiple alphabet problem "shifting" must be resorted to in order to produce the correct letters, indicate same by placing the numbers above the cipher letters showing which alphabet is necessary to produce the correct letter.

6. APPARATUS

The apparatus necessary for expeditious cipher work varies in amount. Such articles as typewriters, dictionaries, and maps are always indispensable. Rapidity in operations will be increased by devices which will eliminate as much hand work as possible. For this purpose wooden strips about 14 inches long, ½ inch wide and ¼ inch thick, upon which paper may be mounted for the purpose of making sliding alphabets, will be found very useful. A rubber stamp containing the letters of the alphabet is also a convenience in the preparation of frequency tables, or, if the stamp is made with movable letters, straight or mixed alphabets may be made at will. A great amount of helpful apparatus is, of course, desirable, the preparation of which is dependent only on the ingenuity and personal inclination of the operator.

7. COOPERATION

It will be found that a single operator working alone is able to accomplish very little. A group of two operators, working harmoniously as a unit, can accomplish more than four operators working singly. Different minds, centered on the same problem, will supplement and check each other; errors will be found quickly; interchange of ideas will bring results rapidly. In short, two minds, "with but a single thought," bring to bear upon a given subject that concentration of effort and facility of treatment which is not possible for one mind alone.

8. WORD-EQUIVALENTS FOR LETTERS

When pronounced individually, the letters of the alphabet are so easily mistaken and confused, that in cipher work it is essential to use arbitrary words in "calling off" letters. The equivalents which have been adopted by the U. S. Army have been found to be very satisfactory and are given herewith:

A—Able
B—Boy
C—Cast
D—Dock
E—Easy
F—Fox
G—George
H—Have
I—Item
J—Jig
K—King
L—Love
M—Mike

N—Nan
O—Opal
P—Pup
Q—Quack
R—Rush
S—Sail
T—Tare
U—Unit
V—Vice
W—Watch
X—X-ray
Y—Yoke
Z—Zed

PRELIMINARY DEFINITIONS

Cryptology is that branch of knowledge which deals with the origin, development, and methods of all forms of secret communication.

Cryptography is that branch of cryptology which deals with the methods of secret writing.

A cipher, taken in a broad sense, is the name applied to any system of cryptography which involves the concealment (in a cryptographic sense) of the individual letters of a message.

The operation of thus concealing the letters of a message is called enciphering. The operation of translating or finding the secret meaning of such a message, whether done by means of the key or not, is called deciphering.

A code is the name applied to a specialized system of cryptography which involves the use of a book or a document, identical copies of which are in possession of the correspondents. Code books in general are of two kinds: (1) dictionaries, which consist merely of the most important words of a language arranged in alphabetical order, the words being accompanied by numbers usually in sequence; (2) repertoires, which consist not only of words, but also of phrases and sentences arranged in some arbitrary manner, and accompanied by arbitrary designations, either numbers, letters, or words. The latter type of code book is used at present much more frequently than the former.

The operations which apply to this system are called encoding and decoding.

When the code designations of the encoded words of a message are afterwards enciphered, the result is called enciphered code. For example: If the code word for the phrase "By order of the Commander-in-Chief" is POBAL, and if this code word is then enciphered on some system into the form CITAX, the latter word is then enciphered code.

OF THE HISTORY, USES, AND KINDS OF CIPHERS

Ciphers are as old as history—indeed history is full of instances of the conveyance of messages from one person to another by means of signs, symbols, gestures, and various contrivances. One of the stories related by a sixteenth century cryptographer* is of a cipher placed on the tomb of Semiramis, 1200 B. C. The cryptogram was deciphered some 700 years later—the decipherer's pains being rewarded with the salutation, "O, poor, miserable slave of deciphering that thou art; from this time on occupy thyself with more fruitful things than to spend time thus uselessly!"

The first military cipher device known to history was the Scytale, or round-ciphered staff, originated by the Lacedaemonians, and used extensively in Cicero's time. It has been asserted that Cicero himself wrote a treatise on ciphers, but no trace of this is found to exist. Cicero's servant, Tyro, is known to have recorded a number of ciphers which he asserted were used by his master. The generals of ancient times had endless methods of transferring information, such as shaving the head of a slave and writing thereon, then holding the slave until the hair grew, whereupon the messenger departed, to be shaved again when he had reached his destination, for the message to be read. Writing upon the back of the slave with a fluid, such as the juice of certain fruits, which became visible upon application of certain salts, was likewise a common practice. Thus the modern and highly-specialized invisible inks arose from the ancient use of fruit juices for the same purpose.

In the same way the modern straight alphabet ciphers can be traced directly to their forerunner, the cipher used by Julius Caesar: the use of B for A, C for B, D for C, and so forth. Other devices used in past centuries were the famous string cipher, the use of torches, musical notes, and many others too numerous to mention.

By the time printing had been put into use, ciphers had attracted so great a number of devotees, that throughout the sixteenth and seventeenth centuries there was an almost constant stream of books issued dealing with the various branches of cryptology—all under different and very impressive names, such as Steganology, Steganography, Polygraphy, Cryptomenytices, Scotography, and Synthemology or Semaeology. All of the works are interesting and curious, some of them contain valuable information. The first man to write of ciphers, and who is sometimes called "the father of ciphers," was Trithemius, abbot of Spanheim and Wuerzburg, whose book "Chronologica Mystica," a work of great magnitude, was published in 1516. All copies of this were later burned, because of the accusation that the book dealt with witchcraft. The manuscript remained in the monastery, however, and translations and reprints were made from this later. Gabriel de

*Blaise de Vigenère, in *Traicté des Chiffres*. Paris, 1587.

Collanges (Paris, 1561) and Gustavus Selenus (1624) were two writers who drew their material chiefly from Trithemius. Other well known writers on this subject in the sixteenth and seventeenth centuries, were John Baptist Porta (1561), Vigenère (1587), Bishop John Wilkins (1640), Falconer (1685) and innumerable others, all of more or less importance. In fact, in the latter part of the sixteenth century it was considered a necessary part of a man's education to become versed in ciphers.*

Since that time ciphers have increased in value and importance, scope and complexity˙ To those old writers of cipher, whose naiveté is so great a source of interest and even amusement to us today, the modern cipher which often uses scores of complex alphabets in the same message would seem as much like witchcraft as their simpler systems seemed to the people before them. Yet the complex systems of today are but a development of the older, simpler methods. Indeed, it may be said that almost every system of cipher known today can be traced to its forerunner of three centuries or longer ago.

At the present time ciphers and codes are used in almost every form of correspondence, both private and governmental. Commercial codes are as common as business itself. Newspaper correspondence is at times done in cipher. Criminals write and speak in cipher and code. Authorities have never been able to break up the "underground" means of communication in prisons by which "breaks" have been planned, and the "latest gossip" spread, without a spoken word.

Governmental ciphers may be spoken of as including diplomatic and military ciphers. Diplomatic ciphers are in use mostly by a few of the smaller nations. Although usually of good construction, on account of the carelessness of clerks whose almost total ignorance of ciphers in general makes consequent errors in judgment, these ciphers are often unsafe. To quote Bacon: "But in regards to the rawness and unskilfulness of the hands through which they pass, the greatest matters are many times carried in the weakest ciphers." The same is still true today.

Most of the large governments use enciphered code for diplomatic and naval communication, but inasmuch as it is the generally agreed upon assumption on the part of diplomatic and military officers that a new code book or a new cipher system is in possession of the enemy or of foreign governments at the moment of, or very soon after its inception, enciphered code becomes cipher only, so far as the decipherer is concerned.

The importance and value of military ciphers cannot be overestimated. Interception of such messages is no longer dependent upon the capture of messengers only. The use of radio, telegraph, buzzer, telephone, semaphore, heliograph, and klaxon systems of communication in the field all offer much greater opportunities for the interception of messages. All large governments must have a corps of decipherers to handle intercepted messages.

*For a complete bibliography of works on cipher see Part II of Riverbank Publication No. 18, "Synoptic Tables for the Analysis of Ciphers." (In press.)

THE REQUIREMENTS OF A MILITARY CIPHER FOR FIELD USE

The requirements of a military cipher for field use have been laid down by Kerckhoffs,* but they are only such as a knowledge of deciphering would give.

1. *The system should be materially, if not mathematically, indecipherable.* Edgar Allan Poe has said: "Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve." This may or may not be true, but it is certainly true that no one has yet invented a mathematically indecipherable system which is practical. Hence, for our purposes we may consider no system in use today as indecipherable. The most that can be expected of a cipher adapted to field use is that it shall offer to the interceptor sufficient obstacles in the way of decipherment to enable the orders or directions contained therein to be executed. The highest degree of perfection as regards this requirement would be a cipher system, the details of the operation and the alphabets of which would be known to the enemy, but without the key a single message or even a series of messages would be absolutely indecipherable to the enemy for all time. Of course it is impossible to attain such a degree of perfection; so that we must modify this requirement by assuming the enemy to be in possession of everything pertaining to the cipher system, including the alphabets, but that a single message or even a series of messages should resist his efforts towards solution for a sufficient length of time to enable the orders or directions contained therein to be executed.

2. *It should cause no inconvenience if the apparatus and methods fall into the hands of the enemy.* A perfect cipher system would be one which would require nothing but pencil and paper. Apparatus is always subject to capture or derangement. Many cipher machines have been devised. But machines operate upon mechanical principles; it must be assumed, therefore, that if the enemy obtains possession of one of the machines he can find out the details of its operation. Furthermore, a seemingly complicated machine cipher may often be solved by the use of sliding strips of paper, even without a knowledge of the alphabets employed. But since it must be assumed that the enemy is in possession of the machine or the alphabets, since the systems employing machines possess no advantages, so far as secrecy is concerned, over systems not requiring them, and since they entail serious disadvantages, the use of machines is rather infrequent. The statement that many cipher machines have been invented, but very few are in use, quite covers this phase. Their only real advantage is that they usually are made in connection with a typewriter keyboard, so that speed in enciphering and deciphering is possible.

3. *The key should be such that it could be communicated and remembered without the necessity of written notes and should be changeable at the will of the correspondents.* These two requirements are of considerable importance. The capture of men with keys upon their persons, or the capture of positions housing the communication quarters is dangerous.

*Kerckhoffs, A. *La Cryptographie Militaire*, Paris, 1883. Quoted by Hitt, *Manual for the Solution of Military Ciphers*, 1916.

Frequent change of key is about the most important safeguard to any field system; hence this should be made easy.

4. *The system should be applicable to telegraphic correspondence.* This is obvious today, where nearly all communication takes the form of Morse signals.

5. *The apparatus should be easily carried and a single person should be able to operate it.* This is certainly a requisite in the case of a field cipher.

6. *Finally, in view of the circumstances under which it must be used, the system should be an easy one to operate, demanding neither mental strain nor knowledge of a long series of rules.* This requirement is of the utmost importance. "It should be so simple that the thickest 'leftenant' in the army can use it," a British officer has said. The more simple, the less chance of errors in enciphering and deciphering.

Hitt says: "A brief consideration of these six conditions must lead to the conclusion that there is no perfect military cipher." Some of these requirements must be sacrificed in order to meet the most important ones.

In connection with the innumerable attempts on the part of the average person to devise new ciphers, it might be said, "There is nothing new under the sun." The information concerning ciphers that is possessed by the average layman is so meager that it has led an eminent cryptographer to say that a school boy might unknowingly invent a cipher which would resist the efforts of an expert for months, whereas only the actual solution of a cipher devised by a most capable business or professional man would convince the inventor that the claims of indecipherability for his system were unfounded. Edgar Allan Poe's experience in this country is of interest in this connection. (See Poe's Works, Vol. II, p. 490-505.)

Since we are dealing now with military ciphers only, we come at this point to the *kinds* of ciphers.

Ciphers in general may be divided into two great classes: (1) SUBSTITUTION and (2) TRANSPOSITION.

(1) Any message in which one or more letters, numerals, signs, or combinations of these three have been substituted in accordance with a definite system, usually some "key," for the original letters of the plain-text, constitutes a substitution cipher.

(2) Any message, the letters, words, or sentences of the original text of which have been rearranged according to some definite system, constitutes a transposition cipher.

In addition to these two main classes there is the Playfair cipher, which is a variety of substitution cipher, to be discussed later, and the combination of substitution and transposition ciphers, in which the original text is transformed first into a substitution cipher, after which the latter is transformed into a transposition cipher, or vice versa.

After the student has secured a thorough grasp upon the principles underlying the solution of the simpler varieties of substitution ciphers and has thus come to an understanding of the mechanics of a written language, he will be in a better position to comprehend the principles upon which the solution of transposition ciphers are based. We will therefore proceed at once to the methods of solving substitution ciphers.

OF THE FREQUENCY OF LETTERS AND ITS BEARING ON SUBSTITUTION CIPHERS

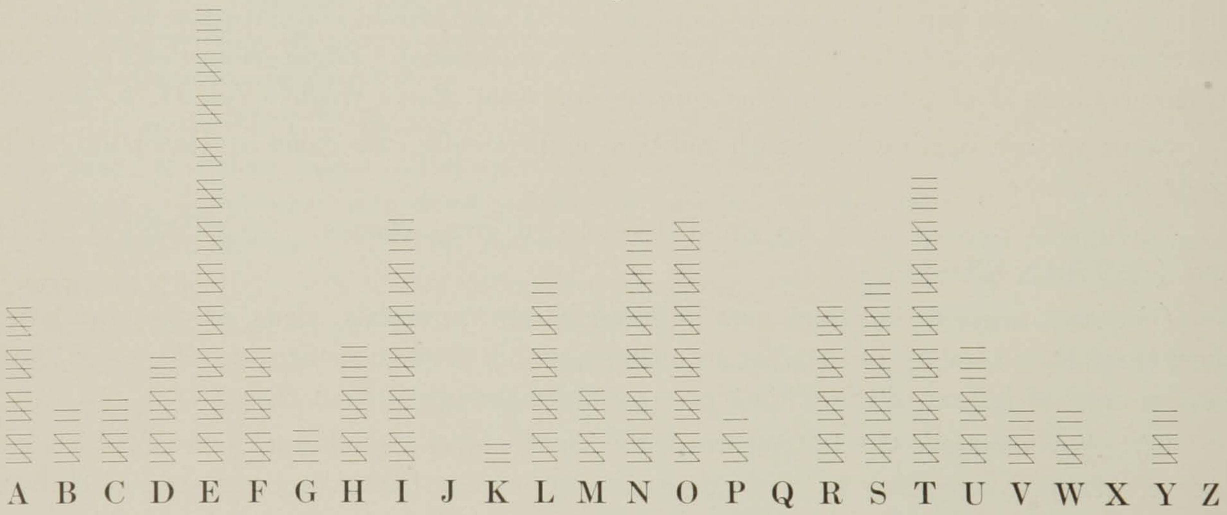
The following message is an ordinary passage of English text such as may be found in any periodical, newspaper, or book:

MESSAGE

"Men would be unlikely to render themselves liable to the penalties of the law if they knew that wherever they might flee their identity could not fail to be discovered. A sure means of identification would not only have the effect of deterring from crime in general but would evidently nullify all attempts of whatever kind at a substitution of persons. No impersonations of a pensioner, or a missing heir, or a business man could ever hope to be successful."

If the letters composing the words of this message (or of any message of similar nature and length) are distributed into what is known as a GRAPHIC FREQUENCY TABLE, shown in Fig. 1, which is nothing else than a short and systematic way of making a count of all the different letters in this message, it will be found that:

Fig. 1.



(1) The letters all vary greatly in the frequency of their use, some being used many more times than others. This results in the production of a series of "crests and troughs," the spatial relations and linear dimensions (frequencies) of which are definitely fixed. By their spatial relations is meant their positions with reference to each other only, i. e., the number of intervals separating any one crest or trough from another.

(2) Opposite the letter A, there is a crest, or a point of high frequency.

(3) Passing over three intervals after A, there is another crest, representing the letter E, which is the point of highest frequency and determines the highest crest in the table.

(4) Passing over two intervals after E, there are two smaller crests, adjacent to each other, representing the letters H and I.

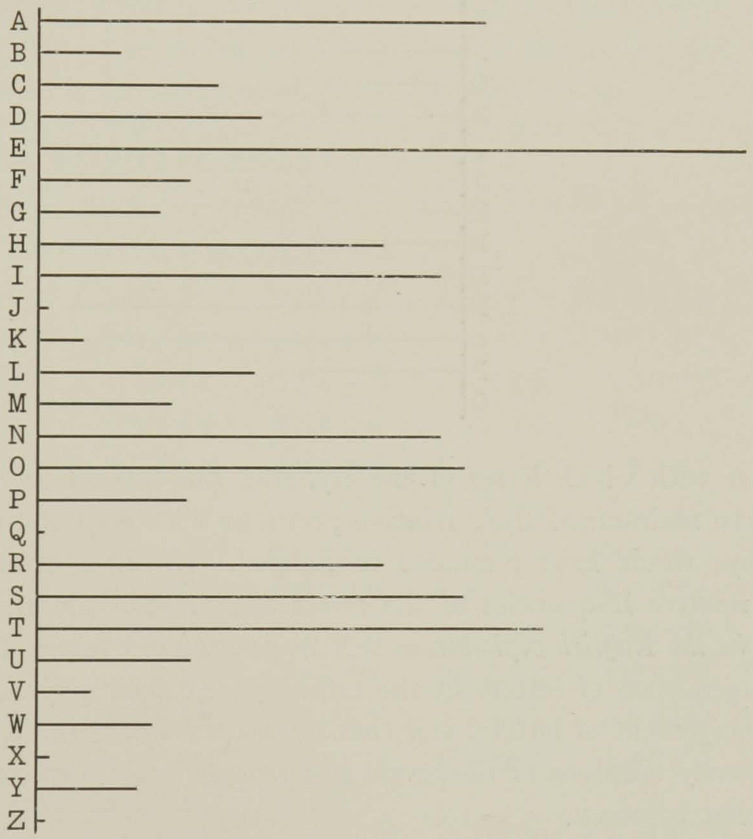
(5) Passing over four intervals after I, there are two more crests, adjacent to each other, representing N and O.

(6) Passing over two intervals after O, there is a sequence of three crests, representing R, S, and T.

(7) The order of frequency of the letters composing this piece of text is as follows: E, T, O, I, N, (S, L), (A, R), F, (H, U), D, M, C, (B, V, W, Y), P, G, K.

Now these characteristics approximate to a fair degree the characteristic or cardinal features of a normal frequency table* made from a total of 25,000 letters, which is shown in Fig. 2. The order of frequency of the letters composing this table is as follows: E, T, A, O, N, I, S, H, R, D, L, C, U, F, M, P, W, G, Y, B, V, K, X, Q, J, Z. The greater the number of letters in any particular portion of text, the more closely will the frequency table applying to it approximate the normal.

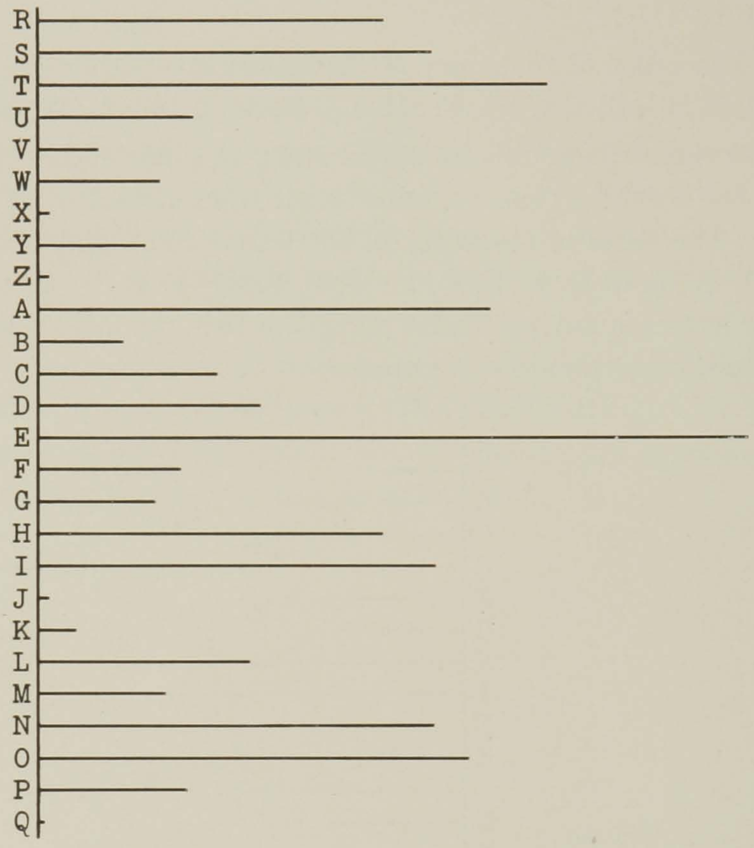
Fig. 2.



Now the relative positions and the frequency of the crests and troughs of the table shown in Fig. 2 would have been absolutely unchanged had the tabulation begun with, say R, instead of A, as the chart in Fig. 3 shows. Compare this chart with that in Fig. 2, noting the relative positions and length of the lines.

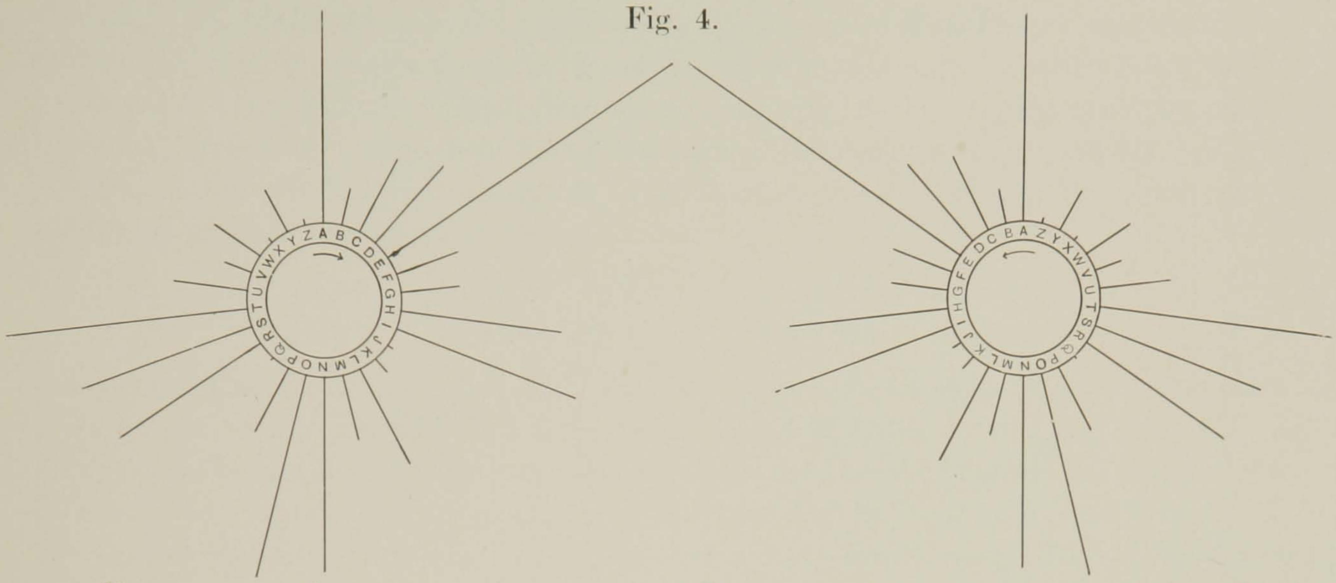
*See page 41.

Fig. 3.



No matter with which letter of the alphabet the tabulation had been begun, these lines would have maintained their relative positions with respect to each other and the length of each line would have remained unchanged. In other words, the spatial arrangements and the relative frequencies of the crests and troughs are the results of certain *internal relations in the English alphabet*, as will be pointed out later. It should be clear, therefore, that the sequence of letters in the ordinary alphabet may be regarded as a continuous, cyclic arrangement of letters, and that no matter where the tabulation begins, the spatial and frequency relations of the crests and troughs remain unchanged. Fig. 4 gives a clear idea of what is meant.

Fig. 4.



Now suppose the message given on page 14 is written by means of an alphabet which has been shifted, say nine spaces forward; that is, for the letter A, the letter J, which is the ninth from A, is written; instead of B, the letter K, which is the ninth letter from B, is written, etc., in accordance with the diagram of alphabets shown below:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
         ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Here is the message in a form which now constitutes a substitution cipher of the simplest kind:

MESSAGE*

```
VNWFX  DUMKN  DWURT  NUHCX  ANWMN  ACQNV
BNUEN  BURJK  UNCXC  QNYNW  JUCRN  BXOCQ
NUJFR  OCQNH  TWNFC  QJCFQ  NANEN  ACQNH
VRPQC  OUNNC  QNRAR  MNWCR  CHLXD  UMWXC
OJRUC  XKNMR  BLXEN  ANMJB  DANVN  JWBXO
RMNWC  RORLJ  CRXWF  XDUMW  XCXWU  HQJEN
CQNNO  ONLCX  OMNCN  AARWP  OAXVL  ARVNR
WPNWN  AJUKD  CFXDU  MNERM  NWCUH  WDUUR
OHJUU  JCCNV  YCBXO  FQJCN  ENATR  WMJCJ
BDKBC  RCDCR  XWXOY  NABXW  BWXRV  YNABX
WJCRX  WBXOJ  YNWBR  XWNAX  AJVRB  BRWPQ
NRAXA  JKDBR  WNBBV  JWLXD  UMNEN  AQXYN
CXKNB  DLLNB  BODU
```

If a graphic frequency table of this cipher message is now made, it will be found that crests and troughs are still present, and moreover, that their relative positions and frequencies have not been changed in the slightest particular, as comparison with Fig. 1 shows.

*Cipher messages are usually sent in groups containing a definite number of letters or figures (usually five or ten) to each group, in order (1) to prevent the would-be decipherer from securing clues from the indications of word lengths which would be furnished if the message were not divided up in this manner; (2) to reduce to a minimum the errors in telegraphic transmission; and (3) to secure the highest degree of economy in transmission.

Fig. 5.

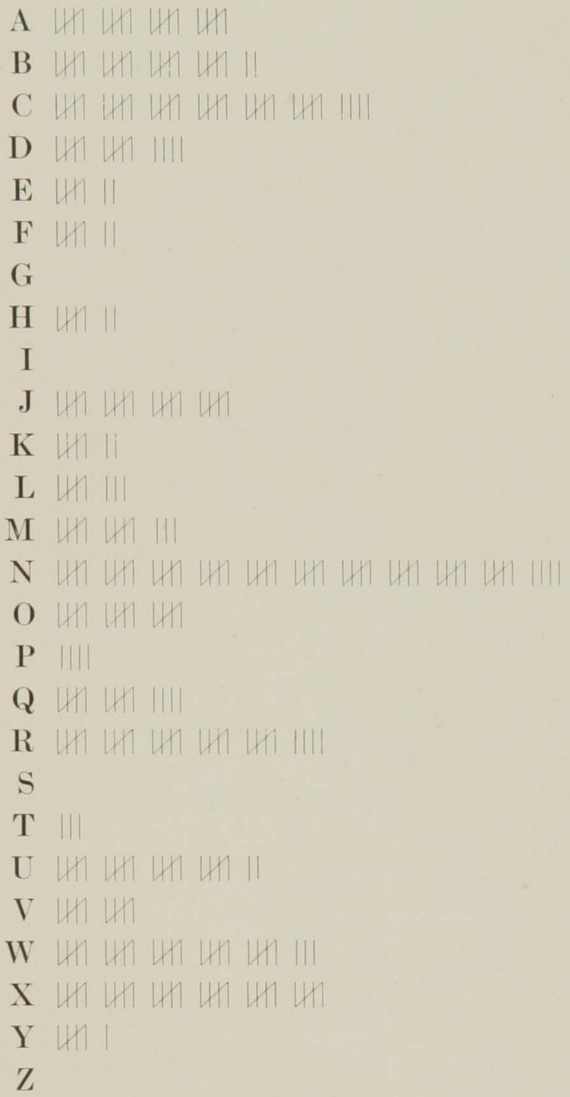
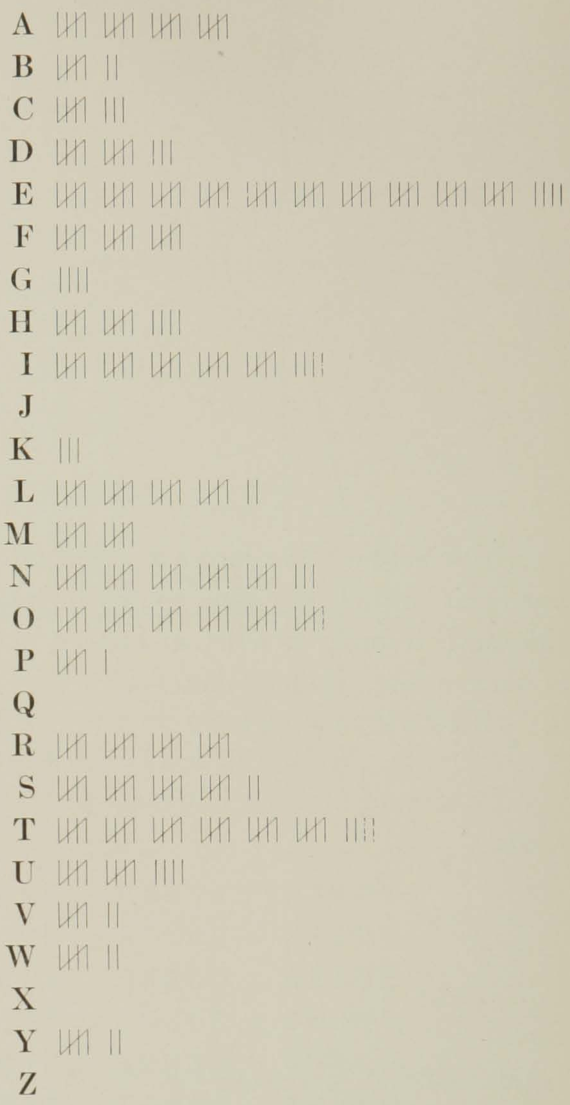


Fig. 1.



For example, the frequency of E in Fig. 1 was 54; at an interval of three spaces before E there is another crest representing A, the frequency of which is 20; on the other side of E, after an interval of two spaces, comes a sequence of two crests, H and I, with frequencies of 14 and 29 respectively. Compare these with their homologous crests and troughs in Fig. 5. The letter N marks the highest crest in the table. Its frequency is 54. Skipping four spaces before N there is another crest, with a frequency of 20; on the other side of N, skipping two intervals comes a sequence of two crests with frequencies of 14 and 29 respectively. In short, the spatial relations of the crests and the troughs in Fig. 5 seem to be exactly the same as those of the frequency table in Fig. 1 which applied to ordinary plain text. This would indicate, without a knowledge of how the enciphering was done, that cipher letter J represents plain-text letter A, K represents B, etc.; in other words, the cipher alphabet begins with J as A, and all the remaining letters follow as in the ordinary alphabet. If, therefore, opposite cipher letter J, the assumed plain-text equivalent A is written, followed by the remaining letters of the alphabet, not only does the whole sequence of assumed plain-text equivalents fit the requirements of the graphic table as regards frequency and spatial relations as found in a normal frequency table for English, but what is more important, if these values are substituted in the cipher text, the words of the plain text immediately appear. Thus:

```
VNWFX   DUMKN   DWURT   NUHCX   ANWMN   A
MENWO   ULDBE   UNLIK   ELYTO   RENDE   R
```

It becomes clear, therefore, that the fact that in this example, the cipher letter N represented plain-text letter E, cipher letter J represented plain-text letter A, etc., had absolutely no effect upon the spatial and frequency relations of the crests and troughs in the graphic table. If A had been represented, for example, by R, B by S, C by T, D by U and E by V, etc., the spatial and frequency relations of the crests and troughs would have been exactly the same. The letter V in this case would have marked the highest crest in the table because it would have represented the plain-text letter E. This leads to the conclusion that the characteristic of being the most frequently used letter in the English language belongs to the letter E, not because of any special quality or peculiarity inherent in the letter E itself, but because *it is the symbol which has been adopted by convention to represent the most frequently used sound in the English language;* any other symbol which will convey the same idea, namely, sound "ee," will serve just as well. This applies not only to the letter E but also to all the other letters in the language.

To explain: If we had been taught that the sounds represented by the symbols E, I and P were, instead, represented by the symbols +, * and 8, respectively, the word PIE would be written 8 * + and the latter would be perfectly intelligible to us. Or, if the sounds represented by our letters A, B, C, D, etc., were taught to us to be represented instead by the symbols V, K, L, X, etc., we would still read the latter as "ay," "bee," "cee," "dee," etc., and the combination LVK would be pronounced "CAB" and would convey the same idea to us as the latter combination does now; for the combination of sounds indicated by CAB has been established by convention to represent a certain definite object, viz., a vehicle, or a means of transportation. The *spoken* words of a language, therefore, may be regarded as combinations resulting from the juxtaposition of definite sounds, which combinations ages of usage have fixed as the representatives of certain objects or ideas; and the *written* words of a language, therefore, may be regarded as combinations resulting from the juxtaposition of definite symbols, which ages of usage have fixed as the representatives of these definite sounds. For example, the juxtaposition of the symbols PIE "spells" to us—that is, calls to our minds—the sounds "pee," "i" and "ee." This combination of sounds, as the result of our previous experience, conveys to our minds, with various resultant sensations, a very definite object. Now if we should use the symbols immediately following these in the regular sequence of symbols in our alphabet, viz., QJF, the combination of sounds called for is perhaps not as easily pronounced but looks altogether strange, because, as we ordinarily say, there is no such word in the language—meaning that usage has not established that sequence of sounds as representing a thing or an idea in English. The necessity for the alphabet now becomes clear; for it becomes essential to fix definitely the sequence of symbols and the sequence of sounds so that when two individuals desire to communicate, that is, to convey to each other the combinations of sounds necessary for the production of intelligible words, they should understand what sounds are called for by the symbols indicated. It should be clear now why written language is absolutely dependent upon this basic principle—the alphabet—which is seen to be really double in nature, involving two separate but coinciding sequences, one of sounds and the other of symbols.

It would not be difficult to explain why the sequence of sounds in the English alphabet, for example, is as we have it today; why, in other words, sound "ay" is followed by sound "bee," etc. This sequence can be traced back through the various languages from which the English language is derived. But it would be difficult indeed to explain how or why the first real alphabet known, that is, one on a purely phonetic basis, came into existence. It is supposed to be a product of the Semitic race and of the Phoenicians. Its history is perhaps as old as language itself. It is also not difficult to explain why the symbol A is now used to represent the sound "ay" in English, because the evolution of the symbols can be traced back to the hieroglyphics of the Egyptians.*

*"The letters in the English alphabet are derived from the corresponding forms in the Latin alphabet, the early forms of which in turn came from the Western Greek alphabet, and the Greek letters from the Phoenician. The origin of the Phoenician letters is not certainly known, though it is not improbable that they were suggested by signs used in Egypt. Although some of the Egyptian hieroglyphics had come to be used as letters, yet Egyptian writing was not strictly alphabetic. The use of an alphabet on a strictly phonetic basis is due to the Semitic race, and probably to the Phoenicians."—Webster's New International Dictionary.

THE KINDS OF ALPHABETS

The student is prepared now to understand the exact meaning of the definitions which follow:

1. An alphabet may be defined as a definitely fixed sequence of symbols representing a definitely fixed sequence of sounds.

2. The normal alphabet for any language is the ordinary alphabet in which the conventional sequence of the sounds used in the language is represented by the conventional sequence of the symbols used in that language; i. e., the two sequences which have been established after generations of use as normal or conventional, coincide. For example, in English the sounds "ay," "bee," "cee," "dee," etc., are represented by the symbols A, B, C, D, etc. To show that these sequences are conventional and arbitrary, it is only necessary to point out that languages vary as regards the order of the alphabet. For example, the Arabic alphabet proceeds thus: ا, alif; ب, ba; ت, ta; ث, tha; ج, jim, or a, b, t, th, j, etc. Any sequence of letters which is written by means of a normal alphabet, and which results in the formation of a word or a series of words in that language constitutes what is known as plain-text.

The meaning of the expression used on page 16 in connection with the cardinal features of a frequency table of English normal or plain text, "internal relations in the English alphabet," should now be clear. The reasons why crests and troughs appear at all in the frequency tables are two: (1) certain sounds are used much more frequently than other sounds, and (2) each sound is always represented by one and only one symbol. The reason why the crests and troughs have definite spatial relations is that the intervals separating the component parts of an alphabet are definitely fixed; i. e., A comes first, E comes fifth, H comes eighth, etc.

3. A cipher alphabet is one in which either the sequence of sounds or the sequence of symbols or both sequences have been altered from the normal, or in which the normal coincidence of the sequences has been altered. Any sequence of letters which has been written by means of a cipher alphabet, and which represents a word or a series of words, constitutes what is known as cipher text.

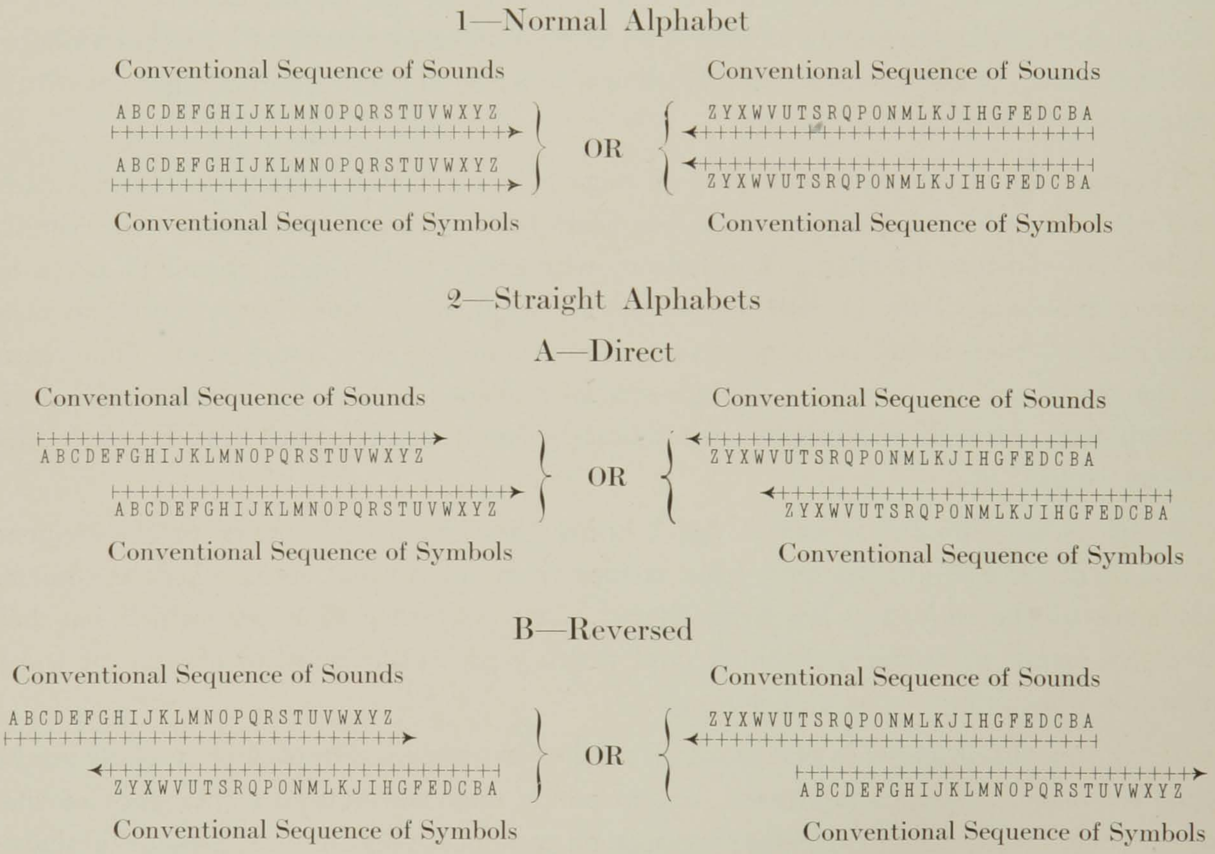
4. A straight alphabet is one in which neither the normal sequence of symbols nor the normal sequence of sounds is altered, but in which only the normal coincidence of these two sequences is changed. The cipher message on page 17 is an example. Straight alphabets may be of two kinds, direct or reversed:

(a) In a direct alphabet the entire normal sequence of symbols, proceeding say from left to right may be shifted one, two, three. . . .to twenty-five spaces to the right of the normal starting point of the entire normal sequence of sounds, proceeding likewise from left to right. In other words, when both sequences are normal and only the normal equivalence of the sequence is changed, a direct alphabet results. The cipher message on page 25 is an example of a direct alphabet cipher.

(b) In a reversed alphabet the entire normal sequence of symbols proceeding say from left to right is applied to the normal sequence of sounds proceeding from right to left; in other words, the normal sequence of symbols is applied to the reversed sequence of sounds, or vice versa, the reversed sequence of symbols is applied to the normal sequence of sounds. In both cases the results are the same.

The meaning of these definitions may be clearly illustrated in the accompanying Fig. 6. In each case the sequences are shown as going in two directions because it is immaterial whether the alphabet is written from left to right or vice versa. Some languages are written from right to left, as for example, Persian.

Fig. 6.


1—Normal Alphabet
Conventional Sequence of Sounds
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Conventional Sequence of Symbols
OR
Conventional Sequence of Sounds
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJIHGFEDCBA
Conventional Sequence of Symbols
2—Straight Alphabets
A—Direct
Conventional Sequence of Sounds
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Conventional Sequence of Symbols
OR
Conventional Sequence of Sounds
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJIHGFEDCBA
Conventional Sequence of Symbols
B—Reversed
Conventional Sequence of Sounds
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA
Conventional Sequence of Symbols
OR
Conventional Sequence of Sounds
ZYXWVUTSRQPONMLKJIHGFEDCBA
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Conventional Sequence of Symbols

5. As regards the manner in which alphabets are mixed, they may be of three kinds:

(a) Key-word mixed alphabets, in which the sequence of letters is commenced by a key-word which is followed by the rest of the unused letters of the alphabet. Such a key-word should be long, and should break up the normal sequence as much as possible. Example: key-word Washington;

Plain-text—A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher—W A S H I N G T O B C D E F J K L M P Q R U V X Y Z

(b) Arbitrarily mixed alphabets, in which the sequence of letters is mixed according to some system previously agreed upon by the correspondents. Such a system, for example, may consist in the writing of the letters of a key-word mixed alphabet in a rectangle, the number of columns of which is determined by the number of different letters in the key-word, numbering the columns in accordance with the numerical sequence determined by that key-word and then writing out the alphabet by taking the columns in their numerical order. Thus:

```
Key-word—W A S H I N G T O N
         9 1 7 3 4 5 2 8 6
         W A S H I N G T O
         B C D E F J K L M
         P Q R U V X Y Z
```

Plain-text—A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher—A C Q G K Y H E U I F V N J X O M S D R T L Z W B P

(c) Random mixed alphabets, in which the sequence of symbols is determined by absolutely random assignments or by drawing out of a hat.

The chief advantage of the first two types of alphabets over the third type is that the former two may be communicated without the necessity of writing out the entire sequence, and can be reproduced from memory, whereas the latter one must be communicated by written notes and thus is dangerous. The chief disadvantage of the first two types is that given a few values, the entire alphabet may be reconstructed because of the clues furnished by the sequences which are usually unbroken, such as BCD, FGH, JKL, XYZ. In the case of the random mixed alphabet, the determination of a few letters gives no clue to the other because the sequence is absolutely hap-hazard and based upon no system whatever.

However, since the number of ways in which an arbitrarily mixed alphabet may be produced from a key-word are legion, as far as safety is concerned, one produced in this way is probably second in safety as compared with one produced by absolutely random assignments, or by drawing out of a hat.

6. As regards the internal nature of mixed alphabets, they may be of two kinds:

(a) Reciprocal alphabets, wherein if, for example, cipher letter X represents plain-text letter A, then cipher letter A represents plain-text letter X. Such an alphabet may be produced arbitrarily by random reciprocal assignments, or by sliding any alphabet against its reverse, in which case a series of twenty-six reciprocal alphabets is produced.

(b) Non-reciprocal alphabets, wherein the reciprocal relation does not hold true except as a matter of chance.

7. As regards their use, alphabets may be of two kinds:

(a) When a cipher alphabet is arranged for the sending of a message, it is called an enciphering alphabet. Example:

Plain text—A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher text—P K T X A C N O V Z B D E G H F I J L Q M S U W R Y

(b) When such an alphabet is arranged for the receiving or translating of a cipher message, it is called a deciphering alphabet. For the example given above the deciphering alphabet would be thus:

Cipher text—A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Plain text—E K F L M P N O Q R B S U G H A T Y V C W I X D Z J

SOLUTION OF STRAIGHT ALPHABET CIPHERS

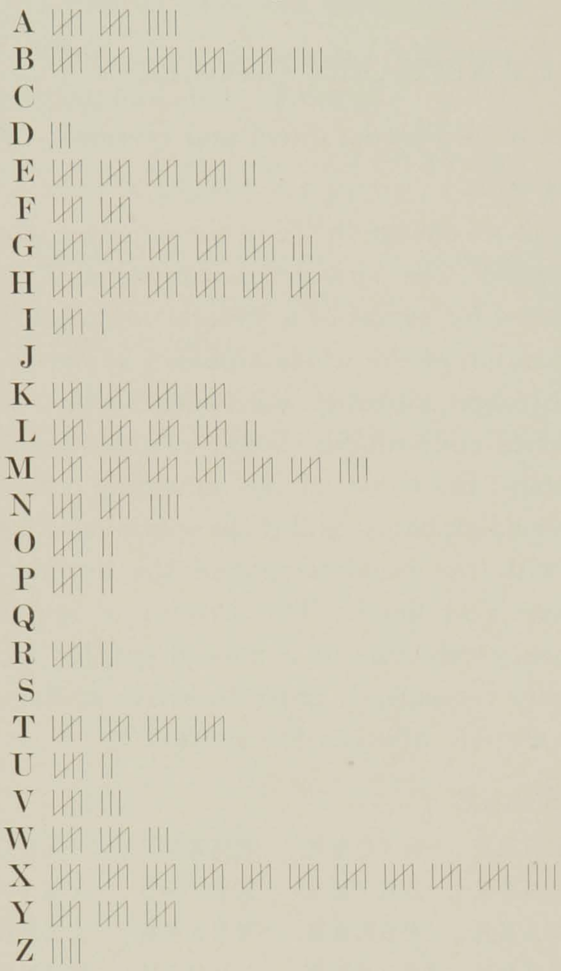
Straight alphabets, it has been said, are of two kinds: direct and reversed. We shall first treat of direct alphabets.

(a) Single alphabet. Since there has been no change in either the sequence of symbols or the sequence of sounds in the cipher alphabet, the correct determination of the value of a single cipher letter in a message enciphered by means of a straight alphabet, whether direct or reversed, will result in the determination of the whole alphabet at once. Consequently, if a graphic frequency table of a straight alphabet substitution cipher is made, the spatial and frequency relations of the crests and troughs should at once disclose what letter represents E. Proceeding from this point, the values of the remaining cipher letters are assigned on the basis of a direct or a reversed alphabet, and if the spatial and frequency relations of the values thus found agree with the requirements of the normal graphic frequency table, the solution of the message is at hand. This process of applying the principles concerning the spatial and frequency relations of a normal graphic frequency table to a graphic frequency table of a cipher message, in order to arrive at the solution of the cipher, is spoken of as "fitting the graphic table to the normal."

MESSAGE

```
FXGPH   NEWUX   NGEBD   XERMH   KXGWX   KMAXF   LXEOX
LEBTU   EXMHM   AXIXG   TEMBX   LHYMA   XETPB   YMAXR
DGXPM   ATMPA   XKXOX   KMAXR   FBZAM   YEXXM   AXBKB
WXGMB   MRVHN   EWGHM   YTBEM   HUXWB   LVHOX   KXWTL
NKXFX   TGLHY   BWXGM   BYBVT   MBHGP   HNEWG   HMHGE
RATOX   MAXXY   YXVMH   YWXMX   KKBGZ   YKHFV   KBFXB
GZXGX   KTEUN   MPHNE   WXOBW   XGMER   GNEEB   YRTEE
TMMXF   IMLHY   PATMX   OXKDB   GWTMT   LNULM   BMNMB
HGHYI   XKLHG   LGHBF   IXKLH   GTMBH   GLHYT   IXGLB
HGXKH   KTFBL   LBGZA   XBKHK   TUNLB   GXLLF   TGVHN
EWXOX   KAHIX   MHUXL   NVVXL   LYNE
```

Fig. 7.



In the accompanying frequency table (Fig. 7) the letter X, which marks the highest crest in the table, is selected as the equivalent of plain-text letter E; wherefore, on the assumption of a direct alphabet sequence, cipher letter T equals A, cipher letter U equals B, cipher letter V equals C, etc. The "fit" is excellent, the correct plain-text values are immediately assigned and substitution results in the solution of the message. The first two lines are as follows:

```
FXGPH   NEWUX   NGEBD   XERMH   KXGWX   KMAXF   LXEOX
MENWO   ULDBE   UNLIK   ELYTO   RENDE   RTHEM   SELVE

LEBTU   EXMHM   AXIXG   TEMBX   LHYMA   XETPB   YMAXR
SLIAB   LETOT   HEPEN   ALTIE   SOFTH   ELAWI   FTHEY
```

This method of deciphering is called "Solution by Frequency Table." There is, however, another method of deciphering such a message which does not necessitate the compilation of a frequency table.

After all, a straight alphabet cipher is only the result of shifting the sequence of symbols a certain number of spaces away from its normal coincidence with the sequence of sounds. If we could find, by means of two direct sequences, one representing symbols, the other sounds, the relative positions these two sequences were in, when the enciphering was being done, the solution of the cipher would be at hand immediately. The question then resolves itself into a search for these positions. We may therefore experiment with two direct sequences, starting with the setting of A on the sequence of symbols to equal B, on the sequence of sounds. We then apply the entire sequence of equivalents thus secured to the first two groups of our message. Thus:

```
Sequence of Sounds (=Plain text)—ABCDEFGHIJKLMNOPQRSTUVWXYZA
Sequence of Symbols (=Cipher)—    ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Cipher letters—FXGPH NEWUX
Sounds indicated—GYHQI OFXVY

This series of letters does not "spell" any plain text, so that evidently the two sequences were not in the position indicated. We therefore move the sequence of symbols one more space to the right, and try again. Thus:

```
Sequence of Sounds—ABCDEFGHIJKLMNOPQRSTUVWXYZAB
Sequence of Symbols— ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Cipher letters—FXGPH NEWUX
Sounds indicated—HZIRJ PGYWZ

This series of letters also does not "spell" any plain text, so we therefore move the sequence of symbols one, then two, then three, four, five, six, seven spaces to the right until the series of sounds indicated spells out plain-text words. Thus:

```
Sequence of Sounds—ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFG
Sequence of Symbols—      ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

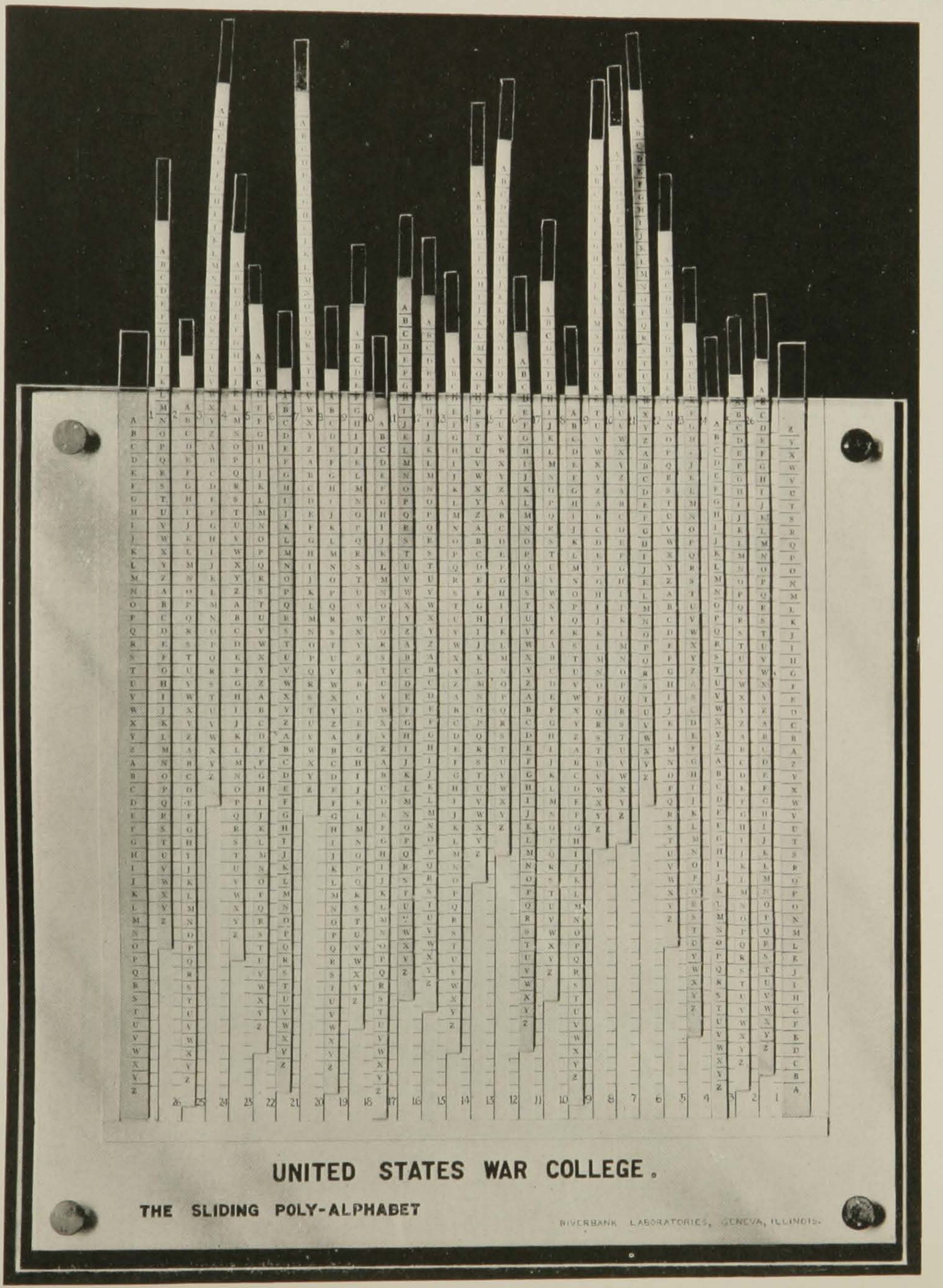
Cipher letters—FXGPH NEWUX
Sounds indicated—MENWO ULDBE

We have thus discovered by successive experiments the positions of the two sequences in encipherment. Now let us analyze these experiments to see if a definite procedure would shorten the labor.

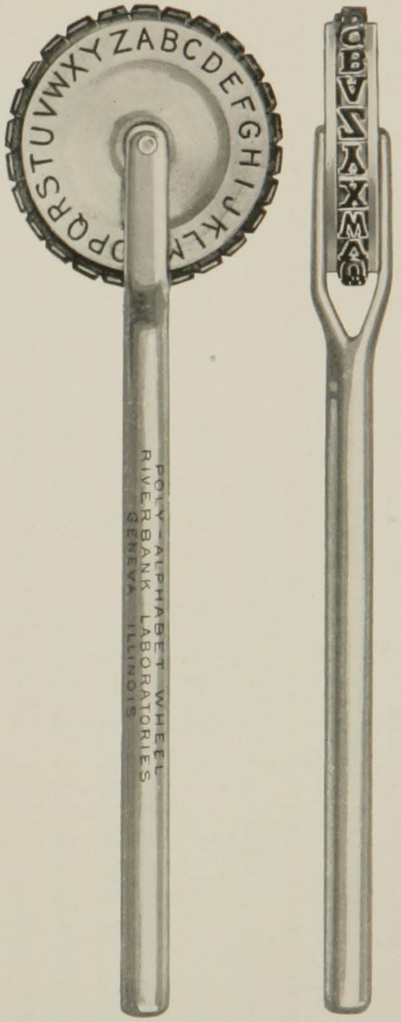
Cipher letters—	FXGPH	NEWUX
A = B—Results of 1st experiment—	GYHQI	OFXVY
A = C—Results of 2d experiment—	HZIRJ	PGYWZ
A = D—Results of 3d experiment—	IAJSK	QHZXA
A = E—Results of 4th experiment—	JBKTL	RIAYB
A = F—Results of 5th experiment—	KCLUM	SJBZC
A = G—Results of 6th experiment—	LDMVN	TKCAD
A = H—Results of 7th experiment—	MENWO	ULDBE

Note now that the net result of these seven separate experiments was simply the continuance of the direct alphabet begun by each cipher letter until the juxtaposition of a certain definite series of letters resulted in the spelling out of plain-text words. This certain series of letters was definite because the number of experiments coincided with the number of spaces the sequence of symbols had been shifted from the normal. If

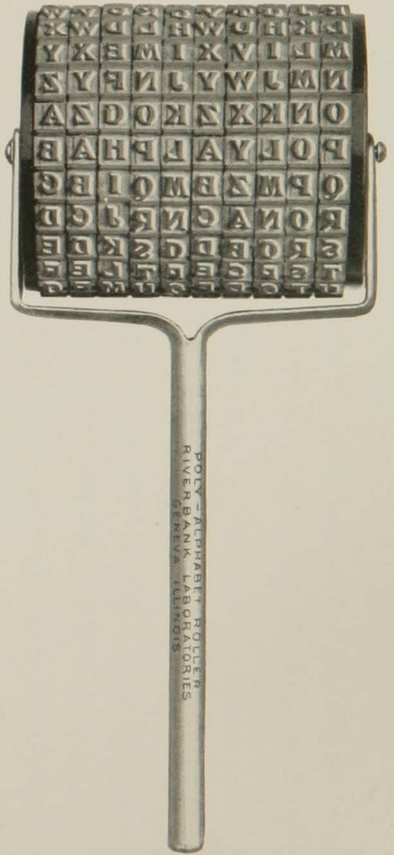
PLATE 1


UNITED STATES WAR COLLEGE.
THE SLIDING POLY-ALPHABET
RIVERBANK LABORATORIES, GENEVA, ILLINOIS.

A


ZABCDEFGHIJKLMNOPQRSTUVWXY
POLY-ALPHABET WHEEL
RIVERBANK LABORATORIES
GENEVA ILLINOIS

B


POLY-ALPHABET ROLLER
RIVERBANK LABORATORIES
GENEVA ILLINOIS

C

we take merely the two groups of cipher letters and continue beneath each letter the direct alphabet started by each letter, all the plain-text equivalents would appear on one horizontal line, which could then easily be selected from all the other horizontal lines because it is the only one which results in the formation of intelligible words. This process of continuing the direct alphabet sequence beneath a group of cipher letters is called "running down." Since each column considered separately consists of only the direct alphabet, it is clear that this "running down" process might be accomplished automatically by the use of the devices shown in Plate 1. The Sliding Poly-Alphabet, A, consists of a series of twenty-six direct alphabets printed upon cardboard strips which are mounted upon celluloid; the strips are all movable, running either in grooves or on tracks, the two pieces of plate glass provided with set-screws at the corners holding the strips firmly, yet loosely enough so that they easily slide up and down. There is in addition a direct alphabet at the extreme left, and a reversed at the extreme right. The sliding strips bear upon their reverse sides other alphabets, i. e., reversed, French or Spanish, etc. Now when a line of cipher text is "set" at the top, that is, when the sliding strips are moved so that a given number (up to twenty-six) of cipher-text letters are brought into one horizontal line, the successive horizontal lines of equivalents, called *generatrices*, are indicated automatically, and thus a vast amount of writing is eliminated. In an alphabet containing twenty-six letters, there are twenty-five generatrices, the twenty-sixth generatrix becoming identical with the letters at the starting point. The second device, the Poly-Alphabet Wheel, B, the idea for which the Riverbank Laboratories is indebted to Lieutenant P. H. Burdick, produces the same results. It makes use of a revolving rubber stamp containing the letters of the direct alphabet equally spaced on the perimeter of the wheel. In order to "run down" a series of cipher letters it is only necessary to start each column with the cipher letter which is to be "run down." The letters all being equidistant from each other, the successive letters all appear upon horizontal lines, or in other words, the successive generatrices are printed. This method possesses some advantageous features which the other does not, the most important being, first, that the apparatus is much smaller and can be carried about easily; secondly, that once a group of cipher letters is "run down," the results are permanently indicated and may be referred to or re-examined at any future time; and thirdly, since the letters are all movable, they may be arranged in accordance with any mixed alphabet sequence.

The third device, the Poly-Alphabet Roller, C, makes use of a series of ten endless rubber belts containing the letters of the direct alphabet equally spaced. These belts fit snugly upon the drum, but may be moved with reference to each other so as to contain ten cipher letters in one line. The device is then inked and rolled upon a sheet of paper.

The various generatrices produced by any of these Poly-Alphabet devices are examined to see whether the letters of one such generatrix spell out any plain-text. If a sequence of plain-text words is found, then the solution of the cipher is attained. The key-letter is sought, that is, the cipher-equivalent or value of plain-text letter A is sought, and this determines the entire cipher alphabet, in a single direct alphabet substitution cipher. The key-letter may be found either by the use of two sliding direct alphabets, setting them so that plain-text M equals cipher F, and then noting what plain-text A equals; or by setting a reversed alphabet against the series of columns produced in the "running down" process so that A of the reversed alphabet is opposite the group of cipher letters which has been "run down." The key-letter will be found on the reversed alphabet directly opposite the plain-text equivalents of the group of cipher letters. This method of deciphering is called "Solution by Running Down" or "Solution by Means of a Poly-Alphabet." An actual example will make this clear. If these two groups of cipher letters are "set" at the top of the Poly-Alphabet, the following generatrices are produced:

0.	FXGPH	NEWUX	0.
1.	GYHQI	OFXYV	25.
2.	HZIRJ	PGYWZ	24.
3.	IAJSK	QHZXA	23.
4.	JBKTL	RIAYB	22.
5.	KCLUM	SJBZC	21.
6.	LDMVN	TKCAD	20.
7.	MENWO	ULDBE	19.
8.	NFOXP	VMECF	18.
9.	OGPYQ	WNFDG	17.
10.	PHQZR	XOGEH	16.
11.	QIRAS	YPHFI	15.
12.	RJSBT	ZQIGJ	14.
13.	SKTCU	ARJHK	13.
14.	TLUDV	BSKIL	12.
15.	UMVEW	CTLJM	11.
16.	VNWFX	DUMKN	10.
17.	WOXGY	EVNLO	9.
18.	XPYHZ	FWOMP	8.
19.	YQZIA	GXPNQ	7.
20.	ZRAJB	HYQOR	6.
21.	ASBKC	IZRPS	5.
22.	BTCLD	JASQT	4.
23.	CUDME	KBTRU	3.
24.	DVENF	LCUSV	2.
25.	EWFOG	MDVTW	1.
0.	FXGPH	NEWUX	0.

The decipherer has simply to examine the successive generatrices to find where the plain text appears. Such an examination takes but a few minutes, and this process should be applied to almost every new problem at the very outset—it may solve the problem, or may furnish valuable clues to the solution. Now note that the plain-text words in these two groups might have been secured by "running up" as well as by "running down," because of the continuous or cyclic nature of the alphabet. "Running up" may be regarded as reversing the process applied in enciphering, in order to get back to the line where the plain text is located; "running down" may be regarded as continuing the process applied in enciphering until one completes the cycle and thus arrives at the line where the plain text is located. This is simply stated for the purpose of pointing out the cyclic nature of the alphabet. By "running down" one must pass over an interval of seven letters in this case; by "running up" one must pass over an interval of nineteen letters. The sum of these two intervals is twenty-six, the total number of letters in the alphabet. In the case of any message, enciphered by means of a direct alphabet, the sum of the intervals necessary to pass over in the "running down" and the "running up" processes is twenty-six. The number of intervals in the "running down" process in any direct alphabet cipher is determined by the number of intervals the alphabets have been shifted in enciphering—or, in other words, by the key-letter. If successive words of a message were enciphered by different key-letters, or in other words, if a series of alphabets were used, it is apparent that the successive words would reappear on different generatrices. This leads to the consideration of the solution of the case where a series of direct alphabets is used.

(b) Series of Direct Alphabets.

In the example above, once the key-letter has been determined upon by the encipherer, he proceeds to encipher the whole message by means of that particular single direct alphabet. Now suppose the correspondents determine to use a key-word, and to encipher the successive words in the message by means of the different key-letters in the word. Thus, suppose the key-word BOSTON has been agreed upon; the first word of the message is enciphered by means of the direct alphabet in which sound A is represented by symbol B; the second word, by means of the direct alphabet in which sound A is represented by symbol O; the third word, by means of the direct alphabet in which sound A is represented by symbol S, etc., until six words have been enciphered. The seventh word then begins a repetition of the cycle. Thus not only might a key-word of many letters be used, but also a key-phrase might be used, at the will of the correspondents, or perhaps the running text of a book might be used. With the key-word SPRING, the message "Repeat the last order. Errors make it impossible to read," would be enciphered thus:

S	P	R	I	N	G	S	P	R	I
REPEAT	THE	LAST	ORDER	ERRORS	MAKE	IT	IMPOSSIBLE	TO	READ
JWHWSL	IWT	CRJK	WZLMZ	REEBEF	SGQK	AL	XBEDHHXQAT	KF	ZMIL

The message would then be sent in groups of five cipher letters as usual.

Now notice that cipher letter W represents E in the first word, H in the second, and O in the fourth. Cipher letter J represents R in the first word and S in the third. In fact, any given cipher letter may represent many different plain-text letters, depending upon the number of different key-letters used, and it follows that the frequency, on the basis of a single alphabet, of any given cipher letter in such a message would give no indication whatsoever as to the letter or letters for which it stands, as will be explained below.

The crest and trough appearance of a graphic frequency table of normal text, or of a cipher message involving the use of only one direct alphabet, is due not only to the fact that there is a wide variation in the frequency with which the different sounds of the language are used, but also to the fact that in such a piece of text, or in such a message a single letter represents one and only one sound, or in other words that a given symbol always represents the same sound. But since in the case under discussion one cipher letter may represent a multiplicity of sounds (plain-text letters), and since the individual frequencies of the sounds represented varies greatly, it follows that the frequency table as a whole will not present the crest and trough appearance, but will appear "solid." It would be impossible to pick out the representative of E, or any other letter. However, if the "running down" process is applied to the cipher letters, the plain-text words will reappear on different generatrices, as stated above. This is because the alphabets used to encipher the successive words have been shifted a varying number of spaces in accordance with the different key-letters, and hence, when the "running down" process is applied, the number of intervals which must be passed over differs in the case of each word, and therefore the plain-text words must come out on different lines. The example above will serve as an illustration.

```
J W H W S L I W T C R J K W Z L M Z R E E B E F S G Q K A L X B E D H H X Q A T K F Z M I L

K X I X T M J X U D S K L X A M N A S F F C F G T H R L B M Y C F E I I Y R B U L G A N J M

L Y J Y U N K Y V E T L M Y B N O B T G G D G H U I S M C N Z D G F J J Z S C V M H B O K N

M Z K Z V O L Z W F U M N Z C O P C U H H E H I V J T N D O A E H G K K A T D W N I C P L O

N A L A W P M A X G V N O A D P Q D V I I F I J W K U O E P B F I H L L B U E X O J D Q M P

O B M B X Q N B Y H W O P B E Q R E W J J G J K X L V P F Q C G J I M M C V F Y P K E R N Q

P C N C Y R O C Z I X P Q C F R S F X K K H K L Y M W Q G R D H K J N N D W G Z Q L F S O R

Q D O D Z S P D A J Y Q R D G S T G Y L L I L M Z N X R H S E I L K O O E X H A R M G T P S

R E P E A T Q E B K Z R S E H T U H Z M M J M N A O Y S I T F J M L P P F Y I B S N H U Q T
-----------                                             ---
  A=S                                                   A=S
            R F C L A S T F I U V I A N N K N O B P Z T     G K N M Q Q G Z J C T O I V R U
                  -------                                                       ---
                   A=R                                                          A=R
            S G D         G J V W J B O O L O P C Q A U     H L O N R R H A K D     J W S V

            T H E         H K W X K C P P M P Q D R B V     I M P O S S I B L E     K X T W
            -----                                       -------------------
             A=P                                                | A=P
                          I L X Y L D Q Q N Q R E S C W                             L Y U X

                          J M Y Z M E R R O R S F T D X                             M Z V Y
                                    -----------
                                        A=N
                          K N Z A N             G U E Y                             N A W Z

                          L O A B O             H V F Z                             O B X A

                          M P B C P             I W G A                             P C Y B

                          N Q C D Q             J X H B                             Q D Z C

                          O R D E R             K Y I C                             R E A D
                          ---------                                                 -------
                             A=I                                                     A=I
                                                L Z J D

                                                M A K E
                                                -------
                                                  A=G
```

The key-letters are sought, as each word is deciphered, by the same methods as explained above. Simply setting two direct alphabets so that, for example, in the case of the first word, plain-text R was represented by cipher J, in which instance A was represented by cipher S. In the same way, P equals A in the second word, R equals A in the third, I equals A in the fourth, N equals A in the fifth, and G equals A in the sixth. Then the cycle repeats itself, until the whole message has been deciphered. In this case each word was enciphered by a different alphabet. This system may be varied by enciphering every group of five, ten or more letters by the various key-letters instead of each word, but the solution is attained by the same procedure, except that a little more study is necessary in order to pick out the entire words.

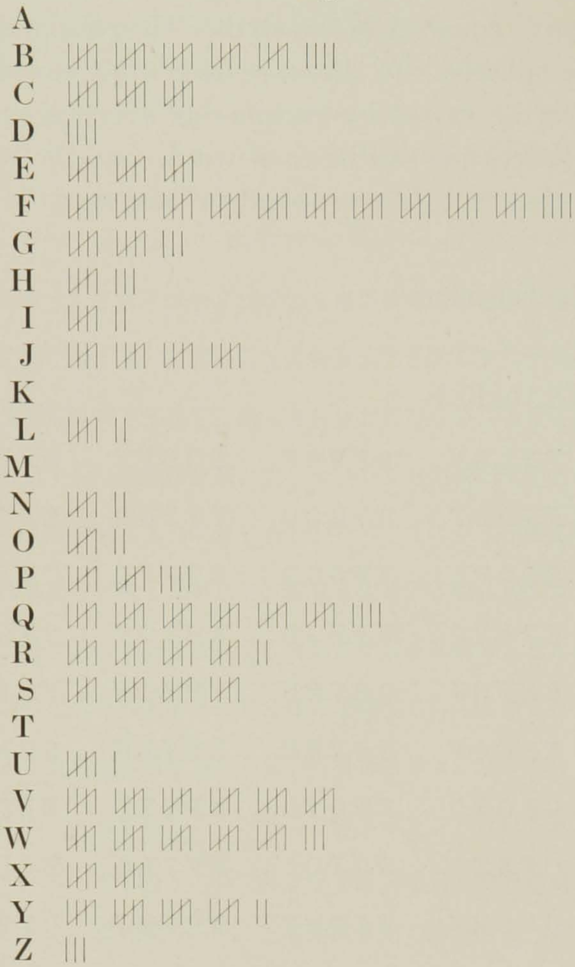
Reversed alphabet ciphers will now be considered.

(a) Single Alphabet.

EXAMPLE

```
XFWNV   PYGIF   PWYBZ   FYLQV   SFWGF   SQCFX   RFYOF
RYBJI   YFQVQ   CFUFW   JYQBF   RVEQC   FYJNB   EQCFL
ZWFNQ   CJQNC   FSFOF   SQCFL   XBDCQ   EYFFQ   CFBSB
GFWQB   QLHVP   YGWVQ   EJBYQ   VIFGB   RHVOF   SFGJR
PSFXF   JWRVE   BGFWQ   BEBHJ   QBVWN   VPYGW   VQVWY
LCJOF   QCFFE   EFHQV   EGFQF   SSBWD   ESVXH   SBXFB
WDFWF   SJYIP   QNVPY   GFOBG   FWQYL   WPYYB   ELJYY
JQQFX   UQRVE   NCJQF   OFSZB   WGJQJ   RPIRQ   BQPQB
VWVEU   FSRVW   RWVBX   UFSRV   WJQBV   WRVEJ   UFWRB
VWFSV   SJXBR   RBWDC   FBSVS   JIPRB   WFRRX   JWHVP
YGFOF   SCVUF   QVIFR   PHHFR   REPY
```

Fig. 8.



In the accompanying frequency table (Fig. 8), the letter F, which marks the highest crest in the table, is selected as the equivalent of plain-text letter E. Attempts made to "fit" this table to the normal, on the assumption of a direct alphabet, do not give good results, but on the assumption of a reversed alphabet, an excellent "fit" is obtained, the correct plain-text values may be assigned at once and substitution results in the solution of the message. Note that the relative positions of the crests and troughs have remained the same here as in the preceding encipherments of the same message. Only the direction of "reading" the series of crests and troughs has been reversed. The first two lines are as follows:

```
XFWNV   PYGIF   PWYBZ   FYLQV
MENWO   ULDBE   UNLIK   ELYTO

SFWGF   SQCFX   RFYOF   RYBJI
RENDE   RTHEM   SELVE   SLIAB

YFQVQ   CFUFW   JYQBF   RVEQC
LETOT   HEPEN   ALTIE   SOFTH
```

This is a "Solution by Frequency Table." But this message also may be solved by the "running down" process, or by the Poly-Alphabet. Suppose two alphabets, one direct, representing the sequence of sounds, the other reversed, representing the sequence of symbols, are now taken for experiment to try to find the relative positions these two sequences were in when the enciphering was done, just as was done before. Setting A to Z in this position, the two sequences are as shown below:

Sequence of Sounds (=Plain text)—ABCDEFGHIJKLMNOPQRSTUVWXYZ
Sequence of Symbols (=Cipher)—ZYXWVUTSRQPONMLKJIHGFEDCBA

Cipher letters—XFWNV
Sounds indicated—CUDME

This series of letters does not "spell" any plain text, so that evidently the two sequences were not in the position indicated. We therefore move the sequence of symbols one space to the right, and try again. Thus:

Sequence of Sounds—ABCDEFGHIJKLMNOPQRSTUVWXYZA
Sequence of Symbols— ZYXWVUTSRQPONMLKJIHGFEDCBA

Cipher letters—XFWNV
Sounds indicated—DVENF

This series of letters also does not "spell" any plain text, so we therefore move the sequence of symbols one more, then two, three, etc., spaces to the right, each time noting whether the juxtaposition of the plain-text equivalents results in the spelling of a word. At the 11th experiment the results are as follows:

Cipher letters—XFWNV
Sounds indicated—MENWO

Now tabulate the results of these experiments:

	Cipher letters—	XFWNV
A = Z—	Results of 1st experiment—	CUDME
A = A—	Results of 2d experiment—	DVENF
A = B—	Results of 3d experiment—	EWFOG
A = C—	Results of 4th experiment—	FXGPH
A = D—	Results of 5th experiment—	GYHQI
A = E—	Results of 6th experiment—	HZIRJ
A = F—	Results of 7th experiment—	IAJSK
A = G—	Results of 8th experiment—	JBKTL
A = H—	Results of 9th experiment—	KCLUM
A = I—	Results of 10th experiment—	LDMVN
A = J—	Results of 11th experiment—	MENWO

Note now that the net result of the ten separate experiments *after the first experiment* was simply the continuance of the direct alphabet sequence started by the letters given by the very first experiment. In other words, after the first experiment, the process was exactly the same as explained on page 27. In the latter case, the first experiment began with the continuing of the direct alphabet sequence started by the cipher letters themselves; in this case, the first experiment began with the finding of the equivalents of the cipher letters when a reversed alphabet was set against a direct alphabet. In this case, A was set opposite Z; but had A been set opposite any other letter, and the same procedure followed, the final result would have been the same as is shown by the following, where Z is arbitrarily set opposite F:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
          Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
```

```
                    Cipher letters—X F W N V
Equivalents on a reversed alphabet—H Z I R J
                                   I A J S K
                                   J B K T L
                                   K C L U M
                                   L D M V N
                                   M E N W O
```

This process of finding the equivalent is spoken of as "finding the reversed alphabet equivalent," or simply "finding the reversed equivalent." In order to solve such a message by means of the Poly-Alphabet, it is therefore necessary first to convert the cipher letters into their reversed equivalents, and then "set" these equivalents. The words of the message will then reappear on some generatrix below. The student should convince himself that "running down" without first finding the reversed alphabet equivalents for the cipher letters will not result in the production of the plain-text for the reason that in encipherment the two sequences, one of sounds, the other of symbols, were going in opposite directions, and therefore, "running down" by means of direct alphabet sequences could not possibly reproduce the plain-text.

(b) Series of reversed alphabets.

Just as the successive words of a message may be enciphered by means of a series of direct alphabets, according to the letters of a key-word, so they may be enciphered by means of a series of reversed alphabets. The reversed alphabet equivalents of the cipher letters would have to be found first, then when these are "run down" the successive words of the message would appear on different generatrixes.

SOLUTION OF SINGLE MIXED ALPHABET CIPHERS

It has been observed so far that in the case of straight alphabet ciphers the correct determination of one value in the message results in the solution of the whole cipher alphabet and the consequent decipherment of the message. The solution could be secured either by means of a frequency table, or by the "running down" process. The solution of mixed alphabet ciphers, however, is secured only by the frequency table method, and that only after considerably more experimentation than is the case with straight alphabet ciphers.

Fig 9.

A	|
B	𝍸 𝍸 ||
C	𝍸
D	𝍸 |
E	𝍸 𝍸 |
F	|
G	
H	||||
I	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 |
J	𝍸 𝍸 𝍸 𝍸 ||
K	𝍸 𝍸 𝍸 𝍸 𝍸 ||||
L	𝍸 |
M	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 ||
N	|||
O	||
P	
Q	𝍸 𝍸
R	𝍸 𝍸
S	𝍸 𝍸 𝍸 ||
T	𝍸 𝍸 𝍸 𝍸 𝍸 ||
U	||||
V	|||
W	|||
X	𝍸 ||
Y	𝍸 𝍸 𝍸 𝍸
Z	||||

MESSAGE

```
IQMIN MKIWU TJBIE THTBT SKNTR RMKIJ
YTKKS IRYIM JIQYK DYJXQ KTKMI MMKIQ
MKJSZ IMISX QYJRM BISKB SZIQX YJSRT
KYCSJ ISUMD VYJOY ITSKM AZTCC MEUSJ
MFIMK BTHMU TMREB MJHTX MJMCS JITKL
ISXSD DYKET KLLMK MJYRI QYIBI YITSK
YKEMD VYJOT KLZKE MJQTB ETJMX ITSKB
IQMMK LTKMM JJMLT DMKIY KEIJY TKNTR
RCJMX MEMET HTBTS KVWYI RMYBI IQJMM
EYWB
```

All attempts to solve this cipher by applying the Poly-Alphabet having failed, a graphic frequency table is made, and appears as shown in Fig. 9. *The fact that this frequency table shows marked crests and troughs and has proved not to be a straight alphabet cipher means that it is almost certainly a single mixed alphabet cipher.* The solution of such a cipher will be facilitated by the compilation of a special kind of table called a Frequency Table with Prefixes and Suffixes.

There are two kinds of frequency tables, as regards their form only.

(1) THE GRAPHIC FREQUENCY TABLE, which is to show only how many times any letter in a message occurs. It is made simply by placing a stroke opposite the tabulated list of the letters of the alphabet. The fifth occurrence of a letter is made by a diagonal stroke. This will add up the occurrences automatically, and the table loses none of its graphic features thereby. Examples of such tables are seen on pages 18, 26 and 34.

(2) THE FREQUENCY TABLE WITH PREFIXES AND SUFFIXES, which can be made to show not only how many times any letter occurs, but will also show for each letter what letter precedes it and what letter follows it, each time that letter occurs—information which is necessary for the solution of most ciphers. (See Fig. 10.) The method which has been adopted is this: Write the alphabet in columnar fashion upon a sheet of cross-section paper, devoting one square to each letter. In the message which follows for solution IQMIN is the first group of cipher letters. In the upper half of the first square opposite I in our table a dash is placed to indicate that it has no prefix, being the first letter of the message. In the lower half of the same square the letter Q is written, which is the suffix of I. The next letter to be tabulated is Q. Its prefix, I, is placed in the upper half of the first square opposite letter Q in the table; its suffix M is placed in the lower half of the same square. The next letter to be tabulated is M. Its prefix, Q, is placed in the upper half of the first square opposite M in the table; its suffix, I, is placed in the lower half of the same square. The prefixes and the suffixes of the succeeding occurrences of any letter are placed in corresponding positions in the succeeding squares, until the last letter of the message is tabulated. In the lower half of the square concerned, a dash is placed, indicating that it has no suffix. When all the letters have been tabulated in such a manner, the most important data—namely, the recurring groups and the number of their recurrences—may be obtained quickly, and should be placed in a condensed table onthe same sheet. This condensed table will show the frequencies of the DIGRAPHS, TRIGRAPHS and POLYGRAPHS, which recur in the message.

(1) A digraph is a pair of letters. Just as certain letters are used more frequently than others in any language, so certain pairs of letters are used more frequently than other pairs of letters.

A digram is a two-letter word.

A frequently recurring digram is also a digraph; but a frequently recurring digraph does not necessarily have to be a digram. Examples: TH is a frequently recurring digraph, but not a digram; IN is a frequently recurring digraph and is also a frequently recurring digram.

(2) A trigraph is a group of three letters.

A trigram is a three-letter word. The statements made above concerning digraphs and digrams apply to trigraphs and trigrams.

(3) A polygraph is a group of more than three letters.

A polygram is a word of more than three letters. The distinctions as given above between digraph and digram apply here also.

In order to show how this data is secured, take the frequency of the letter Q in the accompanying table, Fig. 10. The upper halves of all the squares contain prefixes only, the lower halves, suffixes only. The letter I is indicated as a prefix to Q seven times. This

Fig. 10.

Frequency Table with Prefixes and Suffixes

					5					10					15					20					25					30					35		
A	M Z																																				
B	J I	T T	M I	K S	K T	E M	I I	T E	K I	T T	Y I	W I																									
C	Y S	T C	C M	M S	R J																																
D	K Y	M V	S D	D Y	M V	T M																															
E	I T	M U	R B	K T	K M	K M	B T	K I	M M	M T	M Y																										
F	M I																																				
G																																					
H	T T	T M	J T	T T																																	
I	I Q	M N	K W	B E	K J	S R	Y M	J Q	M M	K Q	Z M	M S	B S	Z Q	J S	Y T	F M	J T	L S	R Q	Y B	B Y	Y T	X T	B Q	K Y	E J	J J	Y R	B I	I Q						
J	T B	I Y	M I	Y X	K S	Y R	Y S	S I	Y O	S M	M H	M M	S I	M Y	Y O	M Q	T M	M J	J M	I Y	C M	Q M															
K	M I	S N	M I	T K	K S	Y D	Q T	T M	M I	M J	S B	T Y	S M	M B	T L	Y E	T L	M M	S Y	Y E	T L	Z E	S B	M L	T M	M I	Y E	T N	S V								
L	K I	K L	L M	K Z	K T	M T																															
M	Q I	N K	R K	I J	K I	I M	M K	Q K	I I	R B	U D	K A	C E	J F	I K	H U	T R	B J	X J	J C	L K	K J	E D	E J	J X	Q M	M K	K M	M J	J L	D K	J X	X E	E E	R Y	J M	M E
N	I M	K T	K T																																		
O	J Y	J T																																			
P																																					
Q	I M	I Y	X K	I M	X Y	I X	I Y	J T	I M	I J																											
R	T R	R M	I Y	J M	S T	M E	Y I	T R	R C	I M																											
S	T K	K I	J Z	I X	I K	B Z	J R	C J	I U	T K	U J	C J	I X	X D	T K	T K	T K																				
T	U J	E H	H B	B S	N R	Y K	K K	R K	I S	Z C	B H	U M	H X	I K	E K	I S	O K	Q B	E J	I S	L K	L D	Y K	N R	E H	H B	B S										
U	W T	S M	E S	M T																																	
V	D Y	D Y	K W																																		
W	I U	V Y	Y B																																		
X	J Q	S Q	Q Y	T M	S S	M I	M M																														
Y	J T	R I	Q K	D J	Q J	X J	K C	V J	O I	D K	J R	Q I	I I	K K	V J	I K	J T	W I	M B	E W																	
Z	S I	S I	A T	L K																																	

Condensed Table.

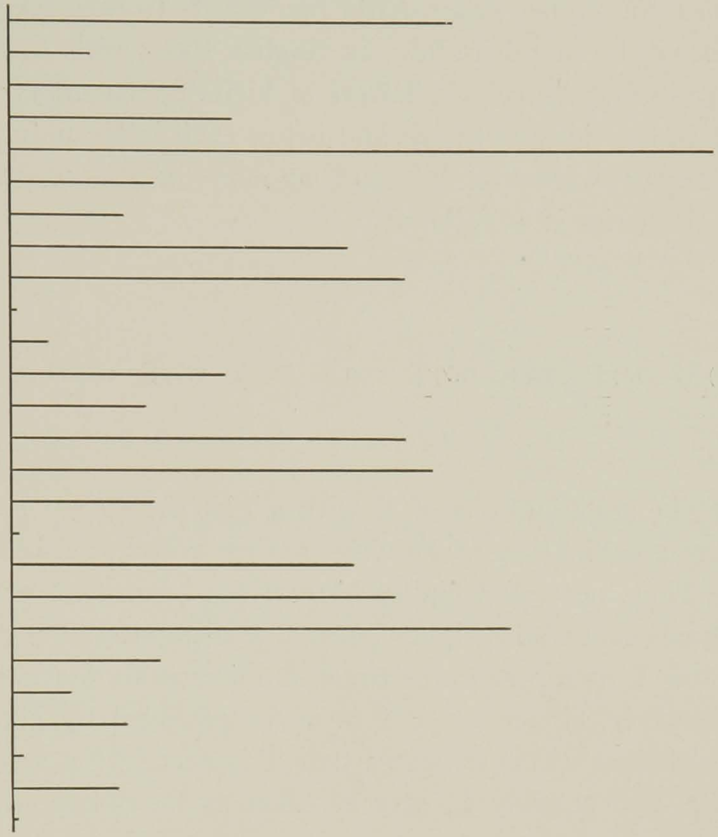
MK-8	TSK-5
TK-8	MKI-4
IQ-7	IQM-3
MJ-6	TKL-3
SK-6	YKE-3
JM-6	
YJ-5	
YI-5	
KM-4	
KL-4	
IS-4	
KI-4	
KE-4	
YK-4	
EM-3	
JI-3	

means the digraph IQ occurs seven times. The letter M is indicated as a suffix to Q three times. This means that the digraph QM occurs three times. Now the letter M is indicated three times as a suffix of Q at the same time I is indicated as a prefix. In other words, the trigraph IQM occurs three times. In a similar manner the trigraph TSK is indicated as occurring five times. Now in order to list all the digraphs it is not necessary to find both the recurring prefixes and suffixes to a letter; either the tabulation of the prefixes, or the suffixes, is all that is necessary. For example, the table shows that opposite the letter Q, the letter I is indicated seven times as a prefix; opposite the letter I, the letter Q is indicated seven times as a suffix. In short, the frequency of the digraph IQ may be secured either from the letter Q, and considering only its prefixes, or from the letter I and considering only its suffixes. As long as the operator is consistent throughout in considering either prefixes only, or suffixes only, the final results will be the same. In the condensed table only recurrences of three or more need be indicated; for the information which may be obtained ordinarily from any less than three recurrences of digraphs or trigraphs is negligible.

Having compiled the data which applies to the particular case in hand, an attempt is to be made to fit the special conditions exhibited by this data to the generalized conditions for ordinary English text as exhibited in a frequency table compiled from a much greater number of letters. If these special conditions happen to approximate or conform closely to the generalized conditions, the normal conditions, in other words, the solution of the cipher will be attained directly. If they do not, considerable experimenting must be done before the solution will be reached. From a frequency table compiled from approximately 25,000 letters taken from various samples of ordinary English text, it has been found that the frequency of individual letters, digraphs and trigraphs is as given in Table I.

TABLE I*.

Frequency Table for English Literary Text



	Order of Frequency.
A-2045	1-E
B- 365	2-T
C- 811	3-A
D-1020	4-O
E-3203	5-N
F- 640	6-I
G- 534	7-S
H-1540	8-H
I-1786	9-R
J- 20	10-D
K- 163	11-L
L- 991	12-C
M- 615	13-U
N-1808	14-F
O-1921	15-M
P- 645	16-P
Q- 28	17-W
R-1530	18-G
S-1746	19-Y
T-2301	20-B
U- 694	21-V
V- 253	22-K
W- 542	23-X
X- 47	24-Q
Y- 474	25-J
Z- 17	26-Z
Total 24639	

Vowels 39.1%: Consonants LNRST, 34.0%: Consonants JKQXZ, 1.1%.

DIGRAPHS

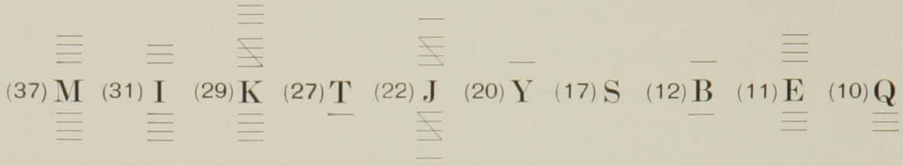
TH-748	ES-370	HA-272	IS-231	HI-209
HE-694	ST-327	AT-265	EA-225	LA-205
IN-465	EN-312	NT-259	IT-223	NE-182
ER-420	ND-305	OF-257	OU-218	AL-181
RE-412	ON-298	OR-238	AR-216	LE-169
AN-403	ED-278	AS-237	NG-215	EC-163

TRIGRAPHS

THE-522	HER- 97	HES- 71	VER- 58	WIT- 50
AND-207	OFT- 77	TIO- 71	ITH- 57	DTH- 50
ING-171	FTH- 76	ETH- 69	TTH- 57	SIN- 48
ERE-116	ATI- 73	HIS- 66	ARE- 56	STH- 48
THA-108	HAT- 73	INT- 65	NTH- 55	TER- 47
ENT- 98	EST- 71	WAS- 59	ALL- 53	REA- 46

*Compiled 1918 at Riverbank Laboratories. The text was composite in character, passages from literary, scientific, military text, etc., being included.

From an inspection of the frequency table applying to this message, shown in Fig. 10, it is seen at once that cipher letter M represents E. Now it is a great advantage to be able to distinguish the cipher equivalents for vowels from those for consonants and the following method will be found useful. In English the vowels E, A, O, and I will usually be found among the first ten cipher letters of highest frequency. Write the ten highest frequency letters in a series and above and below each letter note graphically the number of times the cipher equivalent of E occurs as a prefix and a suffix respectively. Thus, for our message the series is as follows:



Now any of the combinations of E with a high frequency consonant is much more frequent than any combination of E with another vowel. This fact forms the basis of the distinction. Thus, note that cipher letter I has plain-text letter E three times as a prefix and four times as a suffix; cipher letter I is therefore not a vowel. Cipher letter K has plain-text letter E as a prefix nine times and as a suffix five times; it also is therefore not a vowel. However, cipher letter T is never preceded by plain-text letter E and is followed by it only once. This indicates that T is certainly a vowel. On this basis, the letters M, T, Y, S, and possibly B, may be taken to be vowels; while I, K, J, E, and Q, may be taken to be consonants.

Having thus determined the probable vowels and the probable consonants, we return to the frequency table and note what combinations are indicated with several of the high frequency letters. Cipher letter M has already been assumed to be E. Cipher letter I having been assumed to be a consonant, and being the second highest letter in frequency in in the table, it would be logically assumed to be T. The condensed table shows that the trigraph IQM occurs three times, and might well be THE. The frequency table is consulted therefore to corroborate the assumption that Q represents H. It should show that Q is relatively low in frequency, and that it is often preceded by I, the letter which has been assumed to be T, since the digraph TH is among the most frequent in English. These conditions are complied with fully in our table, since Q is seen to occur ten times, seven times of which it is preceded by I; consequently, the assumption made stands corroborated, and these values are filled in throughout the message.

The results are as follows:

```
I Q M I N   M K I W U   T J B I E   T H T B T   S K N T R   R M K I J
T H E T     E   T             T                               E   T

Y T K K S   I R Y I M   J I Q Y K   D Y J X Q   K T K M I   M M K I Q
            T     T E     T H               H         E T   E E   T H

M K J S Z   I M I S X   Q Y J R M   B I S K B   S Z I Q X   Y J S R T
E           T E T       H       E     T             T H

K Y C S J   I S U M D   V Y J O Y   I T S K M   A Z T C C   M E U S J
            T     E                 T       E               E

M F I M K   B T H M U   T M R E B   M J H T X   M J M C S   J I T K L
E   T E           E       E         E           E   E         T

I S X S D   D Y K E T   K L L M K   M J Y R I   Q Y I B I   Y I T S K
T                             E     E       T   H   T   T     T

Y K E M D   V Y J O T   K L Z K E   M J Q T B   E T J M X   I T S K B
      E                             E   H             E     T

I Q M M K   L T K M M   J J M L T   D M K I Y   K E I J Y   T K N T R
T H E E           E E       E         E   T         T

R C J M X   M E M E T   H T B T S   K V W Y I   R M Y B I   I Q J M M
      E     E   E                                 E     T   T H   E E

E Y W B
```

At once it is noted that within the message two sequences of letters look favorable. With the values already assumed they stand as follows:

```
MIMMKIQMKJ ------------- IQYIBIYIT
ETEE-THE--               TH-T-T-T-
```

The first of these suggests at once a word ending in TEEN or TEENTH. Hence K, which was one of the letters indicated as a consonant by the reasoning given on page 42, is assumed to represent N, and the assumption checked by the frequency table. Also Y, which was likewise assumed to be a vowel by the same reasoning, should evidently represent A, and the frequency table is consulted to see whether Y is high enough in frequency to represent A. The frequency table shows Y to be high and accordingly Y is substituted throughout by A as well as K by N. Now the trigraph YKE occurs three times and Y having been assumed to be A, and K to be N, YKE may well be AND. These values are also substituted throughout.

Now the digraphs ER and RE are among the most frequent in English. M has already been assumed to be E, so that it is necessary to search for a letter which, as a suffix with M, might represent ER, and as a prefix with the same letter, might represent RE. In other words, a high frequency reversible combination is sought. Here are the combinations with M which present themselves for study:

MK - 8	JM - 6
MJ - 6	EM - 3
KM - 4	

Of the letters which occur in combination with M, J is the only one to which a value has not already been given and J was indicated previously as being a high consonant. MJ, occurring six times, may well stand for ER; and so likewise JM, six times, for RE. The frequency table is consulted to see if J may represent R, and it is seen to be very good for that letter. Accordingly these values are substituted throughout the message. The results of all these substitutions are shown below:

```
I Q M I N   M K I W U   T J B I E   T H T B T   S K N T R   R M K I J
T H E T     E N T         R   T D                 N           E   T R

                                                _________   _________
Y T K K S   I R Y I M   J I Q Y K   D Y J X Q   K T K M I   M M K I Q
A   N N     T   A T E   R T H A N     A R   H   N   N E T   E E N T H

M K J S Z   I M I S X   Q Y J R M   B I S K B   S Z I Q X   Y J S R T
E N R       T E T       H A R   E     T   N         T H     A R

K Y C S J   I S U M D   V Y J O Y   I T S K M   A Z T C C   M E U S J
N A     R   T     E         R   A   T       N E             E       R

M F I M K   B T H M U   T M R E B   M J H T X   M J M C S   J I T K L
E   T E N         E       E   D     E R         E R E       R T   N

              _______________________________________
I S X S D   D Y K E T   K L L M K   M J Y R I   Q Y I B I   Y I T S K
T             A N D     N     E N   E R A   T   H A T   T   A T     N

Y K E M D   V Y J O T   K L Z K E   M J Q T B   E T J M X   I T S K B
A N D E       A R       N     N D   E R N       D   R E     T     N

I Q M M K   L T K M M   J M M L T   D M K I Y   K E I J Y   T K N T R
T H E E N       N E E   R R E         E N T A   N D T R A     N

R C J M X   M E M E T   H T B T S   K V W Y I   R M Y B I   I Q J M M
    R E     E D E D                 N     A T     E A   T   T H R E E

E Y W B
D A
```

This is about as far as the frequency of single letters, digraphs and trigraphs will carry the decipherer. Further progress must be made by assuming probable words from the skeletons of words shown by the working sheet. Incorrect assumptions soon manifest themselves as such because they will bring into juxtaposition, letters forming impossible combinations. The decipherer therefore should not bind himself rigidly to the rules and requirements of frequency of ordinary text; he should be ready at all times to free himself from any rules or requirements which lead him to no results.

The cipher letters of high frequency which still remain undecided are T and S, which have been indicated as vowels, and of the medium frequency letters, B and R. The representatives of the vowels O and I have yet to be found. The decipherer might experiment with these high frequency letters, trying the former pair out for O and I, and the latter pair for S and L, but another way is to examine the text carefully and try to assume a word. This combination is seen in the last two groups of the second line:

```
KTKMIMMKIQ
N-NETEENTH
```

The letter T, both in position here and in frequency, could well stand for I, giving in this place the word NINETEENTH. When the value of T is substituted throughout the message, the following sequence is noted:

```
YKETKLLMKMJYRIQYI
ANDIN--ENERA-THAT
```

The repeated cipher letter L limits the assumptions for its plain-text equivalent very greatly and the words COMMANDING GENERAL are suggested at once.

A trial of this "guess" results in giving excellent combinations and no impossiblities anywhere. These new values are assigned throughout and the entire message may now be deciphered with ease from the context. This is an illustration of what a good "guess" may lead to, based upon the conditions of the text.

The complete message is as follows: "The Twenty-first Division will entrain not later than March nineteenth enroute to Charleston, South Carolina, port of embarkation, equipped for extensive field service, reporting to commanding general that station and embarking under his directions. The engineer regiment and train will precede Division by at least three days."

In a short message where the ordinary frequency method has failed to lead to solution, because the approximation of the frequency of any letter to the normal frequency table is not close, a method which will often lead to results and which depends upon the assumption of a probable word in the plain-text, is as follows:

Given the cipher groups, IQMIN MKIWU TJBIE THTBT SKNTR, if it is suspected that the message contains a word relative to troop movement, the word DIVISION may be assumed. The requirements of this word are these:

The first letter is medium in frequency.

The second letter is high in frequency and coincides with the fourth and sixth letters.

The third letter is very low in frequency.

The fifth letter is high in frequency.

The seventh letter is high in frequency, as is the eighth, and these should combine in a digraph which is medium in frequency.

One begins, therefore, by attempting to locate this word, looking first for a place where three identical letters are separated by one interval between the first and second, and the second and third appearances. The only possibility is THTBT. When the values derived from this assumption are substituted throughout, the results are as follows:

```
IQMIN   MKIWU   TJBIE   THTBT   SKNTR
         N---   I-S-D   IVISI   ON-I-
```

The combination -I-S-DIVISION suggests FIRST. These assumptions are all substituted throughout, and if no impossible combinations result, are assumed to be correct. Further assumptions are then made, and the process continued as in the preceding method. Such a method as this is to be used only as a last resort, when frequency methods have failed after repeated attempts toward solution.

Cases are encountered in which a single cipher letter stands for two different plain-text letters; but because of the possibilities for error and misinterpretation, such double values usually involve a high frequency letter coupled with one of low frequency, so that the context would determine which of the two is correct. Such cases give no trouble to the decipherer because the high frequency letters, digraphs, and trigraphs are still prominent. The alternate values soon disclose themselves in the process of decipherment and cause no further difficulties.

The method shown here for solving a simple single mixed alphabet cipher is applicable to all cases where only one alphabet is concerned, whether that alphabet involves the use of letters, signs, figures, or combinations of these three symbols. In most of the cases where more than one alphabet is involved, if the cipher can be reduced to single alphabet terms, that is, if the message can be rearranged so that its constituent parts may be examined on the basis of single alphabets, the solution can nearly always be reached with little difficulty.

Synoptic Tables for the Solution of Ciphers

and

A Bibliography of Cipher Literature

Publication No. 18

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Two Hundred copies of this publication were printed of which this is

No. 81

RIVERBANK
LABORATORIES
GENEVA
ILLINOIS

FOREWORD

The tables presented herewith are designed to meet specific pedagogical needs of a course of instruction in modern ciphers. They are not intended, it is frankly admitted, to serve as a guide for the expert in his attempt to analyze complex ciphers such as may be intercepted today.

The method which has been followed in their construction is analogous with that followed in chemical analysis manuals, but only in its broader aspects. The basis for the chemical determination of the nature of an unknown substance consists in the ability to place the unknown successively into one of two alternative classes by means of a series of definite tests until with the last cleavage the solution is reached. It is entirely possible to accomplish this determination with directness and with accuracy in chemical analysis because the laws underlying chemical reactions are definite and unchanging. The tests to be applied are exact, the reagents are all thoroughly understood. It is possible to determine the nature of even the most minute traces of an unknown substance, so refined have the methods of chemical analysis become. Contrast this situation with that which confronts the cipher analyst at the outset of his attempts to solve an unknown. In the first place, except in rare instances in practice, the amount of the unknown is often so limited as to thwart all his attemps at analysis and nothing can be done. In the second place, while it is true that both an unknown chemical substance and a message are composed of definite combinations of discrete units, the former of atoms, the latter of letters, further analogy between them ceases. For while atoms combine in a limited number of ways and positions to form molecules, and the latter combine in a limited number of ways and positions to form more complex substances, letters combine in a limitless number of ways and positions to form words, and words combine in a limitless number of ways and positions to form sentences. True, this difference is only one of degree, not of kind, but whereas the science of chemistry has reached so high a degree of development that each one of the possible combinations may be recognized by at least one test, the science and art of deciphering has not reached such a high level of perfection. In the field of complex ciphers, there is at present no definite means of determining what tests or what methods of solution should be applied because there is no way of determining from external characteristics or even from certain internal signs which one of a great number of complicated and readily modifiable systems of enciphering has been used in the particular message under examination. In fact, in most cases, unless the decipherer is able to secure some information concerning the system used he has no way of knowing what methods to apply until the long and laborious process of elimination has disclosed them.

The analogy between the tables for chemical and for cipher analysis is, therefore, only remote, and it is doubtful whether it can ever be brought closer. But for the purposes for which the tables presented are specifically intended, namely, instruction, it is believed that they will constitute a valuable adjunct to the curriculum of a course in ciphers. It is believed that they will afford the student a means of surveying the most important branches of practical ciphers and to note their similarities and differences. Thus, taken as a whole, they will give a more or less comprehensive bird's-eye view of the entire field of ciphers. If they will thus enable the student to secure a firmer grasp upon the basic principles underlying this branch of knowledge they will have served the purpose for which they were intended.

The Riverbank Publications referred to in the tables are as follows:

No. 15—A Method of Reconstructing the Primary Alphabet given a Single One of the Series of Secondary Alphabets. 1917.

No. 16—Methods for the Solution of Running-Key Ciphers. 1918.

No. 17—An Introduction to Methods for the Solution of Ciphers. 1918.

No. 19—Formulae for the Solution of Geometrical Transposition Ciphers.* 1918.

No. 20—Several Machine Ciphers and Methods for their Solution.* 1918.

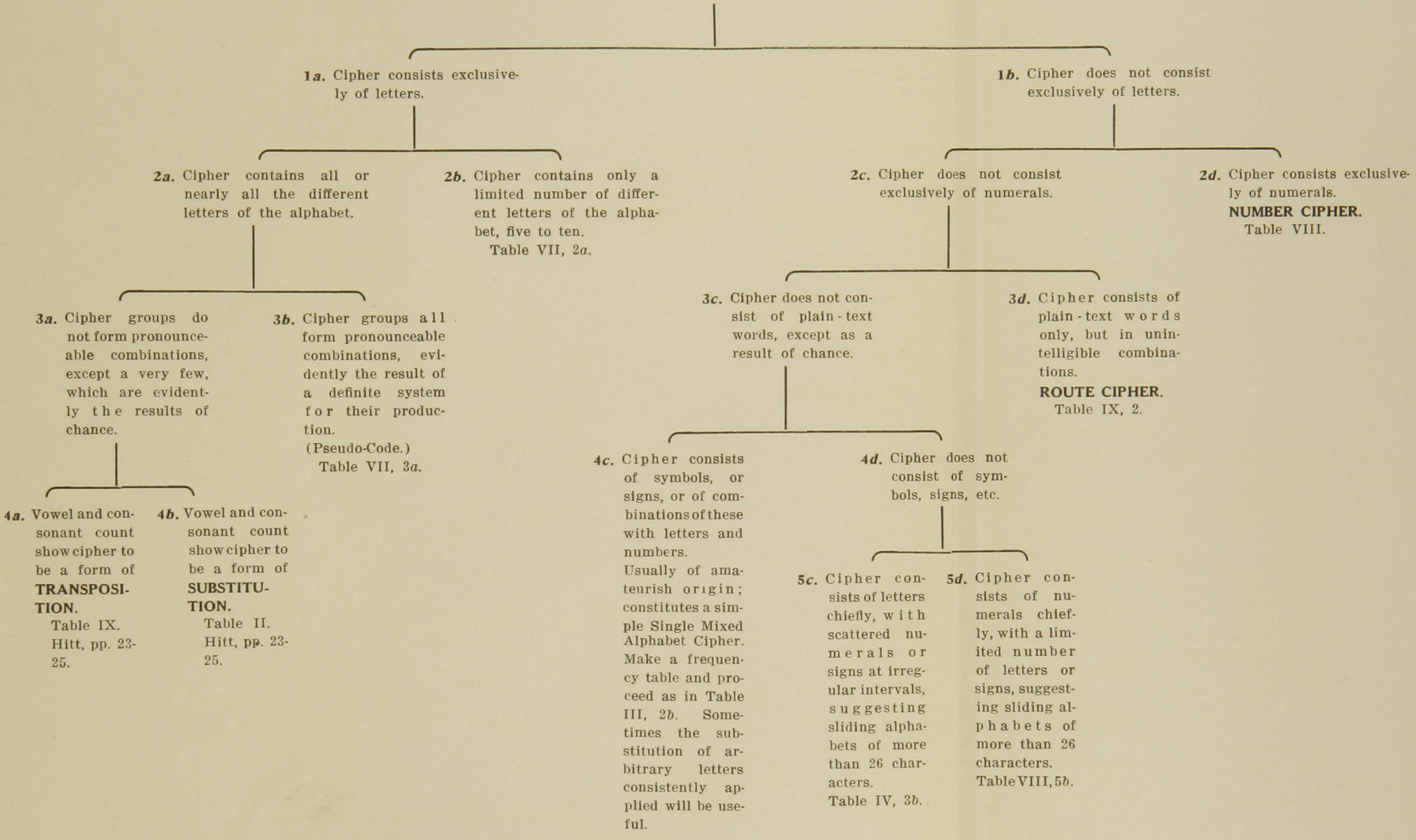
No. 21—Methods for the Reconstruction of Primary Alphabets, Arbitrarily-Mixed Alphabets, Numerical Keys, etc.*

The full titles of works, which in the tables are referred to by only the author's name, will be found in the Bibliography, Part II, pages 14-16.

*Now in press.

TABLE I

Examine the cipher carefully in order to secure from extraneous circumstances such information as may be of value in the subsequent analysis. Certain clues may be found as to language, subject, correspondents, etc.



1a. Cipher consists exclusively of letters.

2a. Cipher contains all or nearly all the different letters of the alphabet.

3a. Cipher groups do not form pronounceable combinations, except a very few, which are evidently the results of chance.

4a. Vowel and consonant count show cipher to be a form of **TRANSPOSITION.** Table IX. Hitt, pp. 23-25.

4b. Vowel and consonant count show cipher to be a form of **SUBSTITUTION.** Table II. Hitt, pp. 23-25.

3b. Cipher groups all form pronounceable combinations, evidently the result of a definite system for their production. (Pseudo-Code.) Table VII, 3*a*.

2b. Cipher contains only a limited number of different letters of the alphabet, five to ten. Table VII, 2*a*.

1b. Cipher does not consist exclusively of letters.

2c. Cipher does not consist exclusively of numerals.

3c. Cipher does not consist of plain-text words, except as a result of chance.

4c. Cipher consists of symbols, or signs, or of combinations of these with letters and numbers. Usually of amateurish origin; constitutes a simple Single Mixed Alphabet Cipher. Make a frequency table and proceed as in Table III, 2*b*. Sometimes the substitution of arbitrary letters consistently applied will be useful.

4d. Cipher does not consist of symbols, signs, etc.

5c. Cipher consists of letters chiefly, with scattered numerals or signs at irregular intervals, suggesting sliding alphabets of more than 26 characters. Table IV, 3*b*.

5d. Cipher consists of numerals chiefly, with a limited number of letters or signs, suggesting sliding alphabets of more than 26 characters. Table VIII, 5*b*.

3d. Cipher consists of plain-text words only, but in unintelligible combinations. **ROUTE CIPHER.** Table IX, 2.

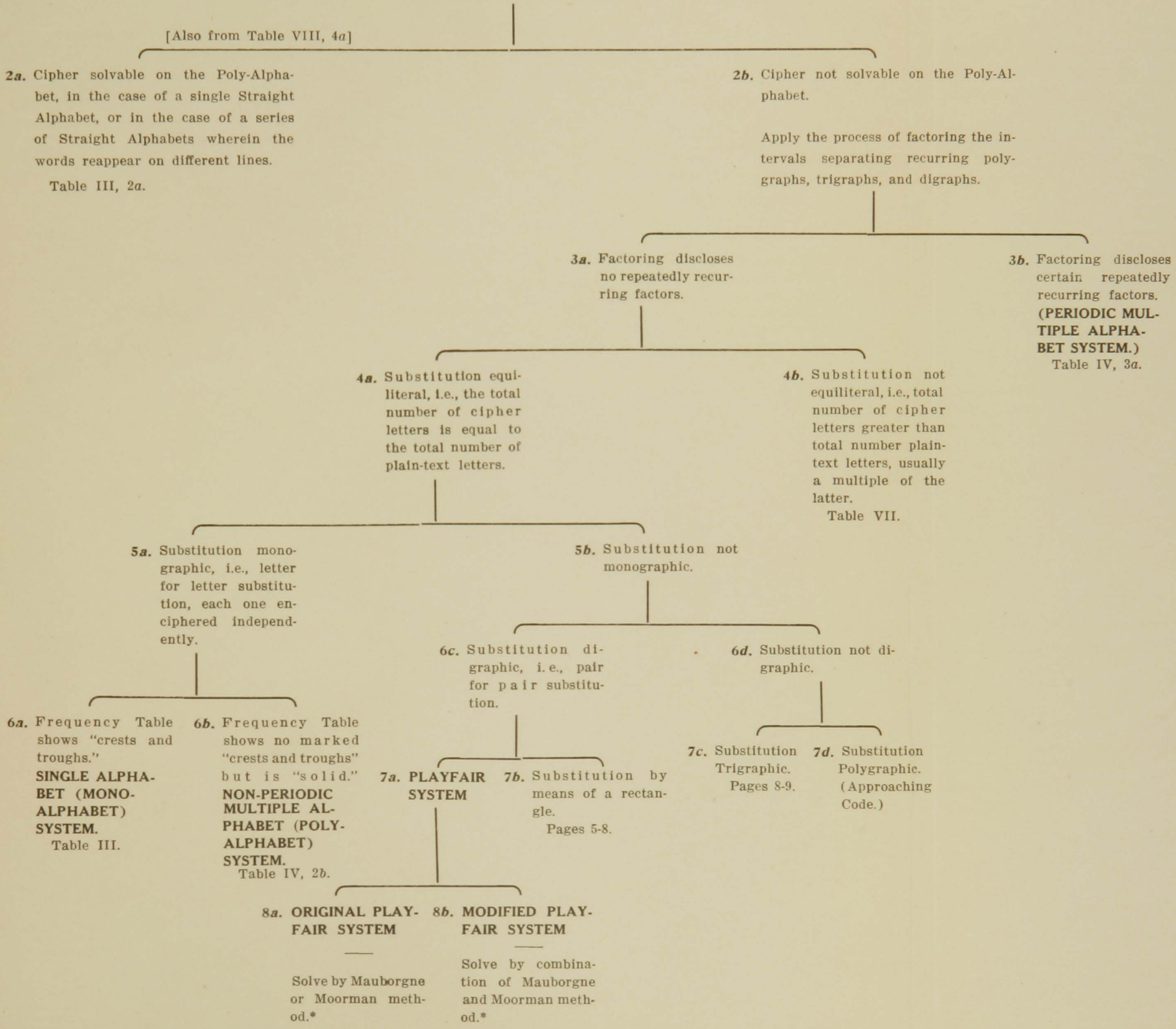
2d. Cipher consists exclusively of numerals. **NUMBER CIPHER.** Table VIII.

TABLE II

[From Table I, 4*b*]

1. SUBSTITUTION CIPHER

Set a few groups on the Poly-Alphabet or apply the "running-down" process.



[Also from Table VIII, 4*a*]

2a. Cipher solvable on the Poly-Alphabet, in the case of a single Straight Alphabet, or in the case of a series of Straight Alphabets wherein the words reappear on different lines.
Table III, 2*a*.

2b. Cipher not solvable on the Poly-Alphabet.

Apply the process of factoring the intervals separating recurring polygraphs, trigraphs, and digraphs.

3a. Factoring discloses no repeatedly recurring factors.

3b. Factoring discloses certain repeatedly recurring factors. **(PERIODIC MULTIPLE ALPHABET SYSTEM.)**
Table IV, 3*a*.

4a. Substitution equiliteral, i.e., the total number of cipher letters is equal to the total number of plain-text letters.

4b. Substitution not equiliteral, i.e., total number of cipher letters greater than total number plain-text letters, usually a multiple of the latter.
Table VII.

5a. Substitution monographic, i.e., letter for letter substitution, each one enciphered independently.

5b. Substitution not monographic.

6a. Frequency Table shows "crests and troughs." **SINGLE ALPHABET (MONO-ALPHABET) SYSTEM.**
Table III.

6b. Frequency Table shows no marked "crests and troughs" but is "solid." **NON-PERIODIC MULTIPLE ALPHABET (POLY-ALPHABET) SYSTEM.**
Table IV, 2*b*.

6c. Substitution digraphic, i. e., pair for pair substitution.

6d. Substitution not digraphic.

7a. **PLAYFAIR SYSTEM**

7b. Substitution by means of a rectangle.
Pages 5-8.

7c. Substitution Trigraphic.
Pages 8-9.

7d. Substitution Polygraphic. (Approaching Code.)

8a. **ORIGINAL PLAYFAIR SYSTEM**

Solve by Mauborgne or Moorman method.*

8b. **MODIFIED PLAYFAIR SYSTEM**

Solve by combination of Mauborgne and Moorman method.*

* See Mauborgne, J. O., *An Advanced Problem in Cryptography and Its Solution.* Leavenworth Press, 1914. Hitt, *Manual for the Solution of Military Ciphers*, 1st edition, pp. 76-83; 2nd edition, pp. 76-82.

TABLE III

[From Table II, *2a* and *6a;* VII, *5a*]

1. SINGLE ALPHABET (MONO-ALPHABET) SYSTEM

(Frequency table shows "crests and troughs")

[Also from Table I, *4c;* VII, *2a;* VIII, *5a;* VIII, *5d*]

2a. STRAIGHT ALPHABET CIPHER

(This should have been solved under Table II, *2a.*)

3a. DIRECT ALPHABET

4a. Solve by the Frequency Table Method, i. e., "fitting the frequency table to the normal" to find **A.** Substitute the plain-text values in sequence.

4b. Solve by means of a Poly-Alphabet or by applying the ''running down'' process.

3b. REVERSED ALPHABET

4c. Solve by the Frequency Table Method, same as in *4a* of this table.

4d. Find the Reversed Alphabet equivalents for three or four groups and proceed as in *4b* of this table. Find the key letter and apply to the entire message.

See Riverbank Publication No. 17, pages 25-36, and Hitt, pages 39-62.

2b. MIXED ALPHABET CIPHER

3c. RECIPROCAL ALPHABET

3d. NON-RECIPROCAL ALPHABET

Make a frequency table with prefixes and suffixes and assume values based upon the frequency of individual letters, digraphs, and trigraphs.

See Riverbank Publication No. 17, pages 37-46, and Hitt, pages 44-50.

In case of a Reciprocal Alphabet, assignment of values is aided by the reciprocal relation. If the deciphering alphabet when completed exhibits signs of its being a Secondary Alphabet, based upon a Primary Alphabet using a key word, reconstruct the Primary Alphabet; or if the deciphering alphabet when completed exhibits signs of its being derived from a generating rectangle, reconstruct the latter. Sometimes these operations, when attempted upon the basis of partially deciphered material, will result in the complete reconstruction of the alphabet and the consequent entire decipherment. See Riverbank Publications Nos. 15, 16, and 21.

TABLE IV

[From Table II, 6b]

1. MULTIPLE ALPHABET SYSTEM

[Also from Table VIII, 4*d*]

2a. The individual alphabets of the entire system are employed at regular and definite intervals, resulting in either a **PERIODIC SYSTEM** or a **PROGRESSIVE SYSTEM.**

[Also from Table II, 3*b*]

3a. The individual alphabets are limited in number in any single message, and are employed at definite intervals, thus forming the constituent cycles of a **PERIODIC SYSTEM.**

4a. Periodicity governed by the successive single letters of the plain text. **(MONOLITERAL PERIODICITY.)** Compile single frequency tables on the basis of the number of alphabets suggested by the most common factor.

Table V.

4b. Periodicity governed by successive groups of letters of the plain text, groups being equal in length. **(POLYLITERAL PERIODICITY.)** Determine the length of the groups and the number of alphabets employed. (See Valerio, pp. 36-42.) Compile single frequency tables upon these bases, then proceed as in 3*a* of this table, except in the application of the plain-text equivalents, substitution must be made on the basis of successive groups of letters governed by the same key letter instead of by the successive single letters.

[Also from Table I, 5c]

3b. The individual alphabets are not limited in number in any single message, all of them being used in straight succession, thus forming the constituent cycles of a **PROGRESSIVE SYSTEM.**

These systems usually employ two concentric disks, or two sliding strips, which are moved regularly 1, 2, 3 . . . spaces after each letter or after a definite number of letters.

4c. **STRAIGHT ALPHABETS**

Solve by means of the Poly-Alphabet (in the case of Reversed Alphabets first find the Reversed Alphabet equivalents before setting), reading diagonally up or down; or setting the successive cipher letters 1, 2, 3 . . . spaces above or below each other and then reading horizontally. Sometimes one alphabet may be broken into sections which are then rearranged, as in the Pasanisi Disk, described by Gioppi, pp. 58-62. See Riverbank Publication No. 20.

4d. **MIXED ALPHABETS**

Break up the message into its constituent cycles and apply the frequency method to them. Attempt a reconstruction of the Primary Alphabets. In case one of the alphabets is a Straight Alphabet, the reconstruction process is rendered relatively simple. See Riverbank Publications Nos. 20 and 21.

[Also from Table VIII, 5*b*]

2b. The individual alphabets of the entire system are not employed at regular and definite intervals, and do not result in either a Periodic System or a Progressive System. **(A-PERIODIC SYSTEMS.)**

3c. The successive alphabets are applied to word lengths. The various alphabets limited in number by a short key word, or a short key number; or the successive words are enciphered on random generatrices of a Poly-Alphabet.

3d. The successive alphabets are employed irregularly; or the total number of alphabets is large, etc.; ciphers of more or less complexity in decipherment because of the lack of recurrences.

Pages 10-13.

4e. **STRAIGHT ALPHABETS** (This case should have been solved under Table II, 2*a*.

5a. **DIRECT** Solve on the ordinary Poly-Alphabet or by applying the "running down" process according to the Direct Alphabet sequence.

5b. **REVERSED** Find the Direct Alphabet equivalents and proceed as in 5*a* of this table.

4f. **MIXED ALPHABETS**

5c. **KEYWORD ALPHABETS**

5d. **RANDOM-MIXED, OR ARBITRARILY-MIXED, ALPHABETS**

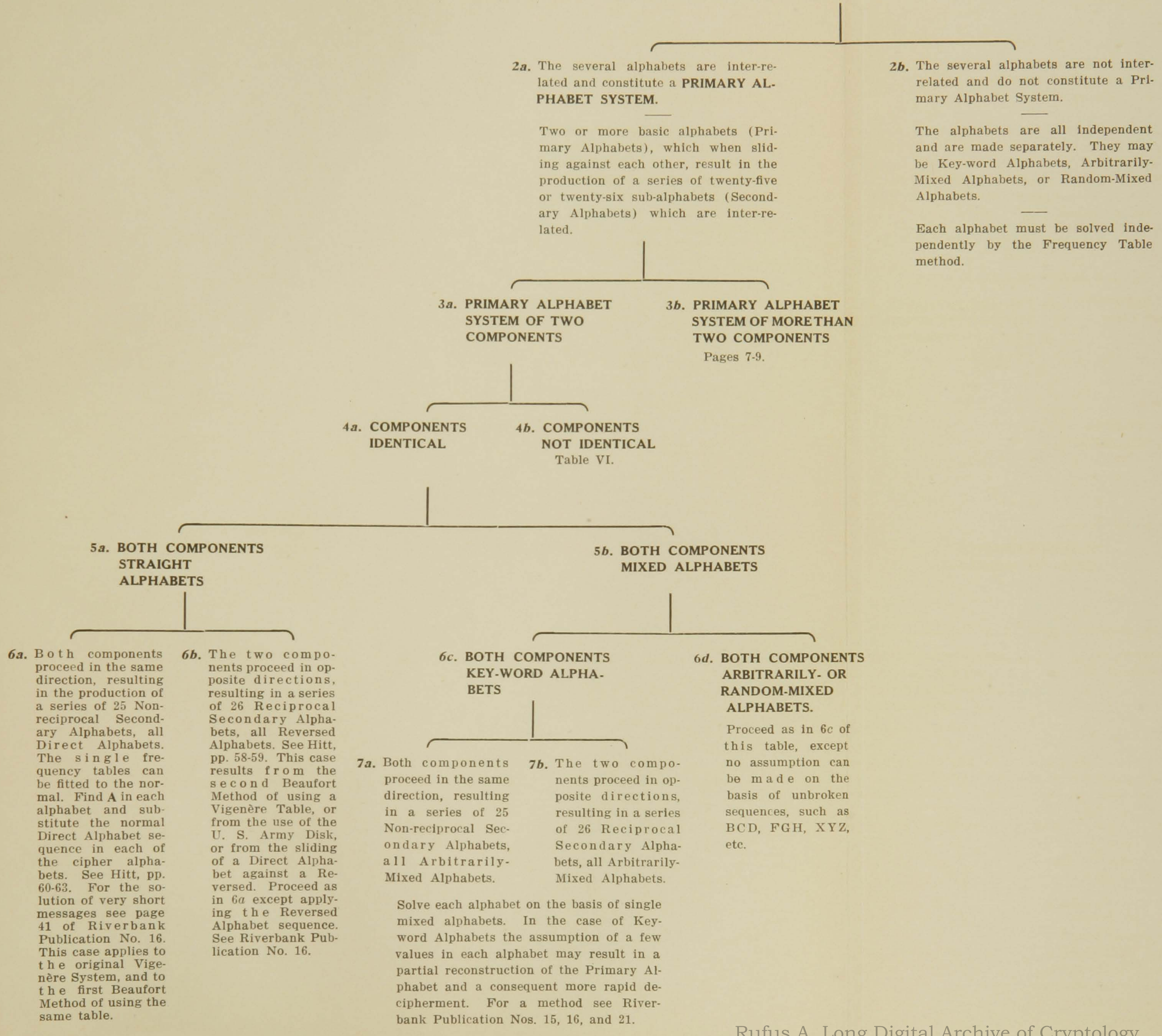
Assume probable words and attempt to localize them in the message on the basis of repeated letters. In case of 5c, attempt reconstruction of the Key-word Alphabet. When the successive words are enciphered on random generatrices of a Poly-Alphabet which is made up of Keyword, Arbitrarily-Mixed, or Random-Mixed Alphabets, solution of a single message, or even of a series of messages, is a very difficult achievement.

TABLE V

1. MULTIPLE ALPHABET SYSTEM—Continued

[From Table IV, *4a*]

(Periodicity governed by the successive single letters of the plain text.)



2a. The several alphabets are inter-related and constitute a **PRIMARY ALPHABET SYSTEM.**

Two or more basic alphabets (Primary Alphabets), which when sliding against each other, result in the production of a series of twenty-five or twenty-six sub-alphabets (Secondary Alphabets) which are inter-related.

2b. The several alphabets are not inter-related and do not constitute a Primary Alphabet System.

The alphabets are all independent and are made separately. They may be Key-word Alphabets, Arbitrarily-Mixed Alphabets, or Random-Mixed Alphabets.

Each alphabet must be solved independently by the Frequency Table method.

3a. **PRIMARY ALPHABET SYSTEM OF TWO COMPONENTS**

3b. **PRIMARY ALPHABET SYSTEM OF MORETHAN TWO COMPONENTS**
Pages 7-9.

4a. **COMPONENTS IDENTICAL**

4b. **COMPONENTS NOT IDENTICAL**
Table VI.

5a. **BOTH COMPONENTS STRAIGHT ALPHABETS**

6a. Both components proceed in the same direction, resulting in the production of a series of 25 Non-reciprocal Secondary Alphabets, all Direct Alphabets. The single frequency tables can be fitted to the normal. Find **A** in each alphabet and substitute the normal Direct Alphabet sequence in each of the cipher alphabets. See Hitt, pp. 60-63. For the solution of very short messages see page 41 of Riverbank Publication No. 16. This case applies to the original Vigenère System, and to the first Beaufort Method of using the same table.

6b. The two components proceed in opposite directions, resulting in a series of 26 Reciprocal Secondary Alphabets, all Reversed Alphabets. See Hitt, pp. 58-59. This case results from the second Beaufort Method of using a Vigenère Table, or from the use of the U. S. Army Disk, or from the sliding of a Direct Alphabet against a Reversed. Proceed as in *6a* except applying the Reversed Alphabet sequence. See Riverbank Publication No. 16.

5b. **BOTH COMPONENTS MIXED ALPHABETS**

6c. **BOTH COMPONENTS KEY-WORD ALPHABETS**

7a. Both components proceed in the same direction, resulting in a series of 25 Non-reciprocal Secondary Alphabets, all Arbitrarily-Mixed Alphabets.

7b. The two components proceed in opposite directions, resulting in a series of 26 Reciprocal Secondary Alphabets, all Arbitrarily-Mixed Alphabets.

Solve each alphabet on the basis of single mixed alphabets. In the case of Key-word Alphabets the assumption of a few values in each alphabet may result in a partial reconstruction of the Primary Alphabet and a consequent more rapid decipherment. For a method see Riverbank Publication Nos. 15, 16, and 21.

6d. **BOTH COMPONENTS ARBITRARILY- OR RANDOM-MIXED ALPHABETS.**

Proceed as in 6c of this table, except no assumption can be made on the basis of unbroken sequences, such as BCD, FGH, XYZ, etc.

TABLE VI

[From Table V, *4b*]

1. MULTIPLE ALPHABET SYSTEM—Continued

2. Primary Alphabet System of two components which are not identical.

3a. One of the components is a Straight Alphabet.

4a. The Straight Alphabet component is a Direct Alphabet.

5a. The Mixed Alphabet component is a Key-word Alphabet. Assume values for several of the high frequency letters in each alphabet and attempt reconstruction of the Mixed Alphabet on the basis of symmetry of position, and also of unbroken sequences, such as BCD, FGH, JKL, etc. Partial reconstruction will proceed simultaneously with decipherment, each aiding the other. Keep watch for the key word applying to the message by noting the successive cipher equivalents of A. See Riverbank Publications Nos. 15 and 22.

5b. The Mixed Alphabet component is an Arbitrarily-Mixed or a Random-Mixed Alphabet. Proceed as in *5a* except no assumptions of unbroken sequences in the mixed alphabet component can be made. See Hitt, pp. 63-71.

4b. The Straight Alphabet component is a Reversed Alphabet. Proceed as in *4a* except applying the Reversed Alphabet sequence to the Straight Alphabet component.

3b. Neither of the components is a Straight Alphabet, both Mixed Alphabets.

4c. Both components are Key-word Alphabets.

4d. Both components are Arbitrarily-Mixed or Random-Mixed Alphabets.

Solve the individual alphabets on the basis of single Mixed Alphabets. Attempt reconstruction of the Primary Alphabets. See Riverbank Publication No. 21.

TABLE VII

[From Table II, 4*b*]

1. SUBSTITUTION NOT EQUILITERAL

Usually, if the number of plain-text letters is *n*, the number of cipher letters is 2n, 3n, etc.

[Also from Table I, 2*b*]

2a. The number of different letters in the cipher message limited, usually not more than ten.

Systems using alphabets consisting of the various combinations of 2, 3, 4 . . . elements. (See Myers, pp. 65-165.) The number of characters in each combination is determined by the number of elements in the system. The least number of combinations possible must approximate 26, one for each letter of the alphabet.

$2^n=2^5=32$, a Biliteral Alphabet
$3^n=3^3=27$, a Triliteral Alphabet
$4^n=4^3=64$, a Tetraliteral Alphabet
$5^n=5^2=25$, a Pentaliteral Alphabet
etc., etc.

Example of a Pentaliteral Alphabet, resulting from the use of a rectangle and a key word:

	G	R	A	N	T
G	A	B	C	D	E
R	F	G	H	I	K
A	L	M	N	O	P
N	Q	R	S	T	U
T	V	W	X	Y	Z

Example:
Plain text— T H E
Cipher—NN RA GT

Solution: Make a frequency table of combinations, or assign arbitrary single letters to each different combination and then make a frequency table. Proceed as in Table III, 2*b*. See Hitt, pages 83-85.

2b. The number of different letters in the cipher message approximates 26.

[Also from Table I, 3*b*]

3a. Cipher groups all pronounceable. (Pseudo-code.)

4a. Regular arrangement of vowels and consonants, of the form CVCVC or VCVCV; groups all of the same length, either 5 or 10 letters.

5a. Regularity produced by the insertion of nulls. Compile a frequency table on the basis of every other letter and proceed as in Table III.

5b. Regularity produced by means of a table, or a rectangle on one side of which are consonants only, on the other side vowels only. Each plain-text letter requires two cipher letters.
Compile a frequency table of pairs and attempt reconstruction of the table, or rectangle.

6a. Rectangle based upon Straight Alphabets only. Make a frequency table of pairs and attempt a reconstruction of the rectangle.

6b. Rectangle not based upon Straight Alphabets.

7a. Rectangle based upon a Key-word Alphabet.

7b. Rectangle based upon an Arbitrarily-Mixed or a Random-Mixed Alphabet.

Solution by frequency of pairs. Attempt reconstruction of table.

4b. No regular arrangement or alternation of vowel and consonant.

Syllable ciphers (Built-up ciphers). Groups of irregular lengths usually. Substitution of letters or syllables for syllables of the plain text. Not often found and difficult to decipher in case of good systems. Solution by frequency of digraphs and trigraphs of the language.

3b. Cipher groups not pronounceable, except as the result of chance. Cipher groups usually the result of a square or a rectangular table, for enciphering not only letters but also syllables, words, phrases, etc. Approaching a code system.

The alphabets at the sides may be Key-Word Alphabets, Arbitrarily-Mixed, or Random-Mixed Alphabets, or numbers.

Solution: Make a frequency table of pairs and apply the frequency table method modified by considerations arising from the frequency of the most common words, for which substitution will have to be made by single pairs. Attempt a reconstruction of the alphabets at the sides.

TABLE VIII

[From Table I, *2d*]

1. NUMBER CIPHER

(Mathematical Ciphers)

Divide up the message into pairs of numbers unless already in this form.

2a. Interval between the lowest and the highest pair of numbers approximates 26.

3a. Cipher is solvable by means of the Poly-Alphabet (or by equivalent procedure) as below.

Apply the Normal Alphabet sequence to the numbers in sequence.

4a. **DIRECT ALPHABET**

Set two or three of the groups on the Poly-Alphabet or apply the "running down" process. Procedure and principles the same as in Table II, *2a*.

4b. **REVERSED ALPHABET**

Find the Reversed Alphabet Equivalents for two or three of the groups and proceed as in *4a*, of this table.

3b. Cipher is not solvable by means of the Poly-Alphabet (or equivalent procedure).

Apply letter equivalents consistently or continue to deal with the pairs of numbers, and apply the process of factoring the intervals separating recurrences.

4c. Factoring discloses no repeatedly recurring factors.

Compile a single frequency table.

5a. Frequency table shows marked "crests and troughs." Single Mixed Alphabet. Proceed as in Table III, *3d*.

5b. Frequency table shows no marked "crests and troughs," but is "solid." Multiple Alphabet (Poly-Alphabet System). Proceed as in Table IV, *2b*.

4d. Factoring discloses certain repeatedly recurring factors.

Periodic Multiple Alphabet System.

Proceed as in Table IV, *2a*.

Periodicity may be produced by the use of a key word in conjunction with a basic table. An example of such a system:

	0	1	2	3	4	5	6	7
1	A	B	C	D	E	F	G	H
2	I	J	K	L	M	N	O	P
3	Q	R	S	T	U	V	W	X
4	Y	Z						

The values of the letters of a key word are added successively to the values of the plain-text letters. Thus:

Key word—	H	E	L	P
Value—	17	14	23	27

Plain text—	T	H	E	E	N	E	M	Y	W	I
Plain-text values—	33	17	14	14	25	14	24	40	36	20
Key-letter values—	17	14	23	27	17	14	23	27	17	14
Cipher—	50	31	37	41	42	28	47	67	53	34

2b. Interval between lowest and highest pairs does not approximate 26. The numbers range from 01 to 00 or 00 to 99, implying usually that each plain-text letter has several values used at random.

3c. The several values for each plain-text letter are produced by means of a rectangular table. Rectangle with sides 10x3, letters within.

4e. Letters in sequence of Straight Alphabet, numbers straight. Make a frequency table and attempt to find arrangement of left hand numbers. See Hitt, pp. 86-88.

4f. Letters in rectangle not in sequence of Straight Alphabet.

5c. Letters in Key-word Alphabet sequence. Attempt reconstruction of Key-word Alphabet from VWXYZ sequence.

5d. Letters in Random-Mixed Alphabet sequence.

Make frequency tables of sequences from 1 to 10, 11 to 20, etc.; match these, combine and proceed as if Single Mixed Alphabet, Table III, *2b*.

3d. The several values for each plain-text letter are given by a series of 4 Direct Alphabets, with letters and numbers in sequence.

4g. Alphabets are continuous from 01 to 00.

4h. Alphabets are independent, in cycles of 25 or 26.

Make 4 frequency tables and try to fit each to the normal frequency table.

TABLE IX

[From Table I, 4*a*]

1. TRANSPOSITION CIPHER

2. Including Route Ciphers, which are only a type of transposition ciphers wherein the words are treated as individual letters. Regard each word as a single letter or apply arbitrary letters or numbers to the words and proceed as below.

3a. **SIMPLE SYSTEM**

4a. Vertical writing.

4b. Reversed writing.

4c. Rail fence cipher.

See Hitt, pages 28-30.

3b. **MORE COMPLEX SYSTEM**

4d. Transposition based upon geometrical designs.

Factoring process applied first to suggest possible rectangles.

5a. Construct rectangles suggested by the factors and attempt reading by all methods. See Hitt, pp. 26-38.

5b. Solve by means of formulae. See Riverbank Publication No. 19.

4e. Transposition not based upon geometrical designs.

5c. Transposition based upon rearrangement of entire columns, or rows, or both.

6a. **COLUMNAR TRANSPOSITION**

Factor to suggest possible rectangles. Write the message on strips of cross-section paper and apply method of anagrams.

6b. **LINEAR TRANSPOSITION**

Same procedure as in 6*a* except working with rows instead of columns.

6c. **COMBINED COLUMNAR AND LINEAR TRANSPOSITION**

Proceed as in 6*a*, then as in 6*b*, i. e., anagram columns, then horizontal lines.

See Hitt, pp. 26-38.

5d. Transposition based upon rearrangement or redistribution of individual letters by means of a grille. Solve by anagram method and attempt reconstruction of the grille. See Gioppi, pp. 33-31.

DIGRAPHIC AND TRIGRAPHIC SUBSTITUTION

The chief advantage of digraphic and trigraphic substitution is that it prevents the decipherer from basing his analysis upon the frequency of individual letters in the language, and forces him to base any analysis to be made upon the frequency of digraphs and trigraphs: a circumstance which causes the analysis to become correspondingly difficult and, in addition, lessens the reliance which may be placed in it.

There are several ways of procuring digraphic substitution, of which the Playfair System is by far the most practical. Most of the other systems require tables, the use of which entails the expenditure of much labor, and the loss of one copy of which renders the entire system utterly unsafe. An excellent example of such a table is that shown in Fig. 1, which was taken from *La Crittografia*, pp. 84 and 85. Here the reciprocal relation

	+	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	W	
+	i x	g u	d o	m q	a g	j h	s p	c f	k i	b z	y q	e m	q r	k k	f p	k n	u o	e c	h j	i p	d f	n c	m r	c t	d i	m d	h a	+
A	v b	x z	k j	y j	h p	p l	e t	+d	c i	d w	x n	z l	y p	v n	h h	c c	r f	c x	p s	z y	h y	s r	y e	f b	g n	w g	i j	A
B	c k	l p	q t	h e	r s	u r	c r	z h	g v	w c	h l	y n	k t	w t	m c	k h	e w	g f	s q	y t	w a	h v	f n	v o	e u	+i	g d	B
C	g i	d x	m u	a o	n h	s f	+g	w l	m m	a h	g r	b+	h s	z u	y m	w u	r z	e y	b f	t a	+x	l d	q b	a q	v+	q u	u s	C
D	x k	k m	y z	r y	f+	t r	+t	x e	j k	+y	p o	g j	j x	p e	m o	+b	u k	h w	x u	r h	k y	i i	n q	e a	l f	w y	a i	D
E	l w	q n	h p	q g	j q	+q	o b	s a	n l	p x	o p	v s	a f	+k	x r	u+	n t	t z	l i	r a	k d	b y	s l	z g	c q	j v	b p	E
F	d d	m i	a x	n b	w j	l c	z s	i e	u a	r v	s+	t x	o y	j c	b v	t t	+n	l o	t g	r q	v z	l s	g s	y y	j l	h n	n v	F
G	k c	y k	r m	v z	o a	o v	b q	y i	x a	c+	d k	m y	n w	t q	a y	z m	r r	y b	c j	f v	o n	+a	b h	t u	s z	m e	k h	G
H	q a	+w	k+	p t	t o	b c	x q	l r	a n	v q	+r	v p	b j	y x	f z	l z	e b	a d	w d	c l	q o	p n	b u	v w	a t	q f	d q	H
I	m f	o h	t n	u x	u e	f g	q c	t b	o m	d u	a w	r t	x e	v y	q w	y a	+s	o z	q v	u g	p q	v h	t j	++	q z	x y	o u	I
J	y v	r c	w k	f m	t y	z o	k a	o+	+e	k b	x s	d h	f y	q l	v f	u v	o k	e d	y o	p r	v g	o q	e z	d l	m z	k l	u y	J
K	h b	j f	j i	g+	e t	s u	x o	v l	b o	+h	a b	+m	j z	d a	+o	s w	v m	s g	u m	y c	b l	v t	x d	g w	d t	y h	q e	K
L	s m	n j	p w	f e	c u	w b	d y	u j	v k	e r	n f	w n	r i	s d	o e	f q	b a	n p	h g	f u	s h	x g	u w	m s	p j	h o	e+	L
M	r l	w v	u d	b n	+z	g z	i+	t w	w p	f a	n u	p u	p p	c h	q q	d n	v i	+c	+v	l x	o f	c b	s e	p y	g k	j y	r u	M
N	t e	p b	f c	+u	r g	x p	l j	s o	c d	o s	l a	u t	e h	x w	p g	q i	l q	d v	t+	r o	e p	m j	f w	u f	w o	x t	g l	N
O	j g	g d	e f	v d	z n	l n	m t	r p	i a	s n	w m	j p	r b	i h	g t	p c	e j	j u	u z	n i	v r	i w	g e	v v	f l	i q	z v	O
P	w s	u l	n a	o o	s k	d m	y u	n n	q+	z+	l y	r f	a e	t v	h u	d j	m l	i t	j s	a r	h c	m k	x h	e i	m x	s j	l b	P
Q	p h	h+	c v	i f	b w	k w	h z	e c	z c	n o	v x	r e	j m	t i	e a	h t	w w	m n	+l	t m	b b	c z	i r	y d	u h	t y	i n	Q
R	u q	e s	o l	j a	x i	q k	a p	n d	d s	l l	z k	z q	m+	g b	y s	n s	o g	f s	g p	b d	i k	m w	f i	w e	d c	o p	t f	R
S	f j	e g	z r	z w	l m	m v	c e	k q	l t	t k	p z	p d	e v	l+	o i	n g	+f	b r	a u	u b	z i	k e	t c	y w	z a	g y	k o	S
T	n r	c s	i g	s v	x+	n+	r w	f r	y r	q m	i v	s i	w r	q s	i b	h d	v j	g m	d e	w x	f o	g x	p m	f k	j d	e q	m g	T
U	e o	f h	s s	x l	m b	i d	u x	i s	q y	z j	l g	d p	p a	k r	w f	+b	z b	r+	b e	c w	n k	z x	j o	i c	j w	o r	l v	U
V	c y	z e	a+	x m	o c	y f	j n	j t	i u	m p	t p	l h	k g	k p	a m	b x	b k	h i	o t	e k	k u	y+	o x	q j	i m	f t	h x	V
X	t d	g h	y g	d g	k v	i l	w i	l u	p v	r d	z b	d+	u c	v c	a j	k f	n e	h f	e n	j j	n z	d r	z z	w h	i z	a a	n m	X
Y	v u	i o	g q	k s	q z	a v	v e	x b	k z	g g	a c	g a	z d	c n	b k	j r	a l	+j	t h	r n	b s	p f	j+	k m	f x	d b	s x	Y
Z	p i	s y	x j	q h	y l	v a	p k	e x	b g	s t	u i	r j	a k	g o	o d	j e	w+	r k	s b	f f	u p	e m	o w	u u	a s	x v	s c	Z
W	z p	b t	l e	b i	h r	r x	u n	a z	x x	x f	f d	j b	c g	o j	l k	n y	m h	w q	t l	p+	b m	c o	m a	t s	d z	g c	q p	W
	+	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	W	

Fig. 1

of plain text and cipher text is such that the same table can be used for enciphering and deciphering. For example:

```
Enciphering—TH  EN  EM  YP  RE  PA  RE
            YR  XR  +K  AL  QK  UL  QK

Deciphering—YR  XR  +K  AL  QK  UL  QK
            TH  EN  EM  YP  RE  PA  RE
```

Note that two pairs, even if they involve a common letter, do not have a common letter in the cipher equivalent, except as a matter of chance. The result of this fact is that no grouping of cipher pairs representing combinations of E with other letters can be made upon the basis of a common letter in such cipher pairs.

The process of arranging such a table, however, is very laborious, so that frequent change is impractical. Another form of such a table which may, on the other hand, be changed very frequently, but which does not possess the reciprocal relation, is that shown in Fig. 2, but here there is an added disadvantage—that of having a common cipher letter as a result in those pairs which represent plain-text pairs having a letter in common. Thus ER, EN, ES, and ET are enciphered by TU, TK, TV, and WT respectively, or by the reversals of the latter. These digraphs are found at the intersection of the vertical column determined by the first letter of each pair as located in the top line, and the row determined by the second letter of each pair as located in the first column at the left. When the cipher pair is taken at the intersection of the row determined by the first letter, and the vertical column determined by the second letter of each pair, the equivalents for these same combinations are UK, KF, VL, and WN, or their reversals; but note that all the combinations ending with the same letter will show a letter in common.

The same results may be obtained by employing sliding strips, as shown in the accompanying diagram. The direct alphabet, I, and the second mixed alphabet, IV, are fixed; the first mixed alphabet, III, is mounted upon a movable strip with another direct alphabet, II; the sliding alphabets are moved so that the first letter of the pair on alphabet II is placed beneath A on alphabet I, then under the second letter of the pair on I, the two cipher equivalents of the pair are found on III and IV. Thus, for the word THIS the successive positions and encipherments are as follows:

```
      (  I—ABCDEFGHIJKLMNOPQRSTUVWXYZ  Fixed Alphabet
      ) II—TUVWXYZABCDEFGHIJKLMNOPQRS )
TH=SA<                                 } Movable Alphabets
      )III—MQUVWXZSTENOGRAPHYBCDFIJKL )
      ( IV—CRYPTOGAMSBDEFHIJKLNQUVWXZ  Fixed Alphabet

      (  I—ABCDEFGHIJKLMNOPQRSTUVWXYZ  Fixed Alphabet
      ) II—IJKLMNOPQRSTUVWXYZABCDEFGH )
IS=SL<                                 } Movable Alphabets
      )III—PHYBCDFIJKLMQUVWXZSTENOGRA )
      ( IV—CRYPTOGAMSBDEFHIJKLNQUVWXZ  Fixed Alphabet
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	S C	T R	E Y	N P	O T	G O	R G	A A	P M	H S	Y B	B D	C E	D F	F H	I I	J J	K K	L L	M N	Q Q	U U	V V	W W	X X	Z Z	A
B	T C	E R	N Y	O P	G T	R O	A G	P A	H M	Y S	B B	C D	D E	F F	I H	J I	K J	L K	M L	Q N	U Q	V U	W V	X W	Z X	S Z	B
C	E C	N R	O Y	G P	R T	A O	P G	H A	Y M	B S	C B	D D	F E	I F	J H	K I	L J	M K	Q L	U N	V Q	W U	X V	Z W	S X	T Z	C
D	N C	O R	G Y	R P	A T	P O	H G	Y A	B M	C S	D B	F D	I E	J F	K H	L I	M J	Q K	U L	V N	W Q	X U	Z V	S W	T X	E Z	D
E	O C	G R	R Y	A P	P T	H O	Y G	B A	C M	D S	F B	I D	J E	K F	L H	M I	Q J	U K	V L	W N	X Q	Z U	S V	T W	E X	N Z	E
F	G C	R R	A Y	P P	H T	Y O	B G	C A	D M	F S	I B	J D	K E	L F	M H	Q I	U J	V K	W L	X N	Z Q	S U	T V	E W	N X	O Z	F
G	R C	A R	P Y	H P	Y T	B O	C G	D A	F M	I S	J B	K D	L E	M F	Q H	U I	V J	W K	X L	Z N	S Q	T U	E V	N W	O X	G Z	G
H	A C	P R	H Y	Y P	B T	C O	D G	F A	I M	J S	K B	L D	M E	Q F	U H	V I	W J	X K	Z L	S N	T Q	E U	N V	O W	G X	R Z	H
I	P C	H R	Y Y	B P	C T	D O	F G	I A	J M	K S	L B	M D	Q E	U F	V H	W I	X J	Z K	S L	T N	E Q	N U	O V	G W	R X	A Z	I
J	H C	Y R	B Y	C P	D T	F O	I G	J A	K M	L S	M B	Q D	U E	V F	W H	X I	Z J	S K	T L	E N	N Q	O U	G V	R W	A X	P Z	J
K	Y C	B R	C Y	D P	F T	I O	J G	K A	L M	M S	Q B	U D	V E	W F	X H	Z I	S J	T K	E L	N N	O Q	G U	R V	A W	P X	H Z	K
L	B C	C R	D Y	F P	I T	J O	K G	L A	M M	Q S	U B	V D	W E	X F	Z H	S I	T J	E K	N L	O N	G Q	R U	A V	P W	H X	Y Z	L
M	C C	D R	F Y	I P	J T	K O	L G	M A	Q M	U S	V B	W D	X E	Z F	S H	T I	E J	N K	O L	G N	R Q	A U	P V	H W	Y X	B Z	M
N	D C	F R	I Y	J P	K T	L O	M G	Q A	U M	V S	W B	X D	Z E	S F	T H	E I	N J	O K	G L	R N	A Q	P U	H V	Y W	B X	C Z	N
O	F C	I R	J Y	K P	L T	M O	Q G	U A	V M	W S	X B	Z D	S E	T F	E H	N I	O J	G K	R L	A N	P Q	H U	Y V	B W	C X	D Z	O
P	I C	J R	K Y	L P	M T	Q O	U G	V A	W M	X S	Z B	S D	T E	E F	N H	O I	G J	R K	A L	P N	H Q	Y U	B V	C W	D X	F Z	P
Q	J C	K R	L Y	M P	Q T	U O	V G	W A	X M	Z S	S B	T D	E E	N F	O H	G I	R J	A K	P L	H N	Y Q	B U	C V	D W	F X	I Z	Q
R	K C	L R	M Y	Q P	U T	V O	W G	X A	Z M	S S	T B	E D	N E	O F	G H	R I	A J	P K	H L	Y N	B Q	C U	D V	F W	I X	J Z	R
S	L C	M R	Q Y	U P	V T	W O	X G	Z A	S M	T S	E B	N D	O E	G F	R H	A I	P J	H K	Y L	B N	C Q	D U	F V	I W	J X	K Z	S
T	M C	Q R	U Y	V P	W T	X O	Z G	S A	T M	E S	N B	O D	G E	R F	A H	P I	H J	Y K	B L	C N	D Q	F U	I V	J W	K X	L Z	T
U	Q C	U R	V Y	W P	X T	Z O	S G	T A	E M	N S	O B	G D	R E	A F	P H	H I	Y J	B K	C L	D N	F Q	I U	J V	K W	L X	M Z	U
V	U C	V R	W Y	X P	Z T	S O	T G	E A	N M	O S	G B	R D	A E	P F	H H	Y I	B J	C K	D L	F N	I Q	J U	K V	L W	M X	Q Z	V
W	V C	W R	X Y	Z P	S T	T O	E G	N A	O M	G S	R B	A D	P E	H F	Y H	B I	C J	D K	F L	I N	J Q	K U	L V	M W	Q X	U Z	W
X	W C	X R	Z Y	S P	T T	E O	N G	O A	G M	R S	A B	P D	H E	Y F	B H	C I	D J	F K	I L	J N	K Q	L U	M V	Q W	U X	V Z	X
Y	X C	Z R	S Y	T P	E T	N O	O G	G A	R M	A S	P B	H D	Y E	B F	C H	D I	F J	I K	J L	K N	L Q	M U	Q V	U W	V X	W Z	Y
Z	Z C	S R	T Y	E P	N T	O O	G G	R A	A M	P S	H B	Y D	B E	C F	D H	F I	I J	J K	K L	L N	M Q	Q U	U V	V W	W X	X Z	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Fig. 2

Given a single long message or a series of messages in the same alphabets, a frequency table of pairs may be made the basis of solution, by assigning high-frequency-digraph values to the most frequent pairs. In the latter case, where two pairs having a common cipher letter have a common letter in their respective cipher equivalents, this relation would be a great aid in the assignment of values, since it would enable the decipherer to assign his values accordingly. In the case of key-word and direct alphabets the reconstruction of the alphabets may be attempted. Arbitrarily-mixed and random-mixed alphabets may also be used in such tables.

Still another form of table which may be used for digraphic substitution is that shown in Fig. 3. Here there are concerned one mixed and two direct alphabets and a quadricular table. The first letter of a pair is sought in Alphabet I, its equivalent taken in Alphabet II, and by following the horizontal line in the quadricular table determined by the second letter of the pair in Alphabet III to the vertical column determined by the first letter, the cipher letter is taken at the intersection. Thus:

```
  I—A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 II—F S K Z R B J E Y Q A H L T G X P D C U I W N V O M
III
 A  H T C G W S R K B F J V I Q A E L U D P X M Z O Y N
 B  T C G W S R K B F J V I Q A E L U D P X M Z O Y N H
 C  C G W S R K B F J V I Q A E L U D P X M Z O Y N H T
 D  G W S R K B F J V I Q A E L U D P X M Z O Y N H T C
 E  W S R K B F J V I Q A E L U D P X M Z O Y N H T C G
 F  S R K B F J V I Q A E L U D P X M Z O Y N H T C G W
 G  R K B F J V I Q A E L U D P X M Z O Y N H T C G W S
 H  K B F J V I Q A E L U D P X M Z O Y N H T C G W S R
 I  B F J V I Q A E L U D P X M Z O Y N H T C G W S R K
 J  F J V I Q A E L U D P X M Z O Y N H T C G W S R K B
 K  J V I Q A E L U D P X M Z O Y N H T C G W S R K B F
 L  V I Q A E L U D P X M Z O Y N H T C G W S R K B F J
 M  I Q A E L U D P X M Z O Y N H T C G W S R K B F J V
 N  Q A E L U D P X M Z O Y N H T C G W S R K B F J V I
 O  A E L U D P X M Z O Y N H T C G W S R K B F J V I Q
 P  E L U D P X M Z O Y N H T C G W S R K B F J V I Q A
 Q  L U D P X M Z O Y N H T C G W S R K B F J V I Q A E
 R  U D P X M Z O Y N H T C G W S R K B F J V I Q A E L
 S  D P X M Z O Y N H T C G W S R K B F J V I Q A E L U
 T  P X M Z O Y N H T C G W S R K B F J V I Q A E L U D
 U  X M Z O Y N H T C G W S R K B F J V I Q A E L U D P
 V  M Z O Y N H T C G W S R K B F J V I Q A E L U D P X
 W  Z O Y N H T C G W S R K B F J V I Q A E L U D P X M
 X  O Y N H T C G W S R K B F J V I Q A E L U D P X M Z
 Y  Y N H T C G W S R K B F J V I Q A E L U D P X M Z O
 Z  N H T C G W S R K B F J V I Q A E L U D P X M Z O Y
```

Fig. 3

```
TH ER EI SN OT HI NG
UH RM RI CS GK EE TP
```

Note that as far as the first letter in each pair is concerned, the encipherment is merely by means of a single mixed alphabet. It is only the encipherment of the second letter which is multi-alphabetical in nature.

The same table shown in Fig. 3, with one additional alphabet, IV, may be used for trigraphic substitution. The equivalent of the first letter in a group is found in Alphabet II directly beneath that letter in Alphabet I. The equivalent of the second letter is found in Alphabet IV directly opposite the letter in Alphabet III. The equivalent of the third letter is found at the intersection of the horizontal line in the quadricular table determined by the second letter, and the vertical column determined by the position of the third letter in Alphabet I. Thus:

```
THE REI SNO THI NGT
URV DDI CQH URE TAN
```

The variations of this system are many; but as far as the two letters in each group of triplets is concerned, encipherment is purely mono-alphabetical. (See Gioppi, pp. 45-46.)

	I—	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	II—	F	S	K	Z	R	B	J	E	Y	Q	A	H	L	T	G	X	P	D	C	U	I	W	N	V	O	M
III	IV																										
A	K	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N
B	S	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H
C	B	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T
D	U	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C
E	D	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G
F	J	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W
G	A	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S
H	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R
I	V	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K
J	I	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B
K	H	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F
L	T	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J
M	L	I	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V
N	Q	Q	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I
O	G	A	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q
P	C	E	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A
Q	M	L	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E
R	F	U	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L
S	X	D	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U
T	O	P	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D
U	Y	X	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P
V	N	M	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X
W	Z	Z	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M
X	W	O	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z
Y	P	Y	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O
Z	E	N	H	T	C	G	W	S	R	K	B	F	J	V	I	Q	A	E	L	U	D	P	X	M	Z	O	Y

Fig. 4

COMPLEX SYSTEMS

When the steps in analysis given in the preceding tables have failed to lead to results, it may be concluded that the cipher is either the result of (1) a modification or a combination of the systems enumerated, such as the combination of Substitution and Transposition systems, or (2) a system simple in itself as regards enciphering, but difficult in its results as far as deciphering is concerned. Some of the latter have been devised by experts who are in possession of all the known methods of attacking ciphers and have elaborated systems which allow no opening for the would-be decipherer. No attempt is made here to enumerate or to elucidate all of these systems, but among them may be mentioned the following:

(1) Running Key Systems

(2) Multiplex Alphabet Systems

(3) Wheatstone Principle Systems

(4) Fractionating Systems

(5) Auto-key Systems

(6) Variable Key Systems

(1) Running Key Systems. These systems make use of the running text of a book, identical copies of which are in possession of the correspondents. For a brochure on the subject see Riverbank Publication No. 16.

(2) Multiplex Alphabet Systems. These systems make use of a machine on the principle of the Bazeries disk cipher (Bazeries, pp. 250-261). For a brochure on the subject see Riverbank Publication No. 20; also De Viaris, "*L'Art de Chiffrer*," pp. 99-109.

(3) Wheatstone Principle Systems, which are based upon a mechanical cryptograph invented by Sir Charles Wheatstone in 1879. For a discussion of such a cipher and methods for solving it see Riverbank Publication No. 20.

(4) Fractionating Systems. The basic principle here is that the cipher letters or cipher numbers are compounded from parts of plain-text letters according to some definite system. A simple example is the following:

Alphabet—	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numerical Value——	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Each letter is represented by two digits. Write the dispatch horizontally, then apply the two digits for each letter one under the other. Thus:

```
ENEMY PREPARES
01012 11010101
54535 68561859
```

The cipher then is taken in any way in which a rearrangement of the digits may be effected. Thus, a very simple way would be to take the cipher digits in pairs from horizontal lines, and then find their letter equivalents on the conventional alphabet. This dispatch would begin

AAVJJ OSI etc.

In the case of any cipher number above 26, deduct 26 or a multiple thereof and find the equivalent of the remainder. Variations of the system are legion in number. The plain text may be written in groups of three, four, or five letters and the cipher letters may be selected accordingly upon some different scheme. This system, because of the number of unknown factors which are presented to the would-be decipherer, is a very difficult one to solve. Fractionating systems in which each cipher letter represents the halves, thirds, quarters, and possibly greater fractions of 2, 3, 4, or 5 plain-text letters may be devised, and would tax the ingenuity of the expert decipherer. (See Gioppi, pp. 102-114.)

(5) Auto-key Systems. Sometimes called Auto-enciphering Systems. This system was described by Vigenère, reinvented in 1884 by Captain Delauney, and perfected by Josse. The basic principle is that each cipher letter automatically becomes the key for the encipherment of the succeeding plain-text letter. Usually a key-word alphabet or a random-mixed alphabet is used, the letters of which are numbered in sequence. Thus:

A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

MESSAGE: Enemy prepares, etc.

```
          E    N    E    M    Y    P    R    E    P    A    R    E    S
          22  20   22   12   17   14   18   22   14   11   18   22   26
            ↗    ↗    ↗    ↗    ↗    ↗
          22   16   12   24   15    3   21   17    5    6   24   20   20
CIPHER:   E    K    M    U    B    W    T    Y    H    V    U    N    N
```

Each cipher letter is produced in turn by finding the letter-value of the sum of the numerical equivalent of the preceding cipher letter and that of the plain-text letter to be enciphered; when this total exceeds 26, the latter amount is deducted and the letter-value of the remainder is taken as the cipher equivalent.

The great disadvantage of this system is that an error in one place produces errors in all the succeeding letters so that the recipient is caused to lose much time in the translation of a message which has many errors. A method which dispenses with the numerals is to construct a quadricular table from the alphabet as shown in Fig. 6.

	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S
A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A
I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I
W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W
G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G
H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H
V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V
L	J	V	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L
J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J
X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	B	L	J	X
O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O
C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C
M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M
Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z
P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P
B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B
K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K
Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y
R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R
D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D
N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N
T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T
E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E
Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q
U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U
F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F
S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S

Fig. 6

Proceeding down the column determined by E (the first letter of the message) in the first horizontal line, to the line determined by the next plain-text letter N, the letter K, at the intersection, is taken as the cipher letter. Proceeding down the column determined by K in the first horizontal line to the line determined by E, the third plain-text letter, the cipher letter M, at the intersection, is taken as the cipher letter, etc. (See Gioppi, pp. 42-44.)

A method which is the equivalent to the quadricular table in its final results and which is easier to operate, makes use of two sliding strips bearing the alphabets; by shifting the lower strip so that the letter which becomes the key letter for the next encipherment, is placed beneath the letter immediately preceding the first letter in the alphabet concerned, the cipher letter to represent the next text letter is found under the letter itself. The successive positions for the word ENEMY are as follows:

```
                Plain text
                    Cipher
                     26 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
I and II-- { E=E     S  A I W G H V L J X O  C  M  Z  P  B  K  Y  R  D  N  T  E  Q  U  F  S
           { N=K     E  Q U F S A I W G H V  L  J  X  O  C  M  Z  P  B  K  Y  R  D  N  T  E
         III—E=M     K  Y R D N T E Q U F S  A  I  W  G  H  B  L  J  X  O  C  M  Z  P  B  K
          IV—M=U     M  Z P B K Y R D N T E  Q  U  F  S  A  I  W  G  H  V  L  J  X  O  C  M
           V—Y=B     U  F S A I W G H V L J  X  O  C  M  Z  P  B  K  Y  R  D  N  T  E  Q  U
```

Such a cipher is poly-alphabetical in nature and is characterized by the small number of repetitions. It is clear that all letters following the same cipher letter belong to the same alphabet. Frequency tables may be constructed upon this basis and combinations may be sought. It should be kept in mind that all the alphabets concerned in such a system are inter-related and come under the classification of Primary Alphabet Systems involving two identical mixed alphabet components.

(6) Variable-key Systems. Examples of these systems are to be found in those cases where the alphabets employed are applied irregularly, for instance, the alphabet may change after the encipherment of every plain-text letter E; or the key word may be broken irregularly, breaks being indicated by an agreed-upon null or indicator. The basic idea in such systems is the elimination of the external manifestations (such as those exhibited in Periodic Systems) by means of which it is possible to determine the number of alphabets and their respective positions. These systems, however, are not often encountered because of the practical difficulties attendant upon their use and the possibilities of error. (See Gioppi, pp. 34-35; Valerio, pp. 36-42; Bazeries, pp. 128-139.)

BIBLIOGRAPHY

OF WORKS ON CIPHER

Alberti, Leo B. *Opusculi morali* (Chap. on cipher), Venice, 1568.

d'Ambrum, Comiers, *Traité de la Parole, etc.,* Brussels, 1691.

Astle, *The Origin and Progress of Writing*, 1803.

Auriol, d' *Manuel de la correspondance secrete postale et télégraphique*, Parigi, 1887.

Baravelli, *Cifrario*, Roma, 1895.

Bartels, *Leitfaden fuer den Unterricht auf dem königlichen Kriegsschulen*, Berlin, 1881.

Bazeries, Etienne, *Etude sur la cryptographie militaire*, 1900.

Bazeries, Etienne, *Les chiffres secrets dévoilés*, 1901.

Becherus, *Spirensis Character, notitia linguarum universali*, Frankfort, 1661.

Beaufort, *A System of Secret Writing*, London, 1883; 1893.

Bellaso, *Novi et singolari modi di cifrare* (8pp.), Brescia, 1555.

Bellaso, *Vero modo di scrivere in cifra* (16pp.), Brescia, 1564.

Bibliander, Theodorus, *Tract, de ratione communarum lingarum.*

Blair, William, *In Rees's Cyclopaedia, s.v."Cipher."*

Boetzel, A., *Correspondance postale, télégraphique et téléphonique secrète*, 1898.

Boetzel et O'Keenan, *Écriture secrète*, Paris, 1895.

Bolton, *Dictionary of Cryptography*, London.

Bontemps, *Les systèmes télégraphiques*, Paris.

Brachet, *Dictionnaire chiffré*, Paris, 1850.

Breithaupt, Chr., *Disquisitio historica critica, cun'osa de vanis modis occulte scribendi*, Helmstadt, 1727.

Breithaupt, *Ars decifratoria sive occultas scripturas solvendi et legendi scientia*, Helmstadt, 1737.

B(ridges), N., *Sténographie and Cryptographie*, London, 1659.

Brunswick, *Dictionnaire pour la correspondance télégraphique secrète*, Paris, 1868.

B(ulwer), J(ohn), *Chirologia and Chiromania*, London, 1644.

Cardano, Girolamo, *De Rerum Varietate* (Bk. XII, Ch. 61), 1557.

Cardano, *De subtilitate.*

Carlet, du, *Cryptographie*, Paris, 1644.

Carlet, du, Jean Robert, *La Cryptographie*, Toulouse, 1644.

Casaubon, Isaac, 1559 to 1614.

Collange, Gabriel de, *Polygraphie et universelle escriture cabalistique de Trithème*, Paris, 1561.

Colorno, Abram, *Scotographia Italica*, Prague, 1593.

Conrad, David Arnold, *Cryptographia denudata, sive ars decifrandi*, Leiden, 1739.

Corticelli, L., *L'Ozio superato nelle cifre discolte*, Bologna, 1702.

Cospi, *Interpretazione delle cifre* (45 pp.), (English translation by Niceron, 1641), Florence, 1639.

Dalgarno, George, *Ars Signorum*, London, 1661.

Davys, John, *Essay on the Art of Deciphering*, London, 1737.

Delastelle, F., *Cryptographie nouvelle*, Paris, 1893.

Delastelle, F., *Traité élémentaire de cryptographie*, 1902.

Falconer, John, *Cryptomenysis patefacta* ("Art of Secret Information"), London, 1695.

Fleissner, *Handbuch der Kryptographie*, Vienna, 1861.

Friderici, *Cryptographie, oder Geheim-Correspondenz*, Leipzig, 1685.

Gioppi, L., *La Crittografia* (Manuali Hoepli), 1897.

Glauburg, von, *Expositio ad Polygraphiam Trithemii.*

Gravezande, *Introduction à la philosophie*, Leyden, 1737.

Gross, H., *Handbuch fuer Untersuchungsrichter*, Teil II, Munich, 1914.

Hanedi (Resene Gibronte Reneclus), *Steganologia et Steganographia Nova*, Nürnberg, 1617.

Hitt, Parker, *Manual for the Solution of Military Ciphers*, Leavenworth, 1916 and 1918.

Hugo, Germann, *De Origine scribendi.*

Hottinga, D., *De Polygraphie*, Groningen, 1621.

Hulme, F. Edward, *Cryptography*, London, n. d.

Jacob, *Les secrets de nos pères, La Cryptographie*, Paris, 1858.

Jolliet, *Les écritures secrètes dévoilés*, Paris, 1887.

Kasiski, *Die Geheimschriften und die Dechiffrirkunst*, Berlin, 1863.

Kerckhoffs, A., *La Cryptographie militaire*, Paris, 1883.

Kircher, *Polygraphia nova et universalis*, Roma, 1663.

Klüber, J. L., *Cryptographik*, Tübingen, 1809.

Krohn, *Buchstaben und Zahlensysteme fuer die Chiffrirung von Telegrammen*, Berlin, 1873.

Lacroin, P., *Les Secrets*, 1858.

LaCroix, *La cryptographie ou l'art d'écrire en chiffres*, Paris, 1881.

L'Esprit, *Éléments de cryptographie*, Paris, 1889.

Louis, *Dictionnaire, pour la correspondance secrète*, Paris, 1881.

Mamert-Gallian, *Dictionnaire télégraphique économique et secret*, Paris, 1874.

Martin, G. von, *Cours diplomatique*, 1801.

Mauborgne, J. O., *An Advanced Problem in Cryptography and its Solution*, Ft. Leavenworth, 1914.

Meister, Alloys, *Die Anfänge der modernen diplomatischen Geheimschrift*, 1866.

Meister, Aloys, *Die Geheimschrift im Dienste der päpstlichen Kurie*, Paderborn, 1906.

Mengarini, *Cifrario*, Rome, 1892.

Michael, Giovanni (Venetian Ambassador to England in the reign of Queen Mary), *Dispatches Only Lately Deciphered.*

Miller, *Ludwig Heinrich*, 1662.

Montfort, *Anweisung zur Schnell- u. Geheimschrift Tachygraphie u. Cryptographie*, Berlin, 1893.

Myers, *Manual of Signals*, New York, 1872.

Myszkowski, Emile, *Cyrptographie indéchiffrable* 1902.

Niethe, *Wörterbuch von Cryptographie*, Berlin, 1877.

Palatino, M. Giovambattista, *Nel qual s'insegna a scriuere, etc.*, Rome, 1548.

Palatino, Giovambattista, *Discorso de la Cifra*, 1553.

Peters, Karl, *Die Geheimschreibekunst, oder Kryptographik*, 1856.

Phipps, Charles, *The Art of Decyphering* (In The Doctrine of Vulgar and Decimal Fractions), Dublin, 1745.

Porta, John Baptist, *De Furtivis litteraris.*

Porta, John Baptist, *De Literaris antiquis*, 1563.

Porta, J. B., *De occultis literarum notis*, 1563, 1606.

Porta, *Magiae Naturalis*, Frankfort, 1607.

Prasse, de, *De Reticulis*, Lipsiae, 1799.

Puteanus, Erycius, *Epistolae.*

Romanini, Vesin de, *La Cryptographie dévoilée*, Paris, 1857.

Romanini (?), *La crittografia svelata*, Firenze, 1858.

Schneickert, Hans, *Die Geheimschriften im Dienste des Geschäfts-und Verkehrslebens*, 1905.

Schottus, Gaspar, *Schola Steganographica*, Rome, 1665.

Selenus, Gustavus, *Cryptomenytices et Cryptographie*, 1624.

Simonetta, C., *Regles* (In Ecole des Chartres, Vol. 51, 1890), 1474.

Sittler, *Dictionnaire abbréviatif chiffré*, Paris, 1858.

Tenison, Thomas (Archbishop), *Baconiana* (Explanatory references to Biliteral Cipher, pp.-27f.), London, 1679.

Thicknesse, Phillip, *Treatise on the Art of Deciphering, and Writing in Ciphers*, 1772.

Trithemius, Johannes, *Chronologica Mystica*, 1516.

Trithemius, Johannes, *Polygraphie et universelle escriture cabalistique* (a translation into French by Gabriel de Collanges), republished Amsterdam, 1626.

Trithemius, Johannes, *Steganographia cum Clave*, Frankfort, 1551 and 1606.

Trithemius, Johannes, *Sui Ipsius Vindex*, Ingoldstadt, 1616.

Trithemius, Johannes, *Libri Polygraphiae, VI, 1606* (date on cover; title-page bears date 1600).

Trithemius, Johannes, *Steganographia Vindicata*, Col. Agrip, 1635.

Valerio, *De la Cryptographie, Part I*, Paris, 1893; *De la Cryptographie, Part II*, 1896.

Viaris, Henri, *L'Art de chiffrer et déchiffrer les dépêches secrètes*, Paris, 1893, 1895.

Vigenère, Blaise de, *Traicté des Chiffres*, Paris, 1587.

Vigenère, Blaise de, *Traicté du feu et du sel*, Paris, 1618.

Vossius, Gerardus, *De Gram.*

Walchius, Johannes, Fab. 9.

Walter, *Dechiffrir-Wörterbuch,* Winterthur, 1877.

Weker, *De Seretis.*

Wheatstone, Chas., *Scientific Papers of Sir Charles Wheatstone,* published by the Physical Society of London, 1879.

Wilkins, John (Bishop), *Mercury,* London, 1641, 1694.

Wilkins, John (Bishop), *Mathematical and Philosophical Works* (Containing Mercury), London, 1708.

Worcester, Marquis of (Edward Somerset), *Century of Inventions,* 1659.

Wostrowitz, Fleissner von, *Handbuch der Cryptographie,* Wien, 1881.

ARTICLES

Collon, A., "*Etude sur la cryptographie*" in *Revue de l'armée belge,* 1899 to 1902.

Kerckhoffs, *Le Journal des sciences militaires,* 1893.

Mamy, *le Génie civil,* 1885.

Muirhead (Col.), *Lecture in Technical Conferences of the U. S. Army Signal Schools,* 1911 to 1912; 1912 to 1913.

All The Year, Vol. XXXV, p. 506.

American Catholic Quarterly, Vol. XVIII, p. 858.

Appleton's, Vol. VII, p. 627.

Century, Vol. LXXIV, p. 290; Vol. LXXXV, p. 83.

Chamber's Journal, Vol. XX, p. 161; Vol. XXIV, p. 134; Vol. XXV, p. 175; Vol. XLIII, p. 193; Vol. XLIV, p. 70.

Cosmopolitan, Vol. XXXVI, p. 475, 584, 716.

Cornhill, Vol. XXIX, p. 172.

Craftsman, Vol. V, p. 207.

Gentleman's Magazine, N. S., Vol. LXV, p. 365.

Harper's, Vol. XCVII, p. 105.

Internation, Vol. VI, p. 405.

Knowledge, Vol. XI, p. 205; Vol. XII, p. 17.

Macmillan's, Vol. XXIII, p. 328.

Mouth, Vol. LXXXI, p. 558.

Murray's, Vol. VIII, p. 433.

North American, Vol. CXXVIII, p. 315.

Once A Week, Vol. IX, p. 607.

Practical Magazine, Vol. I, p. 314

Formulae for the Solution of Geometrical Transposition Ciphers

Publication No. 19

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Two Hundred copies of this publication were printed of which this is

No. 93

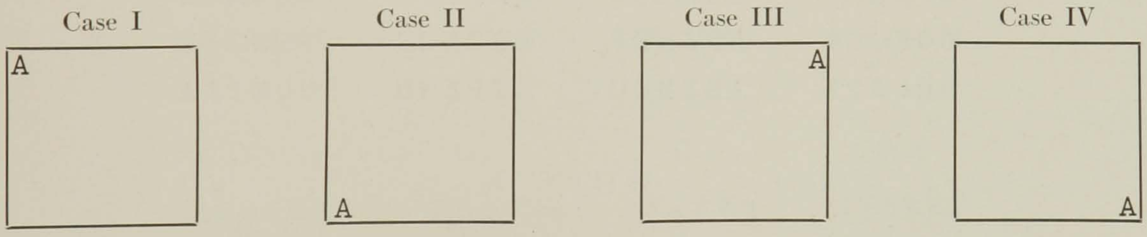
RIVERBANK
LABORATORIES
GENEVA
ILLINOIS

INTRODUCTORY

The geometrical or monoliteral transposition cipher retains the characters of the original text but rearranges the letters according to some geometrical design. It is easily distinguished from a substitution cipher by a count of certain letters which occur in normal English text with a characteristic frequency. Of the total number of letters in a message, the vowels A E I O U constitute 40%, the consonants L N R S T constitute 30%, while the consonants J K Q X Z constitute only 2%. Usually a simple inspection will determine the type of cipher encountered, for, in most substitution ciphers, an inordinately large number of low-frequency letters, such as J, X, or Z, is at once apparent.

The two systems most frequently met with in transposition ciphers are: (1) that in which the letters of the plain text are arranged in a rectangle according to a previously determined law or design, and the cipher letters taken off the horizontal lines—which shall here be known as the *Alpha System;* (2) that in which the plain text is written on the horizontal lines of the rectangle and the cipher letters taken off according to some geometrical design—which shall here be known as the *Beta System.*

The possibilities of monoliteral transposition are legion, but the standard forms usually encountered consist of simple and alternate horizontal, simple and alternate vertical, simple and alternate diagonal, and clockwise and counter clockwise spirals. Each form is further subdivided into four *cases*, depending upon the initial point of the encipherment. Case I is begun in the upper left corner, Case II in the lower left, Case III in the upper right, and Case IV in the lower right corner.



The following table gives all possible combinations of the standard forms of geometrical transpositions. It should be thoroughly understood, as frequent reference is made to it throughout the pamphlet.

HORIZONTAL

SIMPLE

I	II	III	IV
ABCDEF	STUVWX	FEDCBA	XWVUTS
GHIJKL	MNOPQR	LKJIHG	RQPONM
MNOPQR	GHIJKL	RQPONM	LKJIHG
STUVWX	ABCDEF	XWVUTS	FEDCBA

ALTERNATE

I	II	III	IV
ABCDEF	XWVUTS	FEDCBA	STUVWX
LKJIHG	MNOPQR	GHIJKL	RQPONM
MNOPQR	LKJIHG	RQPONM	GHIJKL
XWVUTS	ABCDEF	STUVWX	FEDCBA

VERTICAL

SIMPLE

I	II	III	IV
AEIMQU	DHLPTX	UQMIEA	XTPLHD
BFJNRV	CGKOSW	VRNJFB	WSOKGC
CGKOSW	BFJNRV	WSOKGC	VRNJFB
DHLPTX	AEIMQU	XTPLHD	UQMIEA

ALTERNATE

I	II	III	IV
AHIPQX	DELMTU	XQPIHA	UTMLED
BGJORW	CFKNSV	WROJGB	VSNKFC
CFKNSV	BGJORW	VSNKFC	WROJGB
DELMTU	AHIPQX	UTMLED	XQPIHA

DIAGONALS

SIMPLE

I-*a*	II-*a*	III-*a*	IV-*a*
A B D G K O	G K O S V X	O K G D B A	X V S O K G
C E H L P S	D H L P T W	S P L H E C	W T P L H D
F I M Q T V	B E I M Q U	V T Q M I F	U Q M I E B
J N R U W X	A C F J N R	X W U R N J	R N J F C A

I-*b*	II-*b*	III-*b*	IV-*b*
A C F J N R	J N R U W X	R N J F C A	X W U R N J
B E I M Q U	F I M Q T V	U Q M I E B	V T Q M I F
D H L P T W	C E H L P S	W T P L H D	S P L H E C
G K O S V X	A B D G K O	X V S O K G	O K G D B A

ALTERNATE

I-*a*	II-*a*	III-*a*	IV-*a*
A B F G N O	G N O U V X	O N G F B A	X V U O N G
C E H M P U	F H M P T W	U P M H E C	W T P M H F
D I L Q T V	B E I L Q S	V T Q L I D	S Q L I E B
J K R S W X	A C D J K R	X W S R K J	R K J D C A

I-*b*	II-*b*	III-*b*	IV-*b*
A C D J K R	J K R S W X	R K J D C A	X W S R K J
B E I L Q S	D I L Q T V	S Q L I E B	V T Q L I D
F H M P T W	C E H M P U	W T P M H F	U P M H E C
G N O U V X	A B F G N O	X V U O N G	O N G F B A

SPIRALS

CLOCKWISE

I	II	III	IV
ABCDEF	DEFGHI	LMNOPA	IJKLMN
PQRSTG	CRSTUJ	KVWXQB	HUVWXO
OXWVUH	BQXWVK	JUTSRC	GTSRQP
NMLKJI	APONML	IHGFED	FEDCBA

COUNTER CLOCKWISE

I	II	III	IV
APONML	NMLKJI	FEDCBA	IHGFED
BQXWVK	OXWVUH	GTSRQP	JUTSRC
CRSTUJ	PQRSTG	HUVWXO	KVWXQB
DEFGHI	ABCDEF	IJKLMN	LMNOPA

The solution of a transposition cipher most frequently depends upon determining the size of the rectangle in which the letters of the original text were arranged. This is accomplished by counting the total number of letters in the message as received, and then factoring. Should the message contain 150 letters, the factors 5 x 5 x 3 x 2 are obtained, suggesting a rectangle of either 10 x 15 or 6 x 25. Both of these must be tried, but the one more nearly square (10 x 15) should be experimented with first.* Having decided on a rectangle of a certain size, it has been necessary in the past to prepare, laboriously, innumerable rectangles with the different literal arrangements as given.

The following formulae offer a short cut to the solution of transposition ciphers, by giving a rapid test to each possible case, and eliminating the incorrect ones after substituting the first few letters. It is not the function of the formulae to solve the message completely, but merely to indicate which system, form, and case was used in encipherment. Having determined these facts, a rectangle may be prepared and the message read direct. The formulae are mathematical productions, giving the numerical sequence of the plain-text letters as they occur in the message. Taking each formula in turn, substitution is made until there is a break in the possible combination of letters for plain text.

In preparing the formulae the letter "X" has been used to represent the number of letters in the horizontal rows, and the letter "Y" to represent the number of letters in the vertical columns. In other words, "X" always represents the *horizontal* dimension of any assumed rectangle, and "Y" represents the *vertical* dimension. The symbol "add $1/\overline{X\text{-}3}$" has been arbitrarily coined to represent a certain expression, just as the symbol "$\surd$ " represents the expression "extract the square root of." Similarly, "add $1/\overline{X\text{-}3}$" means

*Many times a message is encountered whose total number of letters is nonfactorable—a ruse sometimes adopted for the purpose of confusing the enemy. In such a case the factorable numbers near the total number are tried. For example, a message giving a total number of 223 letters would be tested as if for 220, 225, or 230.

"add 1 for X-3 terms," and if "X" had a particular value of 10, the expression would indicate that for 10-3, or 7, terms in the formula, the quantity 1 should be added to each succeeding term. Similarly, "sub Y/$\overline{X-1}$" represents "subtract Y for X-1 terms," and "cont/$\overline{X-1}$" represents "continue the progression as indicated for X-1 terms."

Should the formula give: (with X=10, Y=6) 30 . add 1/$\overline{X-5}$. sub Y/$\overline{X-7}$, substitution would give: 30 . 31 , 32 , 33 , 34 , 35 . 29 , 23 , 17 .

This indicates that the thirtieth letter as it occurs in the message is the first letter of the original text, that the thirty-first letter of the message is the second letter of the text, etc.

The solution of a typical message will show clearly the method.

```
    5          10          15          20          25          30
VNNRV      EMTTC       LCOON       OSPUU       EPIMH       LTEEX
   35          40          45          50          55          60
EVGXO      TOREX       ORMEI       TGITH       ECOCN       VERER
   65          70          75          80          85          90
URENN      IEHXE       SSRDI       LIETS       BETHR       IIMPT
   95         100         105         110         115         120
POERA      ETUDT       ENHRO       MBTAR       OEAFD       EOETA
  125         130         135         140         145         150
CYMDR      NOYTN       UTOFE       DORRT       DUBYA       AEECT
```

The message is numbered in groups of five, and the final number (150) factored. The assumption is made that the rectangle is 10 x 15, which will give X a value of 10 and Y a value of 15, and these numbers are substituted in the formulae. Should a complete substitution fail to give a solution, other values are assumed for X and Y and the process repeated. The Simple and Alternate Horizontal, and Simple Vertical (Beta System) in all four cases give no result on substitution; so we proceed to the Alternate Vertical.

```
Case   I.    1 . 2Y . 2Y+1 . 4Y . 4Y+1 .
             1  30    31    60    61
             V   X     E     R     U

Case  II.    Y . Y+1 . 3Y . 3Y+1 . 5Y . 5Y+1 . 7Y . 7Y+1
            15  16    45    46    75    76   105  106
             N   O     I     T     I     L     O    M

Case III.    Y(X-1)+1 . Y(X-1) . Y(X-3)+1 . Y(X-3) . Y(X-5)+1 .
               136         135        106        105        76
                D           E          M          O          L

Case  IV.    Y(X-5) . Y(X-7)+1 . Y(X-7) . Y(X-9)+1 . Y(X-9) .
               75          46         45         16         15
                I           T          I          O          N
```

(Note: The formulae for Cases III and IV, Alternate Vertical, are identical, but a trial proves Case IV.)

The word "DEMOLITION" appears and the method of encipherment is determined as Beta System, Alternate Vertical, Case IV. It is only necessary to carry the substitution in the formulae to the point where either the letters break, or where plain text is evident. In Case I it becomes evident at once that plain text will not ensue, but substitution may be carried on to five terms, to catch a possible error in the message. Case II does not break until the eighth term.

The rectangle may now be prepared, and the message taken direct from the horizontal lines.

```
DEMOLITION
OFBRIDGESO
ROTHERIMPO
RTANTSTRUC
TURESSHOUL
DNOTBEEXEC
UTEDEXCEPT
BYAUTHORIT
YOFTHECOMM
ANDERINTHE
AREAINVOLV
EDORINEXTR
EMEEMERGEN
CYTOPREVEN
TCAPTUREXV
```

DEMOLITION OF BRIDGES OR OTHER IMPORTANT STRUCTURES SHOULD NOT BE EXECUTED EXCEPT BY AUTHORITY OF THE COMMANDER IN THE AREA INVOLVED OR IN EXTREME EMERGENCY TO PREVENT CAPTURE.

Had the message been enciphered by the Alpha System, it would have appeared and been solved as follows:

```
RPNIHTSSDI
EOVAOUHEGR
VTOERAOREB
EYLRIYUUSF
NCVATBLTOO
TNEEYTDCRN
CEDHOPNUOO
AGOTFEORTI
PRRNTCTTHT
TEIIHXBSEI
UMNREEETRL
REEECDENIO
EEXDOEXAMM
XMTNMTETPE
VERAMUCROD
```

```
    5        10        15        20        25
RPNIH     TSSDI     EOVAO     UHEGR     VTOER

   30        35        40        45        50
AOREB     EYLRI     YUUSF     NCVAT     BLTOO

   55        60        65        70        75
TNEEY     TDCRN     CEDHO     PNUOO     AGOTF

   80        85        90        95       100
EORTI     PRRNT     CTTHT     TEIIH     XBSEI

  105       110       115       120       125
UMNRE     EETRL     REEEC     DENIO     EEXDO

  130       135       140       145       150
EXAMM     XMTNM     TETPE     VERAM     UCROD
```

(Alpha System, Alternate Vertical, Case IV.)

```
XY.X(Y-1).X(Y-2).X(Y-3). cont/Y-4
150   140     130     120     110    100    90    80    70    60
 D     E       M       O       L      I      T     I     O     N
```

Before substituting from the formulae it is well to prepare a table of the following terms, using the assumed values of X and Y to obtain their equivalents. The formulae consist entirely of these terms, so once having obtained their values, substitution may be made without duplication of work, and with only the simplest mental arithmetic.

```
 X=           X(Y-1)=
2X=           X(Y-2)=
3X=           X(Y-3)=
4X=           X(Y-4)=
5X=           X(Y-5)=
 Y=
2Y=           Y(X-1)=
3Y=           Y(X-2)=
4Y=           Y(X-3)=
5Y=           Y(X-4)=
XY=           Y(X-5)=
```

FORMULAE—ALPHA SYSTEM

SIMPLE HORIZONTAL

CASE I

(1) Will read plain text.

CASE II

(2) $X(Y-1)+1$. add $1/\overline{X-1}$. $X(Y-2)+1$. add $1/\overline{X-1}$. $X(Y-3)+1$. add $1/\overline{X-1}$.

CASE III

(3) X . sub $1/\overline{X-1}$. $2X$. sub $1/\overline{X-1}$. $3X$. sub $1/\overline{X-1}$.

CASE IV

(4) XY . sub $1/\overline{X-1}$. $X(Y-1)$. sub $1/\overline{X-1}$. $X(Y-2)$. sub $1/\overline{X-1}$.

ALTERNATE HORIZONTAL

CASE I

(5) 1 . add $1/\overline{X-1}$. $2X$. sub $1/\overline{X-1}$. $2X+1$. add $1/\overline{X-1}$.

CASE II

(6) $X(Y-1)+1$. add $1/\overline{X-1}$. $X(Y-1)$. sub $1/\overline{X-1}$. $X(Y-3)+1$. add $1/\overline{X-1}$.

CASE III

(7) X . sub $1/\overline{X-1}$. $X+1$. add $1/\overline{X-1}$. $3X$. sub $1/\overline{X-1}$.

CASE IV

(8) XY . sub $1/\overline{X-1}$. $X(Y-2)+1$. add $1/\overline{X-1}$. $X(Y-2)$. sub $1/\overline{X-1}$.

SIMPLE VERTICAL

CASE I

(9) 1 . $X+1$. $2X+1$. $3X+1$. cont/$\overline{Y-4}$. 2 . $X+2$. $2X+2$. $3X+2$. cont/$\overline{Y-4}$.

CASE II

(10) $X(Y-1)+1$. $X(Y-2)+1$. $X(Y-3)+1$. cont/$\overline{Y-3}$. $X(Y-1)+2$. $X(Y-2)+2$. $X(Y-3)+2$ .cont/$\overline{Y-3}$.

CASE III

(11) X . 2X . 3X . cont/$\overline{Y-3}$. X-1 . 2X-1 . 3X-1 . cont/$\overline{Y-3}$.

CASE IV

(12) XY . X(Y-1) . X(Y-2) . X(Y-3) . cont/$\overline{Y-4}$. (XY)-1 . X(Y-1)-1 .
X(Y-2)-1 . X(Y-3)-1 . cont/$\overline{Y-4}$.

ALTERNATE VERTICAL

CASE I

(13) 1 . X+1 . 2X+1 . 3X+1 . cont/$\overline{Y-4}$. X(Y-1)+2 . X(Y-2)+2 .
X(Y-3)+2 . cont/$\overline{Y-3}$.

CASE II

(14) X(Y-1)+1 . X(Y-2)+1 . X(Y-3)+1 . cont/$\overline{Y-3}$. 2 . X+2 . 2X+2 .
3X+2 . cont/$\overline{Y-4}$.

CASE III

(15) X . 2X . 3X . cont/$\overline{Y-3}$. (XY)-1 . X(Y-1)-1 . X(Y-2)-1 .
X(Y-3)-1 . cont/$\overline{Y-4}$.

CASE IV

(16) XY . X(Y-1) . X(Y-2) . X(Y-3) . cont/$\overline{Y-4}$. X-1 . 2X-1 . 3X-1 .
cont/$\overline{Y-3}$.

SIMPLE DIAGONAL

CASE I-*a*†

(17) 1 . 2 . X+1 . 3 . X+2 . 2X+1 . 4 . X+3 . 2X+2 . 3X+1 .

CASE II-*a*

(18) X(Y-1)+1 . X(Y-2)+1 . X(Y-1)+2 . X(Y-3)+1 . X(Y-2)+2 .
X(Y-1)+3 . X(Y-4)+1 . X(Y-3)+2 . X(Y-2)+3 . X(Y-1)+4 .

CASE III-*a*

(19) X . X-1 . 2X . X-2 . 2X-1 . 3X . X-3 . 2X-2 . 3X-1 . 4X . X-4 .

CASE IV-*a*

(20) XY . X(Y-1) . (XY)-1 . X(Y-2) . X(Y-1)-1 . (XY)-2 . X(Y-3) .
X(Y-2)-1 . X(Y-1)-2 . (XY)-3 .

†Note carefully the distinctions of the *a* and *b* forms in diagonal transpositions, as given in the table on page 7.

CASE I-*b*

(21) 1 . X+1 . 2 . 2X+1 . X+2 . 3 . 3X+1 . 2X+2 . X+3 . 4 .

CASE II-*b*

(22) X(Y-1)+1 . X(Y-1)+2 . X(Y-2)+1 . X(Y-1)+3 . X(Y-2)+2 .
X(Y-3)+1 . X(Y-1)+4 . X(Y-2)+3 . X(Y-3)+2 . X(Y-4)+1 .

CASE III-*b*

(23) X . 2X . X-1 . 3X . 2X-1 . X-2 . 4X . 3X-1 . 2X-2 . X-3 .

CASE IV-*b*

(24) XY . (XY)-1 . X(Y-1) . (XY)-2 . X(Y-1)-1 . X(Y-2) . (XY)-3 .
X(Y-1)-2 . X(Y-2)-1 . X(Y-3) .

ALTERNATE DIAGONAL

CASE I-*a*

(25) 1 . 2 . X+1 . 2X+1 . X+2 . 3 . 4 . X+3 . 2X+2 . 3X+1 .

CASE II-*a*

(26) X(Y-1)+1 . X(Y-2)+1 . X(Y-1)+2 . X(Y-1)+3 . X(Y-2)+2 .
X(Y-3)+1 . X(Y-4)+1 . X(Y-3)+2 . X(Y-2)+3 . X(Y-1)+4 .

CASE III-*a*

(27) X . X-1 . 2X . 3X . 2X-1 . X-2 . X-3 . 2X-2 . 3X-1 . 4X .

CASE IV-*a*

(28) XY . X(Y-1) . (XY)-1 . (XY)-2 . X(Y-1)-1 . X(Y-2) . X(Y-3) .
X(Y-2)-1 . X(Y-1)-2 . (XY)-3 .

CASE I-*b*

(29) 1 . X+1 . 2 . 3 . X+2 . 2X+1 . 3X+1 . 2X+2 . X+3 . 4 .

CASE II-*b*

(30) X(Y-1)+1 . X(Y-1)+2 . X(Y-2)+1 . X(Y-3)+1 . X(Y-2)+2 .
X(Y-1)+3 . X(Y-1)+4 . X(Y-2)+3 . X(Y-3)+2 . X(Y-4)+1 .

CASE III-*a*

(31) X . 2X . X-1 . X-2 . 2X-1 . 3X . 4X . 3X-1 . 2X-2 . X-3 .

CASE IV-*b*

(32) XY . (XY)-1 . X(Y-1) . X(Y-2) . X(Y-1)-1 . (XY)-2 . (XY)-3 .
X(Y-1)-2 . X(Y-2)-1 . X(Y-3) . X(Y-4) .

SPIRAL CLOCKWISE

CASE I

(33) 1 . add $1/\overline{X-1}$. 2X . 3X . add $X/\overline{Y-3}$. sub $1/\overline{X-1}$.

CASE II

(34) X(Y-1)+1 . X(Y-2)+1 . X(Y-3)+1 . cont$/\overline{Y-4}$. 1 . add $1/\overline{X-1}$.

CASE III

(35) X . 2X . add $X/\overline{Y-2}$. sub $1/\overline{X-1}$. X(Y-2)+1 . X(Y-3)+1 .
X(Y-4)+1 . cont$/\overline{Y-5}$. 1 . add $1/\overline{X-2}$.

CASE IV

(36) XY . sub $1/\overline{X-1}$. X(Y-2)+1 . X(Y-3)+1 . X(Y-4)+1 . cont$/\overline{Y-4}$.
add $1/\overline{X-1}$.

SPIRAL COUNTER CLOCKWISE

CASE I

(37) 1 . X+1 . 2X+1 . 3X+1 . cont$/\overline{Y-4}$. add $1/\overline{X-1}$.

CASE II

(38) X(Y-1)+1 . add $1/\overline{X-1}$. X(Y-1) . X(Y-2) . X(Y-3) . cont$/\overline{Y-4}$.
sub $1/\overline{X-1}$.

CASE III

(39) X . sub $1/\overline{X-1}$. X+1 . 2X+1 . 3X+1 . cont$/\overline{Y-4}$. add $1/\overline{X-1}$.

CASE IV

(40) XY . X(Y-1) . X(Y-2) . X(Y-3) . cont$/\overline{Y-4}$. sub $1/\overline{X-1}$.

BETA SYSTEM

SIMPLE HORIZONTAL

CASE I

(41) Will read plain text.

CASE II

(42) $X(Y-1)+1$. add $1/\overline{X-1}$. $X(Y-2)+1$. add $1/\overline{X-1}$. $X(Y-3)+1$.
add $1/\overline{X-1}$.

CASE III

(43) X . sub $1/\overline{X-1}$. $2X$. sub $1/\overline{X-1}$. $3X$. sub $1/\overline{X-1}$.

CASE IV

(44) XY . sub $1/\overline{X-1}$. $X(Y-1)$. sub $1/\overline{X-1}$. $X(Y-2)$. sub $1/\overline{X-1}$.
$X(Y-3)$. sub $1/\overline{X-1}$.

ALTERNATE HORIZONTAL

CASE I

(45) 1 . add $1/\overline{X-1}$. $2X$. sub $1/\overline{X-1}$. $2X+1$. add $1/\overline{X-1}$. $4X$. sub $1/\overline{X-1}$.

CASE II (Y EVEN)

(46) XY . sub $1/\overline{X-1}$. $X(Y-2)+1$. add $1/\overline{X-1}$. $X(Y-2)$. sub $1/\overline{X-1}$.

CASE II (Y ODD)

(47) $X(Y-1)+1$. add $1/\overline{X-1}$. $X(Y-1)$. sub $1/\overline{X-1}$. $X(Y-3)+1$.
add $1/\overline{X-1}$.

CASE III

(48) X . sub $1/\overline{X-1}$. $X+1$. add $1/\overline{X-1}$. $3X$. sub $1/\overline{X-1}$. $3X+1$.
add $1/\overline{X-1}$. $5X$.

CASE IV (Y EVEN)

(49) $X(Y-1)+1$. add $1/\overline{X-1}$. $X(Y-1)$. sub $1/\overline{X-1}$. $X(Y-3)+1$.
add $1/\overline{X-1}$. $X(Y-3)$. sub $1/\overline{X-1}$. (Same as Case II, when Y is odd.)

CASE IV (Y ODD)

(50) XY . sub $1/\overline{X-1}$. $X(Y-2)+1$. add $1/\overline{X-1}$. $X(Y-2)$. sub $1/\overline{X-1}$.
(Same as Case II, when Y is even.)

SIMPLE VERTICAL

CASE I

(51) 1 . add $Y/\overline{X-1}$. 2 . add $Y/\overline{X-1}$. 3 . add $Y/\overline{X-1}$.

CASE II

(52) Y . add $Y/\overline{X-1}$. Y-1 . add $Y/\overline{X-1}$. Y-2 . add $Y/\overline{X-1}$.

CASE III

(53) Y(X-1)+1 . sub $Y/\overline{X-1}$. Y(X-1)+2 . sub $Y/\overline{X-1}$. Y(X-1)+3 .
sub $Y/\overline{X-1}$.

CASE IV

(54) XY . sub $Y/\overline{X-1}$. (XY)-1 . sub $Y/\overline{X-1}$. (XY)-2 . sub $Y/\overline{X-1}$.

ALTERNATE VERTICAL

CASE I

(See Notes)

(55) 1 . 2Y . 2Y+1 . 4Y . 4Y+1 . 6Y . 6Y+1 . cont/$\overline{X-7}$. 2 . 2Y-1 . 2Y+2 .
4Y-1 .

CASE II

(56) Y . Y+1 . 3Y . 3Y+1 . 5Y . 5Y+1 . cont/$\overline{X-6}$. Y-1 . Y+2 . 3Y-1 . 3Y+2 .
5Y-1 .

CASE III (X ODD)

(57) Y(X-1)+1 . Y(X-1) . Y(X-3)+1 . Y(X-3) . Y(X-5)+1 . Y(X-5) .
cont/$\overline{X-6}$.

CASE III (X EVEN)

(58) XY . Y(X-2)+1 . Y(X-2) . Y(X-4)+1 . Y(X-4) . Y(X-6)+1 .
Y(X-6) . cont/$\overline{X-7}$.

CASE IV (X ODD)

(59) XY . Y(X-2)+1 . Y(X-2) . Y(X-4)+1 . Y(X-4) . Y(X-6)+1 .
Y(X-6) . cont/$\overline{X-7}$. (Same as Case III, where X is even.)

CASE IV (X EVEN)

(60) Y(X-1)+1 . Y(X-1) . Y(X-3)+1 . Y(X-3) . Y(X-5)+1 . Y(X-5) .
cont/$\overline{X-6}$. (Same as Case III, where X is odd.)

SPIRAL CLOCKWISE

CASE I

(61) 1 . 2 . add $1/\overline{X-2}$. 2X+2Y-4 . 2X+2Y-3 . add $1/\overline{X-3}$. X+1 .

CASE II

(62) Y . add $1/\overline{X-1}$. Y-1 . 2X+3Y-6 . add $1/\overline{X-3}$. X+Y . Y-2 . 2X+3Y-7 .

CASE III

(63) 2Y+X-2 . add $1/\overline{X-2}$. 1 . 2Y+X-3 . 4Y+3X-12 . add $1/\overline{X-4}$.
2Y+2X-3 . 2 . 2Y+X-4 . 4Y+3X-13 .

CASE IV

(64) X+Y-1 . add $1/\overline{X-1}$. X+Y-2 . 3X+3Y-9 . add $1/\overline{X-3}$.

SPIRAL COUNTER CLOCKWISE

CASE I

(65) 1 . 2X+2Y-4 . sub $1/\overline{X-2}$. 2 . 2X+2Y-3 . 4X+4Y-16 . sub $1/\overline{X-4}$.
X+2Y-3 . 3 . 2X+2Y-2 .

CASE II

(66) 2X+Y-2 . sub $1/\overline{X-1}$. 2X+Y-1 . 4X+3Y-12 . sub $1/\overline{X-3}$. X+Y-2 .
2X+Y .

CASE III

(67) X . sub $1/\overline{X-1}$. X+1 . 3X+2Y-6 . sub $1/\overline{X-2}$. X+2 . 3X+2Y-5 .

CASE IV

(68) X+Y-1 . sub $1/\overline{X-1}$. X+Y . 3X+3Y-9 . sub $1/\overline{X-3}$. Y-1 . X+Y+1 .
3X+3Y-8 .

RAIL FENCE

ALPHA SYSTEM

CASE I

(69) X+1 . 1 . X+2 . 2 . X+3 . 3 . cont.

CASE II

(70) 1 . X+1 . 2 . X+2 . 3 . X+3 . cont.

BETA SYSTEM

CASE I

(71) 1 . 3 . 5 . 7 . cont$/\overline{X-4}$. 2 . 4 . 6 . 8 . cont.

CASE II

(72) 2 . 4 . 6 . 8 . cont$/\overline{X-4}$. 1 . 3 . 5 . 7 . cont.

VERTICAL WRITING

(73) 1 . 3 . 5 . 7 . cont$/\overline{Y-4}$. 2 . 4 . 6 . 8 . cont.

It was found more convenient to solve the simple and alternate diagonal forms of the Beta System by a series of tables than by formulae. The values in the tables will hold true for a number of terms equal to the smaller value of X or Y. That is, if the rectangle is assumed to be 10 x 15, then the first 10 terms in the table indicated will produce the original sequence of letters of the text. Should the rectangle be 6 x 25, then only the first 6 values in the table will produce plain text. In Cases III and IV, it is necessary to begin at the smaller value of X or Y in the table indicated and take the constantly diminishing numbers from the table. That is, if the rectangle is 10 x 15, the first letter of the text will be the value for 10 in the table, the second letter of text will be the value for 9, third for 8, fourth for 7, etc. In the cases noted the table will produce plain text at the end of the message instead of at the beginning. Two examples should make the use of the tables perfectly clear.

```
BURN THE BRIDGE BEFORE THE ENEMY CAVALRY REACHES
   THE TOWN.
                                  BURNTHE
                                  BRIDGEB
                                  EFORETH
                                  EENEMYC
                                  AVALRYR
                                  EACHEST
                                  HETOWNX
```

Case I-*a*, Simple Diagonal:

```
    5          10          15          20          25
BUBRR       ENIFE       TDOEA       HGRNV       EEEEE
   30          35          40          45          50
AAHBT       MLCEH       YRHTC       YEORS       WTNXX
```

Table A:

1	2	4	7	11	16	22
B	U	R	N	T	H	E

Case IV-*b*, Alternate Diagonal:

```
    5          10          15          20          25
XNTRS       WOEYC       HYRHT       ECLMT       BEEEE
   30          35          40          45          50
AAHEV       NRGHT       DOEAE       FINRR       EBUBX
```

Table G:

28	16	15	7	6	2	1
H	E	T	O	W	N	X

It will frequently happen that the first letters produced by the table will *not be the initial or ending letters of the message, but they will form possible combinations* and should be tested.

	A	B
1	1	1
2	2	3
3	4	6
4	7	10
5	11	15
6	16	21
7	22	28
8	29	36
9	37	45
10	46	55
11	56	66
12	67	78
13	79	91
14	92	105
15	106	120
16	121	136
17	137	153
18	154	171
19	172	190
20	191	210
21	211	231
22	232	253
23	254	276
24	277	300

TAKE ALL VALUES IN THIS DIRECTION: ↓

SIMPLE DIAGONAL

Case I-*a*. Table A (beginning of message). To smaller value of X or Y.

Case I-*b*. Table B (beginning of message). To smaller value of X or Y.

Case II-*a*. Table B (end of message). To smaller value of X or Y.

Case II-*b*. Table A (end of message). To smaller value of X or Y.

Case III-*a*. Table C (beginning of message). Start at smaller value of X or Y.

Case III-*b*. Table D (beginning of message). Start at smaller value of X or Y.

Case IV-*a*. Table D (end of message). Start at smaller value of X or Y.

Case IV-*b*. Table C (end of message). Start at smaller value of X or Y.

	C	D
24	277	300
23	254	276
22	232	253
21	211	231
20	191	210
19	172	190
18	154	171
17	137	153
16	121	136
15	106	120
14	92	105
13	79	91
12	67	78
11	56	66
10	46	55
9	37	45
8	29	36
7	22	28
6	16	21
5	11	15
4	7	10
3	4	6
2	2	3
1	1	1

TAKE ALL VALUES IN THIS DIRECTION: ↓

ALTERNATE DIAGONAL

	E	F
1	1	1
2	2	3
3	6	4
4	7	10
5	15	11
6	16	21
7	28	22
8	29	36
9	45	37
10	46	55
11	66	56
12	67	78
13	91	79
14	92	105
15	120	106
16	121	136
17	153	137
18	154	171
19	190	172
20	191	210
21	231	211
22	232	253
23	276	254
24	277	300

TAKE ALL VALUES IN THIS DIRECTION: ↓

Case I-*a*. Table E (beginning of message). To smaller value of X or Y.

Case I-*b*. Table F (beginning of message). To smaller value of X or Y.

Case II-*a*. Table F (end of message). To smaller value of X or Y.

Case II-*b*. Table E (end of message). To smaller value of X or Y.

Case III-*a*. Table G (beginning of message). Start at smaller value of X or Y.

Case III-*b*. Table H (beginning of message). Start at smaller value of X or Y.

Case IV-*a*. Table H (end of message). Start at smaller value of X or Y.

Case IV-*b*. Table G (end of message). Start at smaller value of X or Y.

TAKE ALL VALUES IN THIS DIRECTION: ↓

	G	H
24	277	300
23	276	254
22	232	253
21	231	211
20	191	210
19	190	172
18	154	171
17	153	137
16	121	136
15	120	106
14	92	105
13	91	79
12	67	78
11	66	56
10	46	55
9	45	37
8	29	36
7	28	22
6	16	21
5	15	11
4	7	10
3	6	4
2	2	3
1	1	1

ROUTE CIPHERS

In route ciphers the normal sequence of the words of the message is broken, entire words being transposed and arranged according to some pre-determined geometrical design. The formulae as given apply with equal accuracy and facility to ciphers of this type as to the monoliteral transpositions. It is only necessary to consider the values derived from substitution in the formulae, or from the tables, as applying to whole words, instead of single letters.

THE OBJECT OF THE DEMOLITION CAN ONLY BE PROPERLY ATTAINED THROUGH AN ACCURATE GRASP OF THE TACTICAL SITUATION. IT IS UNPARDONABLE TO COMPLETELY WRECK A LINE OF COMMUNICATION WHICH FRIENDLY TROOPS MAY REQUIRE IN THE NEAR FUTURE. IT IS LIKEWISE UNPARDONABLE TO FAIL TO WRECK COMPLETELY A LINE OF COMMUNICATION THAT IS CERTAIN TO PASS INTO HOSTILE CONTROL FOR A LONG PERIOD OF TIME.

The above message contains 64 words and suggests a rectangle 8x8. They are arranged into such a figure according to the Beta System, and taken off for the cipher as Alternate Diagonal, Case III-*b*. The message would be sent as follows:

```
                    5                                          10
     BE THE ONLY CAN OF WRECK MAY COMPLETELY GRASP DEMOLITION THE
                          15                                   20
ACCURATE TO TROOPS LIKEWISE LINE IS FRIENDLY UNPARDONABLE AN OF
                    25                 30
OBJECT THROUGH IS WHICH IT A INTO TIME PASS COMPLETELY FUTURE
                   35                                      40
COMMUNICATION IT ATTAINED THE PROPERLY SITUATION OF NEAR WRECK TO
                 45                              50                 55
OF PERIOD CERTAIN TO THE LINE TACTICAL A IN FAIL IS LONG A THAT TO
                            60
REQUIRE UNPARDONABLE COMMUNICATION FOR CONTROL OF HOSTILE.
```

On receiving the above message, the words are numbered in groups of five, and an assumption is made as to the size of rectangle used in enciphering, based on the largest factors of the total number of words in the message. Substitution is made in the formulae in sequence until a possible combination of words for plain text appears. This determines the method of encipherment. The correct rectangle is then prepared and the message read direct.

Table F gives us the following sequence for Alternate Diagonal, Case III-*b* (Beta System):

```
 36    22     21  11      10       4    3    1
THE  OBJECT  OF  THE  DEMOLITION  CAN  ONLY  BE
```

NOTES

The formulae as given are particularly useful in solving large rectangles, and while in general they hold true for all sizes, care should be taken in considering the accuracy of over six terms in rectangles having four letters or less to a side. The formulae will hold true for the number of terms given for all rectangles having a least dimension of five. However, in many cases the formulae will hold true for the entire message, which may therefore be solved without preparing a single rectangle; but this is outside of their expressed function, which is merely to test for the case used.

In cases where there was a certain progression noted by the symbol "cont/$\overline{\text{X-7}}$," it was necessary to develop as many as seven terms to show the exact character of the progression (Beta System, Alternate Vertical, Case I, for instance). Should the value of X be less than the number of terms developed, then those beyond X should be discarded and the next term beyond the progression taken up. This justifies itself mathematically; for should X = 5 then the expression "cont/$\overline{\text{X-7}}$" would solve "cont/$\overline{\text{-2}}$," which indicates that the progression has been carried two terms beyond the term intended.

The tables as given for the solution of the Diagonals of the Beta System offer a means of determining the size of the rectangle used in encipherment, if it happens to be enciphered by the systems covered by the tables. It was stated that the sequence as given in the tables would hold true only for a number of terms equal to the least dimension of the rectangle used. If substitution was made from the tables, and plain text developed to a certain point and broke, then the number of letters in the unbroken text is one dimension of the rectangle.

D E M O L I T I O N Z V H R L

It is evident from the above that the text breaks at the end of the word DEMOLITION, hence one side of the rectangle must have a dimension of 10, and if the message contains 150 letters, the other dimension must be 15.

It has been previously suggested that there are almost unlimited possibilities for complicating transposition. A few of these will be given. In addition to the relatively simple Alpha and Beta Systems, where either the text or the cipher message is taken from horizontal lines, it is possible to place the letters of the text into the rectangle according to one system, for instance, alternate diagonal, and take the cipher letters off according to another, for example, alternate vertical. This includes all possible combinations of the standard forms. More complicated geometrical designs than those given may be devised, such as:

1	5	9	13	2
16	17	21	18	6
12	24	25	22	10
8	20	23	19	14
4	15	11	7	3

Instead of a single large rectangle a message may be broken up into several smaller rectangles, each enciphered by a different system. In general, the formulae will result in plain text for a portion of the message in this case, and with such a clue, the method may be readily determined. Nulls are frequently introduced into transposition ciphers; in groups at the beginning or end or systematically throughout the message. The former may be overcome by discarding letters from the first line or so at either the beginning or end of the message, and the latter by fully developing any system that gives text for a portion and then breaks.

Since there are certain letters in English text that rarely begin or end a word, it is possible to obtain a clue as to the case used in encipherment by noting the initial and final letters of the message as received. The most frequent initial letters in English are TAWIBCDSR in the order named, and the most common endings of words are ETDSNRY in the order given. It is rare that a word begins with XJKZQ, or ends with QJZVXIB. This data may be combined with the possible beginnings and endings of the standard forms, and much time saved in employing the formulae. This information should not be taken other than as an indication, but it is sufficient evidence to put off substitution in a certain case of the formulae until all other cases have been tried.

It will be noticed that in the Alpha System the first letter of the cipher message as received is the initial letter of the original text in all Cases I; and that in the Beta System the last letter of the text is the first letter of the cipher in Case IV. Hence should the first cipher letter be Q, the message could not have been enciphered by any Case IV, Beta System.

Several Machine Ciphers
and
Methods for their Solution

Publication No. 20

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Two Hundred copies of this publication were printed of which this is

No. 91

RIVERBANK
LABORATORIES

GENEVA
ILLINOIS

CONTENTS

I. INTRODUCTORY

GENERAL REMARKS

It may be said that there are two great classes of military field ciphers: (1) those which require for enciphering and deciphering nothing more than pencil and paper; and (2) those which require additional apparatus, usually a machine or an instrument.

In order to conform to the important requirements of a field cipher, as laid down by Kerckhoffs, ciphers belonging to the first class must be relatively simple in construction, for the operations must be easy to remember and to perform, and must be such as to reduce to a minimum the many errors which are inevitably connected with cryptographic procedure. For this reason, ciphers of this class afford little safety against attacks of the expert decipherer even when the system is unknown to him. But as regards the second class, since the internal operations of the machine are not dependent upon the encipherer, cryptograms of this class may rise to a degree of complexity which is limited only by practicability—practicability in cipher apparatus or devices being defined by the rapidity with which they may be used, the improbability of and safeguards against errors, and the ease with which the apparatus or machine may be carried about.

At one time it was thought that so long as the apparatus or the system for enciphering could be kept secret, a high degree of safety was attained. But to-day, when it is many times possible to solve a machine cipher without any knowledge of the machine, and furthermore, when it must be admitted that no system or device can be kept secret for any length of time, the greatest of all essentials for a system adapted for regular service is that it should be such that even with a complete knowledge of all the details of the system, including the alphabets, a single message or a series of messages in the same alphabets and key should resist the efforts of the enemy's decipherers for so long that the knowledge gained through their solution, even when achieved, will be absolutely valueless.

The fact that the internal complexity of a machine would be no obstacle to the use of the machine, so long as the actual operation of enciphering and deciphering is simple, has led to many attempts on the part of both the layman and the expert to devise such machines. Those which have been invented by the laity we may pass over in a few words as hardly being worthy of serious consideration, because a system or a device which may appear safe and practical to the average layman usually appears simple and impractical to the cipher expert.

In the pages which follow we shall take up several machine ciphers which have been devised and shall attempt to give an exposition of their relative merits and defects.

DISK CIPHERS

The disk cipher has ever been a favorite form. Within one short chapter of his excellent book Gioppi[1] describes four different cipher devices, each in form a disk. Of

[1] *La Crittografia*, Milan, 1897. See Capitolo III.

these, the last, which he attributes to De Viaris, is a marvel indeed, for it prints the letters as they are enciphered!

Another is a disk arrangement for the well-known four-alphabet number cipher, which, of course, is susceptible to the simplest methods for solution, though the disk itself be entirely unknown, since a frequency table of any message would at once cause the E's, and the RST and NO sequences to stand out prominently. This device is illustrated in Fig. 1.

Still another, the Pasanisi Disk shown in Fig. 2, is also capable of solution without knowledge of the apparatus. The outer disk of this device contains 36 characters—the normal alphabet, followed by numbers 1 to 9 and an interrogation point. The inner disk contains the same 36 characters, but the sequence of the outer disk is here reversed, and in addition, is separated into six equal parts or sectors, each bearing its respective number, whose order may be changed at will by the correspondents by means of a key. The letters of a message are then enciphered by numbers or letters indifferently, since the inner disk is supposed to revolve one space after each letter, or after a definite number of letters, or according to any other plan which is previously agreed upon. A message enciphered by this device presents a somewhat curious appearance at first, for numbers and the interrogation point intermingle with letters in apparently no systematic manner. However, a solution may be obtained, after a little experimentation, by using two sliding strips, one containing the 36 characters in normal sequence, and the other, the same in reverse order. By trying different intervals of sliding or moving the second strip, some words of the clear text will be certain to appear, on account of the sequence being unbroken within the groups of six. With trial for further text the reversed alphabet is then broken and rearranged as required, and the solution is achieved.

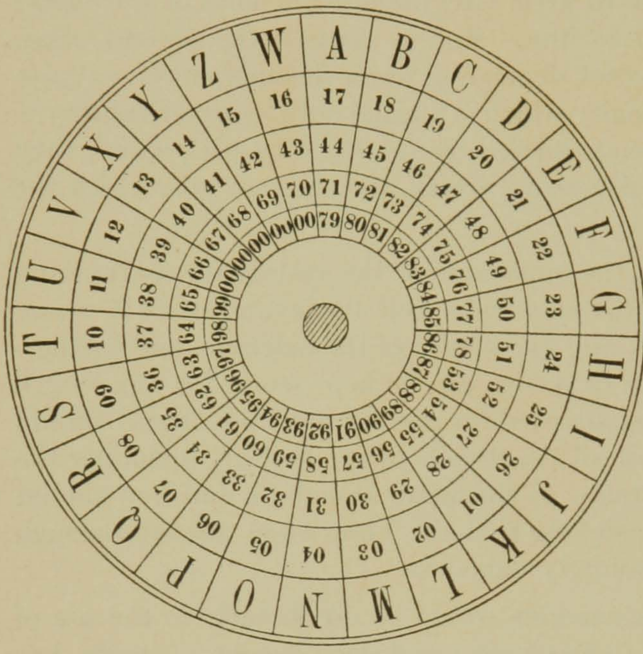


Fig. 1

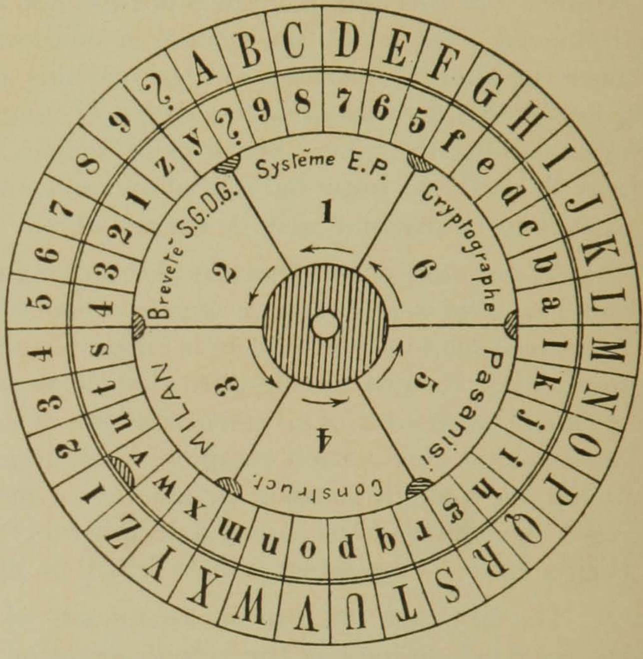

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 ?
Systeme E.P
Cryptographe
Pasanisi
Constructeur
MILAN
Breveté S.G.D.G.
1
2
3
4
5
6

Fig. 2

Indeed, it may be said that many ciphers generated by very complicated cipher machines may be solved with no knowledge of the mechanism involved, and by the use of nothing more than two strips of paper which may be slid against each other.

A device of just such a character whose apparent complexity dissolves into nothing on close study, is the device of M. Charles Gavrelle—"Cryptographe Chiffreur de M. Gavrelle"—described by Bazeries,[1] and shown in the accompanying Fig. 3.

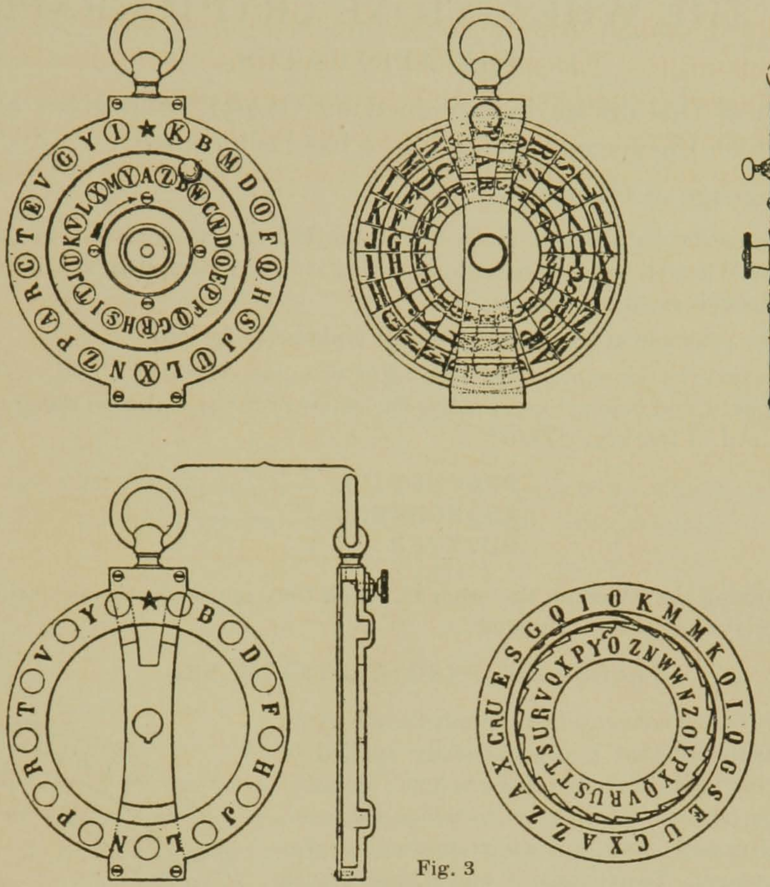


Fig. 3

Here, the apparatus makes use of double-faced revolving disks, the one side showing two, the other three alphabets. The three alphabets (direct) are used only to set, by means of a key word, the alphabets on the reverse side (which are made up by joining a fixed straight sequence with one which is movable and mixed, therefore partaking of both the character of mixed, and also of straight alphabets). Then the letters of a second key word determine when and where the revolutions shall be made. If these revolutions are made periodically, the number of alphabets can be determined by factoring, and the message solved, without knowledge of the device itself, by the frequency method. If, however, the alphabets determined by the letters of the key word are used a-periodically, solution becomes no more than a case of experimentation with the alphabets to find the point of change from one to the next.[2]

[1] *Les Chiffres Secrets Dévoilés,* Paris, 1901, pages 128-139.

[2] See the method given on page 14 for finding recurrences and placing portions of the cipher text.

Another device, more ingenious, and one which also takes the form of a disk, was called "The Cryptograph," invented by Sir Charles Wheatstone, the eminent English scientist and mathematician. The device embodies some very valuable principles. We shall here take up the solution of messages enciphered by means of this device, for to our knowledge, the method has nowhere been recorded.

II. THE WHEATSTONE CRYPTOGRAPH

1. THE APPARATUS

The mechanism of this device is explained by Gioppi,[1] who gives an illustration of the machine from which the accompanying Fig. 4 has been copied.

Quoting the language of Gioppi:

> Colonel Laussedat in a report made before the Military Commission in the Paris Exposition 1867, describes the Wheatstone Cryptograph, declaring it to be indecipherable (in which he is mistaken, in the opinion of some experts). He says:
>
> "Here is the principle upon which the cipher alphabet is formed:
>
> Any word may be chosen as the key. For example, PROJECTILE. This word is written with the letters spaced, and below it are written the letters of the alphabet in their regular order omitting the letters contained in the key. Thus:
>
> ```
> PROJECTILE
> ABDFGHKMNQ
> SUVXYZW
> ```
>
> Then by taking the letters in the order in which they appear in the successive columns, the following conventional alphabet is obtained:[2]
>
> ```
> PASRBUODVJFXEGYCHZTKWIMLNEQ
> ```
>
> The letters of the conventional alphabet are written on a circle of cardboard that is concentrically applied to a metal disk having at its circumference a regular alphabet completed by the termination sign +, to which the encipherer returns after each word, but which does not appear in the cipher message. Two hands, 1 and 2, are moved simultaneously on the double disk but with different speeds, according to such a law as to bring the first hand above the letter B whereupon the second hand does not go to the same letter, that is V, as shown in the figure, but to another letter of the internal disk. When it is desired to encipher a letter, the large hand is advanced to the place occupied by such a letter in the normal alphabet and the letter at which the small hand stops in the conventional alphabet is taken. Therefore, the system contains two keys: the disposition of the cryptographic alphabet and the starting point."

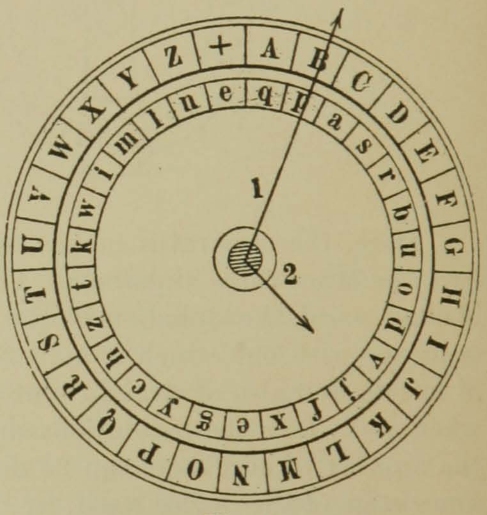


Fig. 4

> According to the experts, with this double disk a cryptogram written with 26 or 30 alphabets is obtained. As I will show later, the deciphering is not rendered difficult. In any case if absolute

[1] See *La Crittografia*, pages 53-55.

[2] Note that W, which does not occur normally in the Italian alphabet, is placed last.

secrecy is desired, care must be taken that the instrument does not fall into the hands of the enemy, as with only a few trials the mystery would be disclosed.

However, Gioppi makes no further reference to this device nor to the method of solving messages enciphered by means of it.

Upon consulting a description of the device by the inventor himself,[1] it was found that the description given by Gioppi is not strictly correct. Wheatstone's exposition and directions are as follows:

> Choose any name or word, in which the same letter does not recur, as "France," "Carlton," "Palmerston."
>
> Write down beneath it the omitted letters of the alphabet in their regular order, placing them in columns, thus:

C	*a*	*r*	*l*	*t*	*o*	*n*
b	*d*	*e*	*f*	*g*	*h*	*i*
j	*k*	*m*	*p*	*q*	*s*	*u*
v	*w*	*x*	*y*	*z*		

> Then write the letters as they appear in the successive vertical columns, in a single row, thus:
>
> *c b j v a d k w r e m x l f p y t g q z o h s n i u*
>
> The letters of the alphabet of the Cryptograph are then to be placed in the above order round the inner ring, the initial letter C in this case being placed exactly below the blank of the permanent alphabet.
>
> It is not *necessary* to adopt a word in which the same letters do not recur. Any word whatever will answer the purpose by erasing the redundant letters. For example:

S	*e*	*b*	*a*	[*s*]	*t*	*o*	*p*	[*o*]	*l*
c	*d*	*f*	*g*	*h*	*i*	*j*	*k*	*m*	*n*
q	*r*	*u*	*v*	*w*	*x*	*y*	*z*		

> This gives:
>
> *s c q e d r b f u a g v h w t i x o j y p k z m l n*
>
> *
>
> At the commencement, the long hand must correspond with the blank of the outer circle and the short hand be directly under it.
>
> The long hand must be brought successively to the letters of the despatch (outer circle), and the letters indicated on the inner circle by the short hand must be written down.
>
> At the termination of each word the long hand must be brought to the blank, and the letter indicated by the short hand also written down. By this arrangement the cipher is continuous, no intimation being given of the separation of the words.
>
> Whenever a double letter occurs, some unused letter (as, for instance, *q*) must always be substituted for the repeated letter; or the latter may be omitted.
>
> It will be best to divide a despatch into short sentences, and to commence each sentence with the instrument adjusted as at the beginning of the despatch. By this arrangement an error in one sentence cannot affect the other sentences.
>
> The full-stop at the end of each sentence should be represented by a dash following the letter that is used to conceal the blank or termination of the last word.
>
> *
>
> The chief circumstances which render this cipher so secure are these:
>
> 1. The same letter of the despatch is represented indifferently by any letter of the cipher.
>
> 2. No indication of the number of letters that there may be in any word is afforded.

[1] *The Scientific Papers of Sir Charles Wheatstone*, published by the Physical Society of London, 1879, pages 342-348.

3. There is no clue to the separation of the words, as the blank is itself represented indifferently by all the letters of the alphabet.

4. The changes in the signification of a letter depend on a *regular law*, the accessory hand making in some cases a complete revolution after one letter, and in others after two, three, or more letters.

5. The permutations of the cipher alphabets are practically infinite.

* *

It would seem, therefore, that Gioppi entirely missed the basic principle upon which Wheatstone placed so much reliance. Gioppi's example of the conventional alphabet, which is mounted on the inner disk, shows that it contains 27 characters, the same number as contained in the alphabet on the outer disk, which consists of the normal sequence terminated by the character +. Wheatstone's own directions show that the inner alphabet contains only 26 characters. The basic principle is, therefore, that concerned with the sliding of a 26-character alphabet against a 27-character one, a condition which results in the production of a variable factor of great importance. It results, in fact, in the transformation of what might otherwise be a single alphabet (mono-alphabet) system, into what has been denoted as a multiple alphabet system, involving 26 alphabets employed absolutely irregularly, dependent not only upon the disposition of the letters of the outer and inner alphabets but also upon the sequence of the letters of the text to be enciphered, and the starting point. The statement above to the effect that the system contains two keys (1) the disposition of the cryptographic alphabet and (2) the starting point, is, therefore, correct.

In the pages which follow we shall attempt to show that:

(1) The Wheatstone system, which is based upon a rather valuable principle, and which on superficial consideration seems safe and desirable, is in reality not complicated and is easy to decipher;

(2) Even if the outer alphabet should also be made a mixed alphabet, a modification which would immediately suggest itself to any decipherer, the system would be made somewhat more difficult to solve but would nevertheless be solvable, and within a very practical length of time.

First, as in the case of all systems intended for regular service such as field army communication, it must be assumed (1) that the enemy is in possession of all the information relating to the system, and (2) that he has intercepted, at least, a series of twenty-five short messages, or five long ones, in the same key and alphabets. In this case, by a short message is meant one of approximately 50 letters; by a long message, one of approximately 500 letters. These amounts are believed to be not only reasonable from the point of view of the decipherer but to be at the lower limit of the probable number.

2. SOLUTION OF MESSAGES WHEN ONLY THE INNER ALPHABET IS MIXED

A SINGLE MESSAGE

In order to show the method which may be used to solve messages enciphered by the original Wheatstone System, let us first study the enciphered message, together with its plain text, which the author himself gives as follows:

The following despatch of the Duke of Wellington, translated into a cipher constructed by means of this instrument, will afford an exercise both for translating into cipher and re-translating into ordinary language. The key-word is *France.* The dash indicates that the long and short hands of the cryptograph are both to be brought back to the blank, so that the following sentence may be translated without running on from the preceding.

Arruda, 8th October, 1810.

Lieut.-Gen. Viscount Wellington, K. B., to Lieut.-Gen. Hill.

SIR:

P Z L S P Q R E Q A J D I T F B U F Z O H Q O S U Q U D I K I T O R T W E Z A C
M T P L E R A U E S K G S O F G F D K H L S J I R K H F H M F A D A Y I V U O H A
O B L N O G R E J A I B K M P J Z T M J A B Q C N F P O M Y H Y R C Z D C W B X U B Z—

Z B I L I J T E J Y S P F D L C X E T K Q A S O X O U N N O D Q J C W E C L X P
U Y I E M M C M S Y V C F P O K W C D E D V D A G L P E E K N A G V K M N U U L S
H X Y X Y V G F Q P U Y I O R Q K L P T C Z H H K——

Z B K U P V S W Z W X A Q X D R E K T K Q A S O X O U I R S K O M F S T I I X G
W T Q J J V D Y F N A H L S I I X I A G Q L Z X V O G N H G R B U O H Y Z O O P W V
Y D D M Q J K F M O B J P D Y V R B A W K G W S J I R J G I T O W T V E Z B H S O S L V
U N B C H Q S O T E I E B D Q M G W H G J A M I S X F I F B B P A V P E S V C J U T
A D——

P Z L P T Y V X Q X D T G L T T A F C V M H O M B I N J K W V Y A Z O C Q L A I
U K F E G F N C N F I Z H H K V Z Y Q U G L I V E N K A H T R V F V E B W H W L R Y
C M L X W S Y S Y J H U F S F P O K E G Z R X L U B F T——

(Signed) WELLINGTON.

The* Quarter* Master* General* sends* orders* to* Major* General* Fane* to* withdraw* the* Cavalry* under* his* command* to* Togal* and* Loures*———

I* request* you* also* to* send* a* Brigade* of* six* pounders* to* Sobral* de* Monte* Agraca* to* join* the* Sixth* Division*[1] I* also* request* you* to* send* from* Villa* Franca* the* nine* pounder* Brigade* to* Capua* de* Montecheque* where* it* is* to* remain* in* reserve* and* in* readiness* to* move* at* a* short* notice*———

There* must* be* a* Brigade* of* Infantry* for* the* occupation* of* the* lines* extending* from* the* high* road* to* the* Tagus*.———

Let us make a detailed analysis of this example by studying the letter-for-letter transcription of the message with the cipher text, shown herewith:

```
THE+QUARTER+MASTER+GENERAL+SENDS+ORDERS+TO+MAJOR+GENE
PZLSPQREQAJDITFBUFZOHQOSUQUDIKITORTWEZACMTPLERAUESKGS

RAL+FANE+TO+WITHDRAW+THE+CAVALRY+UNDER+HIS+COMMAND+TO
OFGFDKHLSJIRKHFHMFADAYIVUOHAOBLNOGREJAIBKMPJZTMJABQCN

+TOGAL+AND+LOURES+_____I+REQUEST+YOU+ALSO+TO+SEND+A+BR
FPOMYHYRCZDCWBXUBZ     ZBILIJTEJYSPFDLCXETKQASOXOUNNOD

IGADE+OF+SIX+POUNDERS+TO+SOBRAL+DE+MONTE+AGRACA+TO+JO
QJCWECLXPUYIEMMCMSYVCFPOKWCDEDVDAGLPEEKNAGVKMNUULSHXY

IN+THE+SIXTH+DIVISION+_____I+ALSO+REQUEST+YOU+TO+SEND+
XYVGFQPUYIORQKLPTCZHHK     ZBKUPVSWZWXAQXDREKTKQASOXOU

FROM+VILLA+FRANCA+THE+NINE+POUNDER+BRIGADE+TO+CAPUA+D
IRSKOMFSTIIXGWTQJJVDYFNAHLSIIXIAGQLZXVOGNHGRBUOHYZOOP
```

[1] Wheatstone has failed to indicate here the long dash which marks the end of the second sentence. We have made an exact copy of his and Gioppi's expositions.

```
E+MONTECHEQUE+WHERE+IT+IS+TO+REMAIN+IN+RESERVE+AND+IN
WVYDDMQJKFMOBJPDYVRBAWKGWSJIRJGITOWTVEZBHSOSLVUNBCHQS

+READINESS+TO+MOVE+AT+A+SHORT+NOTICE+     THERE+MUST+B
OTEIEBDQMGWHGJAMISXFIFBBPAVPESVCJUTAD_____PZLPTYVXQXDT

E+A+BRIGADE+OF+INFANTRY+FOR+THE+OCCUPATION+OF+THE+LIN
GLTTAFCVMHOMBINJKWVYAZOCQLAIUKFEGFNCNFIZHHKVZYQUGLIVE

ES+EXTENDING+FROM+THE+HIGH+ROAD+TO+THE+TAGUS+_____
N̄KAHTRVFVEBWHWLRYCMLXWSYSYJHUFSFPOKEGZRXLUBFT
```

Following Wheatstone's directions the cipher alphabet for his example becomes as follows:

```
FRANCE
BDGHIJ
KLMOPQ
STUVWX
YZ
```

```
FBKSYRDLTZAGMUNHOVCIPWEJQX
```

Let us see whether we can obtain these results without having Wheatstone's apparatus by means of two ordinary alphabets alone, taking the first two words of this illustrative message as a check upon the system. The key letter, i. e., the letter which must be brought to the + space on the outer disk is F, the first letter of the inner alphabet, whereupon the two alphabets are in this position:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
+ABCDEFGHIJKLMNOPQRSTUVWXYZ
FBKSYRDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQX
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The cipher letter for T is P, as given by the message.

Now it is clear that in the device itself, in order to reach the letter H, from the position left by the previous plain-text letter T, the large hand will have to travel over 15 equal spaces of a perimeter divided up into 27 spaces as against the small hand which will have to travel over a like number of spaces of a perimeter divided up into only 26 spaces.

Let us count, on the outer alphabet, represented above by the upper alphabet, the intervals between the successive plain-text letters of the first two words of the message, proceeding always in the same direction, viz., from left to right. Thus:

```
T  H  E  +  Q  U  A  R  T  E  R  +
 15 24 22 17  4  7 17  2 12 13  9
```

Let us now count a like number of intervals on the inner alphabet, represented above by the lower alphabet, beginning with cipher letter P:

```
T  H  E  +  Q  U  A  R  T  E  R  +
P  Z  L  S  P  Q  R  E  Q  A  J  D
 15 24 22 17  4  7 17  2 12 13  9
```

Comparison with the cipher letters for these two words in the example will show that this method of counting the intervals has given the same results as the Wheatstone apparatus. It is clear that we can reproduce the entire cipher message without Wheatstone's apparatus by this method of counting the intervals. But if it is desired to secure these results without having to go through this laborious procedure, two sliding strips of cross-section paper containing the alphabets may be used, *remembering only that every time the encipherer passes from a plain-text letter to one which precedes it in the normal or upper alphabet, the lower strip containing the cipher alphabet must be moved one space to the left.* The successive positions of the two sliding strips for the first words of Wheatstone's example are shown in the diagrams below, in which the small figures in parentheses indicate the successive plain-text and cipher letters concerned:

```
                      (1)
1. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   FBKSYRDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXF

          (2)
2. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   BKSYRDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXFB

       (3)
3. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   KSYRDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXFBK

  (4)              (5) (6)
4. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   SYRDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXFBKS

   (7)              (8) (9)
5. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   YRDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXFBKSY

       (10)         (11)
6. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   RDLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXFBKSYR

  (12)
7. +ABCDEFGHIJKLMNOPQRSTUVWXYZ
   DLTZAGMUNHOVCIPWEJQXFBKSYRDLTZAGMUNHOVCIPWEJQXFBKSYRD
```

Note that in the seven different positions shown above, only in the case of letters (1), (2), (3), (4), (7), (10), and (12) did the lower strip have to be moved, and in each case only one space to the left.

It follows, therefore, that the Wheatstone apparatus is only a mechanical device so arranged as to produce automatically this shifting back one space, each time a plain-text letter is followed by one which precedes it in the normal alphabet. How that result is accomplished does not concern us—some arrangement of gears is probable. It is also clear that when a certain number of letters has been enciphered by means of two sliding strips, the lower alphabet will have slid 26 spaces, bringing the two alphabets back to their original starting point. The arrangement is such that when the outer hand has completed twenty-seven revolutions, the inner hand has completed twenty-six revolutions, thus completing one cycle and bringing the two hands back to their original starting point. Now the number of letters which is necessary in order to effect a completion of one cycle will not be fixed definitely, but since it depends only upon the disposition of the letters of ordinary English text, *the number may be determined experimentally as an average which will apply to all* *cases using the normal alphabet as the outer alphabet.* This number was found to be approximately fifty letters. This means, then, that we have at hand a definite method by means of which we are enabled to break up a long message into a series of short messages, all in the same key, by finding these cycles. This principle will be very important in the solution of a single message.

It is clear that aside from the 26 to 27 principle, the results are exactly the same as though one used an arbitrarily mixed alphabet sliding against a direct alphabet, shifting the alphabets one space at irregular intervals, always, however, in the same direction.

To prove that this is true, consider the following experiment: instead of using a mixed alphabet on the inner disk, suppose a direct alphabet were used. The following message has been enciphered by this means, the key letter for the specific message being unknown:

MESSAGE

```
DQZQN APRWX CUQXL FSTMT IIYAW
```

Let us "set" these groups upon a Sliding Poly-Alphabet. The results are as follows:

```
DQZQN  APRWX  CUQXL  FSTMT  IIYAW
ERARO  BQSXY  DVRYM  GTUNU  JJZBX
FSBSP  CRTYZ  EWSZN  HUVOV  KKACY
GTCTQ  DSUZA  FXTAO  IVWPW  LLBDZ
HUDUR  ETVAB  GYUBP  JWXQX  MMCEA
IVEVS  FUWBC  HZVCQ  KXYRY  NNDFB
JWFWT  GVXCD  IAWDR  LYZSZ  OOEGC
KXGXU  HWYDE  JBXES  MZATA  PPFHD
LYHYV  IXZEF  KCYFT  NABUB  QQGIE
MZIZW  JYAFG  LDZGU  OBCVC  RRHJF
NAJAX  KZBGH  MEAHV  PCDWD  SSIKG
OBKBY  LACHI  NFBIW  QDEXE  TTJLH
PCLCZ  MBDIJ  OGCJX  REFYF  UUKMI
QDMDA  NCEJK  PHDKY  SFGZG  VVLNJ
RENEB  ODFKL  QIELZ  TGHAH  WWMOK
SFOFC  PEGLM  RJFMA  UHIBI  XXNPL
TGPGD  QFHMN  SKGNB  VIJCJ  YYOQM
UHQHE  RGINO  TLHOC  WJKDK  ZZPRN
VIRIF  SHJOP  UMIPD  XKLEL  AAQSO
WJSJG  TIKPQ  VNJQE  YLMFM  BBRTP
XKTKH  UJLQR  WOKRF  ZMNGN  CCSUQ
YLULI  VKMRS  XPLSG  ANOHO  DDTVR
ZMVMJ  WLNST  YQMTH  BOPIP  EEUWS
ANWNK  XMOTU  ZRNUI  CPQJQ  FFVXT
BOXOL  YNPUV  ASOVJ  DQRKR  GGWYU
CPYPM  ZOQVW  BTPWK  ERSLS  HHXZV
```

It would be an easy matter indeed for a decipherer to pick out the plain text. Beginning with the letter S and ascending irregularly a step at a time, the message SEND+MACHINE+GUN+AT+ONCE+ is clearly seen. It is to be noted, however, that this apparent irregularity is in reality regular: that is, each time a plain-text letter is followed by one which precedes it in the normal alphabet, a step upward is to be taken. If the alphabets of the Poly-Alphabet contained the + sign, the latter would also appear in the correct places between words. In this case the successive words are separated by an A or a Z.

After carefully studying the example given by the author it was seen that the basic principles upon which the solution of messages enciphered by the Wheatstone system depends, are three in number:

(1) The cycle, which consists in the return of the alphabets to the original starting point when 27 revolutions of the outer hand have been completed, will in practice be completed after approximately 50 letters of the plain text have been enciphered, as stated above;

(2) Similar letters in the plain text when near each other will be enciphered by letters adjacent or near each other in the inner or cipher alphabet, with the result, therefore, that if one could recognize only the encipherments of the plain-text letter E, or of any other high-frequency letter, throughout the text, the complete cipher alphabet could be reconstructed;

(3) Two identical cipher letters (a) when in juxtaposition always indicate that the two plain-text letters which they encipher are adjacent to each other in the outer alphabet but in the reverse order; and (b) when near each other usually indicate that the plain-text letters which they encipher are near each other in the outer alphabet, but in the reverse order.

As an illustration of what is meant by principles (2) and (3), consider the encipherment of the following phrase by means of the same alphabets, given in Wheatstone's example:

```
ELEVEN+ELEMENTS+EVER+EXCEPTED+
FLBCKGQSAYMRNWWSTXZERASZGEFMMZ
             --            --
```

Note now the successive cipher letters representing the plain-text letter E. They are as follows:

```
F.B.K..S.Y.R....T.Z..A..G..M
```

Comparison with the cipher alphabet applying to the Wheatstone example will disclose the fact that the sequence of the successive encipherments of letter E is almost identical with a section of this alphabet. Here is the complete alphabet exactly as on page 10:

```
FBKSYRDLTZAGMUNHOVCIPWEJQX
```

Note the double cipher letters W and M; in the former case they encipher the digraph TS, in the latter case they encipher the digraph ED; in both cases the individual letters of these sets of digraphs are found in juxtaposition in the outer alphabet, but in reverse order, viz., ST and DE. Note also the cipher letter Z, representing E, C, and + respectively. These are close to each other in the outer alphabet and in the reverse order, viz., + . . C . E.

As an illustration of principle (1), consider the example which Wheatstone gives. Note that the message begins with T, enciphered by P. Whenever T is enciphered by P at any future time in this message, we shall know that the cycle has been completed. This holds true for any letter and its corresponding cipher equivalent. Since in ordinary text recurrences of digraphs, trigraphs, and polygraphs are inevitable, and since the operation of the laws of chance will result in the falling of such recurrences near or about the completion points of cycles, such recurrences at intervals of approximately 50 letters may be taken as the external indications of the completion of the cycle and the entrance upon the next cycle. If, therefore, we can find these external indications of the completion of the cycle, it will be entirely possible to regroup the cipher letters of a single long message in such a manner that the message may be broken up into a series of messages, all in the same key. Since there are two characters which occur with great frequency in the message, namely, + and E, we should be able to find these breaking points which would indicate the completion of the cycle.

This indeed can be found and illustrated best by writing out the sentences of the message on cross-section paper in lines containing about 50 to 60 letters, cutting the lines apart, and then shifting them so as to bring the greatest number of recurrences within adjacent columns, as has been done in the accompanying Fig. 5. Note that at an interval of approximately 50 letters, the cycle has been completed. One great help in this example is the fact that Wheatstone advocated (see page 7): "It will be best to divide a despatch into short sentences and to commence each sentence with the instrument adjusted as at the beginning of the despatch. By this arrangement an error in one sentence cannot affect the other sentences. The full-stop at the end of each sentence should be represented by a dash following the letters." It is clear, therefore, that this safeguard against errors constitutes a very serious weakness of the system, for it immediately gives the decipherer notice that a cycle has been completed, and that a new one is about to begin.

Now let us follow through the encipherment of the most frequent character, namely, the termination mark showing the completion of words, in order to see if what has been stated above as the second principle will hold true. We can do this best by making a distribution of the cipher letters, giving their positions in each message by means of cross-section paper, as shown in Chart A of the accompanying Fig. 6. For comparison we shall also make the same kind of a chart for the plain-text letter E, shown in Chart B of the same figure.

A careful study of these two charts will disclose the fact that the successive cipher letters for either the + or the letter E, or better, for the combination of the two, will give the sequence of the letters of the inner alphabet. Note, for example, that B is followed by Y, S, and K in cycles 4, 6, and 8 in A, Fig. 6; and by Y in cycle 7, B of Fig. 6. It may be concluded therefore that these letters are close to each other in the inner alphabet, but the question is, in what order? Now in Chart A, line 8, B is followed by KS, that is, K comes between B and S, and therefore one may assume that the sequence is BKS. In line 11 of Chart A, K is followed by Y, but from the reasoning above, K is in juxtaposition with S,

```
Cycle             1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60
1                 P  Z  L  S  P  Q  R  E  Q  A  J  D  I  T  F  B  U  F  Z  O  H  Q  O  S  U  Q  U  D  I  K  I  T  O  R  T  W  E  Z  A  C  M  T  P  L  E  R  A  U  E  S  K  G  S  O  F
                  T  H  E  +  Q  U  A  R  T  E  R  +  M  A  S  T  E  R  +  G  E  N  E  R  A  L  +  S  E  N  D  S  +  O  R  D  E  R  S  +  T  O  +  M  A  J  O  R  +  G  E  N  E  R  A    Sentence
2           G  F  D  K  H  L  S  J  I  R  K  H  F  H  M  F  A  D  A  Y  I  V  U  O  H  A  O  B  L  N  O  G  R  E  J  A  I  B  K  M  P  J  Z  T  M  J  A  B  Q  C  N  F  P  O  M             Nº 1
            L  +  F  A  N  E  +  T  O  +  W  I  T  H  D  R  A  W  +  T  H  E  +  C  A  V  A  L  R  Y  +  U  N  D  E  R  +  H  I  S  +  C  O  M  M  A  N  D  +  T  O  +  T  O  G
3                    Y  H  Y  R  C  Z  D  C  W  B  X  U  B  Z
                     A  L  +  A  N  D  +  L  O  U  R  E  S  +
4                 Z  B  I  L  I  J  T  E  J  Y  S  P  F  D  L  C  X  E  T  K  Q  A  S  O  X  O  U  N  N  O  D  Q  J  C  W  E  C  L  X  P  U  Y  I  E  M  M  C  M  S  Y  V  C  F  P  O    Sentence
                  I  +  R  E  Q  U  E  S  T  +  Y  O  U  +  A  L  S  O  +  T  O  +  S  E  N  D  +  A  +  B  R  I  G  A  D  E  +  O  F  +  S  I  X  +  P  O  U  N  D  E  R  S  +  T  O    Nº 2
5                 K  W  C  D  E  D  V  D  A  G  L  P  E  E  K  N  A  G  V  K  M  N  U  U  L  S  H  X  Y  X  Y  V  G  F  Q  P  U  Y  I  O  R  Q  K  L  P  T  C  Z  H  H  K
                  +  S  O  B  R  A  L  +  D  E  +  M  O  N  T  E  +  A  G  R  A  C  A  +  T  O  +  J  O  I  N  +  T  H  E  +  S  I  X  T  H  +  D  I  V  I  S  I  O  N  +
6                 Z  B  K  U  P  V  S  W  Z  W  X  A  Q  X  D  R  E  K  T  K  Q  A  S  O  X  O  U  I  R  S  K  O  M  F  S  T  I  I  X  G  W  T  Q  J  J  V  D  Y  F  N
                  I  +  A  L  S  O  +  R  E  Q  U  E  S  T  +  Y  O  U  +  T  O  +  S  E  N  D  +  F  R  O  M  +  V  I  L  L  A  +  F  R  A  N  C  A  +  T  H  E  +  N
7                 A  H  L  S  I  I  X  I  A  G  Q  L  Z  X  V  O  G  N  H  G  R  B  U  O  H  Y  Z  O  O  P  W  V  Y  D  D  M  Q  J  K  F  M  O  B  J  P  D  Y  V  R [B  A  W]      Sentence
                  I  N  E  +  P  O  U  N  D  E  R  +  B  R  I  G  A  D  E  +  T  O  +  C  A  P  U  A  +  D  E  +  M  O  N  T  E  C  H  E  Q  U  E  +  W  H  E  R  E  +  I  T             Nº 3
8                 B  A  W  K  G  W  S  J  I  R  J  G  I  T  O  W  T  V  E  Z  B  H  S  O  S  L  V  U  N  B  C  H  Q  S  O  T  E  I  E  B  D  Q  M  G  W  H  G  J  A  M  I  S  X  F  I  F
               +  I  T  +  I  S  +  T  O  +  R  E  M  A  I  N  +  I  N  +  R  E  S  E  R  V  E  +  A  N  D  +  I  N  +  R  E  A  D  I  N  E  S  S  +  T  O  +  M  O  V  E  +  A  T  +
9                 B  B  P  A  V  P  E  S  V  C  J  U  T  A  D
                  A  +  S  H  O  R  T  +  N  O  T  I  C  E  +
10                P  Z  L  P  T  Y  V  X  Q  X  D  T  G  L  T  T  A  F  C  V  M  H  O  M  B  I  N  J  K  W  V  Y  A  Z  O  C  Q  L  A  I  U  K  F  E  G  F  N  C  N  F  I  Z  H  H
                  T  H  E  R  E  +  M  U  S  T  +  B  E  +  A  +  B  R  I  G  A  D  E  +  O  F  +  I  N  F  A  N  T  R  Y  +  F  O  R  +  T  H  E  +  O  C  C  U  P  A  T  I  O  N       Sentence
11             K  V  Z  Y  Q  U  G  L  I  V  E  N  K  A  H  T  R  V  F  V  E  B  W  H  W  L  R  Y  C  M  L  X  W  S  Y  S  Y  J  H  U  F  S  F  P  O                                   Nº 4
               +  O  F  +  T  H  E  +  L  I  N  E  S  +  E  X  T  E  N  D  I  N  G  +  F  R  O  M  +  T  H  E  +  H  I  G  H  +  R  O  A  D  +  T  O
12             K  E  G  Z  R  X  L  U  B  F  T
               +  T  H  E  +  T  A  G  U  S  +
                  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55
```

Fig. 5. THE WHEATSTONE EXAMPLE SEPARATED INTO ITS CONSTITUENT CYCLES

CHART A — Showing the successive encipherments of +

Sentence	Cycle		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
	1					S								D							Z								U														C			P						E						F
1	2					S			R									A				U									O							I					P								Q			F						
	3			Y						D								Z																																								
2	4			B								Y				D					T				A						U		N								C				P					E											F		
	5		K							D			L						A							U				H					V				P						Q										K				
	6			B					S								D					T				A						U						O						I								J					F						
	7					S								L						G							U							O			V													J												
3	8	B			K			S			R								T			Z									U				H		O													W				J						X			F
	9			B						S								D																																								
	10							Y					D				L		T									M				N										C				I					E											
4	11	K			Y				L						A										H					C					W					J					F													
	12	K				R						T																																													

CHART B — Showing the successive encipherments of E

Sentence	Cycle		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
	1				L								A							U				H		O								I									E															K		S		
1	2				L																	V													J																							
	3														U																																										
	4					L			T																	O													E														Y					
2	5										G						N																				Q													Y							
	6									Z			A													O																															
	7				L							G									H												W						Q			F				B				Y		R						
3	8					G															H				O				V												E					Q											S				
	9					A																																																			
	10				L		T								G											O																							F												
4	11							G					N			H				V															X																								
	12				Z																																																				

Fig. 6. THE WHEATSTONE EXAMPLE SHOWING THE SUCCESSIVE ENCIPHERMENTS OF THE + SIGN AND THE PLAIN-TEXT LETTER E

wherefore the sequence may be assumed to be BKSY. The sequences with Y are YD, YL, and YR. But another sequence, YDL, line 10, Chart A, gives us reason to assume that the sequence is BKSYDL, with the last sequence in the form DLT in line 10, Chart A. Hence the sequence may be assumed to be BKSYDLT. Now in line 8, Chart A, it is seen that the sequence SRT shows R coming between S and T in the assumed sequence, and we must therefore find a place for this letter. In line 7, Chart B, the sequence Y-R gives us reason for assuming that R immediately follows Y, but a corroboration is necessary, which may be found. Now from the nature of the system, it will be apparent that such combinations as DE, NO, ST, and +A, which are very frequent, and the components of which are in juxtaposition in the outer alphabet, ought to furnish a valuable clew as to the sequence of a series of two or three letters of the inner alphabet since the cipher equivalents of such combinations must be sequent in the inner alphabet. Applying this reasoning to the problem in hand, we go through the message to find a place where R, Y, D, or L are concerned, in order to try to locate such a place. In the first sentence, cycle 3, Fig. 5, the digraph +A of AND shows that +A is enciphered by YR and proves that the sequence is BKSYRDLT. Enough has been shown to demonstrate the method, and to convince that the entire sequence may be reconstructed by the process.

The following examples, taken from the Wheatstone message, are illustrations of the third principle stated above, viz., that two identical cipher letters, (a) when in juxtaposition always indicate that the two plain-text letters which they encipher are adjacent to each other in the outer alphabet, but in the reverse order; and (b) when near each other usually indicate that the plain-text letters which they encipher are near each other in the outer alphabet, but in the reverse order. Note the word POUNDER, which occurs twice, enciphered thus:

```
 [Sentence No. 2]          [Sentence No. 3]
 [Cycle 4, Fig. 5]         [Cycle 7, Fig. 5]

(1) POUNDER            (2) POUNDER
    MMCMSYV                IIXIAGQ
```

Here PO is enciphered by MM and II respectively. Also note that PO-N is enciphered by MM-M and II-I respectively. This indicates that these plain-text letters are in juxtaposition in the outer alphabet, but in the reverse order, viz., NOP. Another illustration of these principles to be found in this same example is the following:

```
[Sentence No. 4]
[Cycle 11, Fig. 5]

      HIGH
      SYSY
```

Often it will be found that a cipher letter repeated after an interval of one, two, sometimes three spaces, will represent letters in juxtaposition in the reverse order in the outer alphabet; and just as often it will be found that a cipher letter repeated after two, three, sometimes five intervals, will represent two letters one space removed from each other in the outer alphabet and in the reverse order. The following are illustrations of this, taken from the same example as shown in Fig. 5:

Cycle 1, letters 29-31,	IKI END	I-I→DE
Cycle 1, letters 6- 9,	QREQ UART	Q--Q→TU
Cycle 2, letters 24-28,	OBLNO ALRY+	O---O→+A

Cycle 1, letters 50-53,	SKGS GENE	S--S→E(F)G
Cycle 2, letters 39-43,	JZTMJ COMMA	J---J→A(B)C
Cycle 5, letters 15-20,	KNAGVK TE+AGR	K----K→R(S)T
Cycle 11, letters 35-41,	SYJHUFS GH+ROAD	S-----S→D(EF)G

It is impossible to have a case where a cipher letter, repeated after but one interval, will represent two letters one space removed from each other in the outer alphabet. The least number of intervals in such a case is two.

Now, naturally, when one has the entire plain text, the procedure given above for reconstructing the cipher alphabet is entirely unnecessary, because one can reconstruct it by applying the method given on page 11. But these principles are essential to the decipherment of a message based upon the Wheatstone system, for in practice the decipherment and the reconstruction of the alphabet proceed simultaneously, one aiding the other.

A SERIES OF MESSAGES

Let us now apply these principles to the solution of the following series of twenty partial messages, diplomatic text, all enciphered by means of the same cipher alphabet, and in accordance with the directions given by Wheatstone, which includes the premise that they would all begin at the same starting point, or key letter. Considering this condition, it is apparent that, given a series of messages of which some of the initial words begin with such digraphs as, for example, BE, CE, DE, etc., (in other words, digraphs in which the second letter comes *after* the first letter in the normal alphabet), the second letter in each pair will be enciphered by the same letter. Likewise, given such initial combinations as LE, NE, RE, SE, etc., (in other words, digraphs in which the second letter comes *before* the first letter in the normal alphabet), the second letter in each pair will be enciphered by the same letter. What is true with respect to initial combinations is also true of combinations within the words and sentences, for the laws of chance are in operation here as they are everywhere else. The messages are as follows:

MESSAGES

1. AGWLSFDEXSSU
2. TNMWVEMPOTMX
3. TFWVWIZDSKRX
4. NUBDPZWOEGZZ
5. FQBAZOWTVEZD
6. RORSWJSVEMPR
7. LFRODSVEMPOU
8. ZODTIEDSVDTM
9. TFWVZJFEQPXT
10. ROWWTTGRMOCS
11. FQBZWFLJIDUJ
12. TFWTILMOSOIX
13. MNJWJSVJFTTE
14. TFPTNVISIJRZ
15. ZOEWTLYLSPSC
16. DSOZCNOWOIHW
17. LDLPTXHHLGED
18. DKNQXALEGZZO
19. YYNSXFDOJSRA
20. AROHVTLEGZZK

Considering what was stated in the preceding paragraph it is clear that, although the shifting-back process is not regular, still in a series of messages all in the same key, when the messages are so arranged as to bring the successive letters into columns, as shown above, a frequency table of any column would be almost a single alphabet frequency table with sometimes two or three values for any given letter. But on the whole, the most frequent cipher letter will represent either a high-frequency letter, or the + sign. And furthermore, if the frequency tables for the successive columns be studied carefully, it may be possible to pick out the cipher equivalents of several of the high-frequency letters.

The frequency tables for the first five columns are as follows:

1.	A	T	N	F	R	L	Z	M	D	Y
	𝍷𝍷	𝍸		𝍷𝍷	𝍷𝍷	𝍷𝍷	𝍷𝍷		𝍷𝍷	

2.	G	N	F	U	Q	O	S	R	D	K	Y
		𝍷𝍷	𝍸		𝍷𝍷	𝍷𝍷𝍷𝍷					

3.	W	M	B	R	D	J	P	E	O	L	N
	𝍸		𝍷𝍷𝍷	𝍷𝍷					𝍷𝍷		𝍷𝍷

4.	L	W	V	D	A	S	O	T	P	Z	Q	H
		𝍷𝍷𝍷𝍷	𝍷𝍷			𝍷𝍷		𝍷𝍷𝍷		𝍷𝍷		

5.	S	V	W	P	Z	D	I	T	J	N	X	C
		𝍷𝍷	𝍷𝍷𝍷		𝍷𝍷		𝍷𝍷	𝍷𝍷𝍷			𝍷𝍷	

Let us first of all try to find E. Since E is not very high as an initial letter,[1] we may omit for the present column 1, and proceed to column 2. It is clear that we should find a cipher letter which is high in column 2 and which also occurs in column 3, since the chances are that E will be enciphered in the next adjacent column by the same cipher letter in at least several cases. Cipher letter O seems to meet these conditions much better than does cipher letter F, because O occurs twice again in column 3, whereas F does not occur. Furthermore, a careful inspection of the first two columns shows that F is combined with three other letters, T, W, and V, twice in the polygraph TFWV, three times in the trigraph TFW, and four times in the digraph TF, leading to the assumption that TFWV represents THE+.

[1] The order of frequency of initial letters in English as given by Hitt is, TOAW (BC)(DS). See Hitt, Parker. *Manual For The Solution Of Military Ciphers*, 1916, page 9.

Now cipher letter W occurs five times in column 3, four times in column 4, and three times in column 5, thus corroborating our assumption that W is E in these columns, and offering further corroboration of the assumption that TFWV represents THE+.

Perhaps if these individual frequency tables be consolidated in pairs, more information could be procured. The combined tables are as follows:

1 & 2.	A	T	N	F	R	L	Z	M	D	Y	G	U	Q	O	S	K
	ǀǀ	卌	ǀǀǀ	卌 ǀǀ	ǀǀǀ	ǀǀ	ǀǀ		ǀǀǀ	ǀǀ			ǀǀ	ǀǀǀǀ		

2 & 3.	G	B	F	U	Q	O	N	S	R	D	K	Y	W	M	J	P	E	L
		ǀǀǀ	卌		ǀǀ	卌 ǀ	ǀǀǀǀ		ǀǀǀ	ǀǀ			卌					

3 & 4.	W	M	B	R	D	J	P	E	O	L	N	V	A	S	T	Z	Q	H
	卌 ǀǀǀǀ		ǀǀǀ	ǀǀ	ǀǀ		ǀǀ		ǀǀǀ	ǀǀ	ǀǀ	ǀǀ		ǀǀ	ǀǀǀ	ǀǀ		

4 & 5.	L	W	V	D	A	S	O	T	P	Z	Q	H	I	J	N	X	C
		卌 ǀǀ	ǀǀǀǀ	ǀǀ		ǀǀǀ		卌 ǀ	ǀǀ	ǀǀǀǀ			ǀǀ			ǀǀ	

It will be seen that W is high in frequency as far as column 5, and in most cases we can assume it to be E.

If in the trigraph OWW, the tenth message, O equals E, then this trigraph probably represents EFE in accordance with the principle explained on page 17. The frequency of the digraph RO in columns 1 and 2 leads us to assume that this is a high-frequency combination, possibly RE. Now REFE suggests REFER, or REFERRING, or REFERENCE. We can test out this word and also our values by using sliding strips of cross-section paper. By means of them the correctness of our values is corroborated and the word is found to be REFERRING, using the Q to indicate the double letter R, in accordance with the directions given by Wheatstone. This gives the values of GRM as ING, with a check on the correctness of R in the 19th position as giving N. The alphabet so far is as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
						O	W		F			M	G					R		T					

Applying this partial alphabet to the sixth message we get either REE-E, or REQ-E. The latter suggests the word REQUEST, which checks itself on the letters U and T which are represented by cipher letter S in the 23rd position.

In the last message ARO may well be PRE, possibly PREPARE, or PREPARATIONS, and in the first message this gives PLE as the probable beginning of the message, probably PLEASE. Enough has been shown of the method by means of which it is possible to decipher the entire series of messages.

However, a much quicker method of solving the entire series, once a start has been made, and the positions of a few letters of the cipher alphabet tentatively determined, is to attempt, by means of these few values, a reconstruction of the rectangle from which the cipher alphabet was derived, which may be called the *generating rectangle*. This is possible not only in the case of the very simple method given by Wheatstone, but also in the case of almost every other method which follows a system, such as taking the columns in accordance with a key number derived from the key word, etc. In fact, this method of forming an arbitrarily mixed alphabet from a key word is a source of grave danger to the system. The decipherer may not be able to reconstruct the generating rectangle completely from only a few values, but he will be able to assume additional values based upon the position of the few letters already placed, to try these new values out, and thus succeed in deciphering more of the messages, which in turn will lead to additional values and positions in the tentative generating rectangle, until the rectangle is completed. Thus he will be able to find the complete cipher alphabet, and from there on he experiences no further difficulty.

In order to illustrate the method let us take the original Wheatstone example again (page 9). It will be admitted that to the alert decipherer the initial groups PZLS and PZLPT, of the first and fourth sentences, suggest THE+ and THERE+ respectively. A trial of these words places the cipher letters S, Y, L, T, Z, and P in positions 4, 5, 8, 9, 10, and 21, respectively, in the cipher alphabet, which is then as follows:

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
 +  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
          S  Y        L  T  Z                                P
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26  1
```

Note that the position of P checks the assumption of THERE for the beginning of the fourth sentence, since by shifting the alphabets as required, P stands for T and then for R, according to the requirements of the cipher text.

Now since S and Y, and L, T, and Z are shown to form two sequences, we may assume them to be parts of two columns of the generating rectangle. Furthermore, since Y and Z are in juxtaposition in the normal alphabet, it follows that these two partial columns are adjacent in the rectangle unless either Y or Z are in the key word, which, being improbable, we will assume not to be the case. There are two possible positions which will meet these requirements:

```
         L                          L . . . S
   (1)  ST          or        (2)   T . . . Y
        YZ                          Z
```

Now the second possibility may be ruled out as being not so probable as the first, since the latter shows two sequences which are likely in the rectangle, viz., ST and YZ.

Returning to the tentative alphabet upon the sliding strips it is noted that the sequence SY is separated from the sequence LTZ by only two intervals. This means that the column in which LTZ occurs consists of five letters; and this in turn means that the column in which SY occurs also consists of five letters. This leaves sixteen letters to be distributed in columns of equal length in the rectangle. These columns cannot be more than five nor less than four letters in length. The most probable arrangement is therefore, four more columns of four letters, indicating a rectangle of six-letter rows, or in other words, a key word of six letters net. Thus:

```
------
------
-L--P-
ST----
YZ
```

By placing P in the diagram, at the correct number of intervals away from Z, eleven, as given by the partial cipher alphabet, further support is given to our hypothesis.

We may proceed now to fill in probable values in this rectangle, based upon such usually unbroken sequences as JKL, PQ, etc. Noting that there are four vacant spaces between T and Y, since there are normally four letters between these two letters in the direct alphabet, we may proceed to fill in these values at once. We may also fill in tentatively J, K, and Q. The rectangle is then as follows:

```
-    -    -    -    -    -
-    -    -    -    -    J
K    L  (MN) (NO)   P    Q
S    T    U    V    W    X
Y    Z
```

Note that the two intervals between L and P are assigned to (MN) and (NO). If M is in the key word, then the sequence must be LNOP; if N is in the key word, the sequence must be LMOP; if O is in the key word, the sequence must be LMNP. At any rate, a trial will soon disclose which of these three conditions is the case.

The cipher alphabet, augmented by these tentative letters, based upon the hypothesis of the generating rectangle of six-letter rows, is as follows:

```
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
  +  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
        K  S  Y        L  T  Z        M  U        N  V        P  W     J  Q  X
                                      N           O
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26  1
```

With this partial alphabet enough subsequent decipherment is easily obtained to enable the complete reconstruction of the alphabet. For example, applied to the second sentence:

```
          * *
PZLPTYVXQXDTGLTT
THERE+MUST+BE+A+
```

The two new values, indicated by the asterisk, are immediately placed into their proper positions in the rectangle, which now is as follows:

```
-    -    -    -    -    -
-    D    G    -    -    J
K    L  (MN) (NO)   P    Q
S    T    U    V    W    X
Y    Z
```

H and I must be assigned to their positions between G and J. Thus:

```
-    -    -    -    -    -
-    D    G    H    I    J
K    L  (MN) (NO)   P    Q
S    T    U    V    W    X
Y    Z
```

Enough has been shown to convince that the procedure is entirely feasible and leads to quick results.

Let us apply this same method of attempting a reconstruction of the generating rectangle for the series of messages under present discussion. From the probable words THE, PLEASE, and REFERRING, the following partial alphabet results:

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
 +  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
          V  L  D  O  W     F        M  G        A     R     T     S
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

Supposing V to be in or about its normal position in the generating rectangle, the following tentative diagrams suggest themselves as being very probable:

(1)
Basic Generating
Rectangle

-	L	-	M	A	T
-	D	F	G	-	-
-	O	-	-	R	S
V	W	-	-	-	

→

(2)
Basic Generating
Rectangle with
Additional Probable
Values

-	L	-	M	A	T	-
-	D	F	G	$\binom{H}{I}$	$\binom{I}{J}$	$\binom{J}{K}$
N	O	P	Q	R	S	U
V	W	X	Y	Z		

With the new values assumed, according to alphabetical sequence, as shown above, the cipher alphabet is augmented and tried out on the series of messages, with the result that no inconsistencies are found and additional deciphered matter is secured. For example, a trial of the alphabet on message number seventeen produces the word DECISION, and determines that letter H occupies the 18th position in the cipher alphabet. Thus in a few moments all the letters of the cipher alphabet are located, and the rectangle is found to be based upon the key word CLIMATE. Often the key word may be guessed from the positions of a few of the letters of the first row. It would not have been hard to guess this one, having given the sequence -L-MAT-.

The plain text for this series of partial messages is as follows:

```
     1 2 3 4 5 6 7 8 9 10 11 12
 1.  A G W L S F D E X S S U
     P L E A S E + R E P O R

 2.  T N M W V E M P O T M X
     T A K E + T H E + N E C

 3.  T F W V W I Z D S K R X
     T H E + D E P A R T M E

 4.  N U B D P Z W O E G Z Z
     B Y + D I R E C T I O N

 5.  F Q B A Z O W T V E Z D
     I N + O R D E R + T O +

 6.  R O R S W J S V E M P R
     R E Q U E S T + T H E M

 7.  L F R O D S V E M P O U
     D I R E C T + T H E + S

 8.  Z O D T I E D S V D T M
     S E C R E T A R Y + O F

 9.  T F W V Z J F E Q P X T
     T H E + P R E S I D E N

10.  R O W W T T G R M O C S
     R E F E R R I N G + T O
```

```
     1 2 3 4 5 6 7 8 9 10 11 12
11.  F Q B Z W F L J I D U J
     I N + R E G A R D + T O

12.  T F W T I L M O S O I X
     T H E R E + H A S + B E

13.  M N J W J S V J F T T E
     L A T E S T + R E P O R

14.  T F P T N V I S I J R Z
     T H I S + A F T E R N O

15.  Z O E W T L Y L S P S C
     S E V E R A L + R E Q U

16.  D S O Z C N O W O I H W
     E V E R Y + D E C E N C

17.  L D L P T X H H L G E D
     D E C I S I O N + I S +

18.  D K N Q X A L E G Z Z O
     E X A M I N A T I O N +

19.  Y Y N S X F D O J S R A
     O N + T H E + A P P L I

20.  A R O H V T L E G Z Z K
     P R E P A R A T I O N S
```

This method of reconstructing the generating rectangle may be used to solve a single very short message, provided the decipherer can assume and find a single word in the message.

In order to show how a single short dispatch may be solved by this method, the following message is given, in which the word ARTILLERY is suspected:

```
XFNAZ XEKYS TKQYE PHILH MGNGL LCTH
```

By the use of sliding strips an attempt is made to locate the word ARTILLERY by means of certain interval-checks on the letters, which will become clear when the actual position of the word is given:

```
+ARTILLERY+
XEKYSTKQYEP
```

The alphabet determined by these letters is as follows:

```
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
X  E     P           Q        S        T              K     Y
```

The nature of the interval-checks may be explained best by showing the successive positions of the two alphabets, in which the successive sets of letters concerned are indicated by the roman numerals.

```
I  II                                                 III   IV
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
+  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
X  E     P           Q        S        T              K     Y
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

                           V        VI             VII
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
+  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
E     P           Q        S        T              K     Y                    E
2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2

               VIII                                   IX                   X
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
+  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
   P           Q        S        T              K     Y                    E
3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3

XI
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
+  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
P           Q        S        T              K     Y                    E     P
4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 1  2  3  4
```

It is seen that cipher letter E meets the requirement that it should represent A and Y (II and X); cipher letter K meets the requirement that it should be R and Q (Q = repeated letter L; III and VII); cipher letter Y meets the requirement that it should be T and R (IV and IX).

Let us now attempt a reconstruction of the generating rectangle. A few trials show that the arrangement which best meets the requirements of the spatial relations of the letters in the partial alphabet is as follows:

```
-E-----Y
------K-
-PQST---
X-
```

This rectangle may be filled out with probable values as follows:

$$\begin{array}{cccccccc} - & E & - & - & - & - & - & Y \\ - & - & - & \binom{G}{H} & \binom{H}{I} & J & K & L \\ - & P & Q & S & T & U & V & W \\ X & Z & & & & & & \end{array}$$

These new values enable further progress in decipherment. The assumption of the two possible values for GH and HI enable us to determine that the HIJ sequence is correct, for it gives FIRE as the word following ARTILLERY. This enables us to place M and G with certainty in the sequence, and probably F. The alphabet is as follows:

```
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
  X  E     P  Z  M  G  Q     H  S     I  T     J  U     K  V  Y  L  W        N
```

This gives the last two words AT+ONCE+ and places C before I in the alphabet. Going back to get the first of the message the word CEASE is secured without difficulty. The entire alphabet may be reconstructed and the key word is found to be DEMOCRA(C)Y. Thus:

```
DEMOCRAY
BFGHIJKL
NPQSTUVW
XZ
```

Alphabet: DBNXEFPZMGQOHSCITRJUAKVYLW

The preceding pages have demonstrated that the Wheatstone principle when used in connection with a direct alphabet on the outer disk, and a mixed alphabet formed by some simple system from a key word on the inner disk, is very easy to solve and offers no security against attack.

The principal circumstance which renders this possible is not so much that the outer alphabet is a direct alphabet, as that it is an alphabet of which the entire sequence is known.

The value of this knowledge concerning the outer alphabet is that the tentative decipherment of any part of a message enables the decipherer to begin the reconstruction of the inner or cipher alphabet at once, a procedure which will demonstrate quickly whether the tentative decipherment is correct or not, and if it is correct, will enable him to add to this partial alphabet.

The question then immediately presents itself as to the security which would be added by the use of another unknown or cipher alphabet on the outer disk also. In such a case the decipherer would be unable to begin a reconstruction of the inner alphabet immediately upon having arrived at a partial decipherment. We shall attempt to show, however, that, even with two dissimilar arbitrarily mixed alphabets, a series of short messages in the same key, or a single long message, may be solved.

3. SOLUTION OF MESSAGES WHEN BOTH ALPHABETS ARE MIXED

A SERIES OF MESSAGES

In order to demonstrate the method of attack upon an a-periodic multiple alphabet cipher of this type when the outer alphabet is mixed, as well as the inner, the steps in the solution of the following series of twenty-six messages, containing partial military orders, will be given:

MESSAGES

```
      1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
 1.   X R B I T P X H O Y L N W C F Z P W E V Y D T C R
 2.   I W P I O Q L U A H E S X G Q L X K I L B O D F T
 3.   W H W D W W R Z C H N S H J V J I L N B Z C M W W
 4.   M V R M B U W F Z J J H E Q J J X G N C G W F D Y
 5.   F P E R W S B U H Z Y S L D P K T P I L X B M J Z
 6.   V M J E S H G Z Y S N I I Y B C N B Z P C W K E J
 7.   M F R T W G O Y U Y R E K W C T L Q F Z H O G G D
 8.   S R N M Z G U T I S L F U Q V I Q U Y J G A K U D
 9.   D M V B J N O Y L U O I S L V N P I C B B Z C M U
10.   Q M M G P X H S F C O K K T O C V L O K A M M T L
11.   X T R B I B U S E Y D F Y S K K A I C O B G T K Y
12.   L E N W P O Y E N N F T I C N S B B T R G Q R L O
13.   D M C E L S P U L C H R Y S S H Q I A G V P R A C
14.   X N W G P C Z L S I Y K O K K Y I I J Z J Y O R U
15.   W H R L U S L U T S A K C S V K G V O X T O E R D
16.   X N W G P C N F F X U V K D G U T I M X E R E H G
17.   H R X I M W G O A V Z Z X N S V H N E Y Q V I A O
18.   V E N W J O U A E T Y B H N I R F O J Y I V U A J
19.   X N W G P C N F F E F X C T U O E G S X M R W H D
20.   J B G N V I I O H M Z W O H E F M E F V J I X B N
21.   C P L E X X H W A S L X S H V G O D Y C N W I C R
22.   M V R M B U E F C L F P V V V D T M U S F D Y L B
23.   H R E S L A T Z S E A L D P J Q P O S B Z F F U F
24.   J H X E F M R N V P S T E N A D L D E Y X U U O T
25.   S N W G A R Y N I A O X C J S E N P V U K T N Q C
26.   W H R L U S L U Y L H N L D Q D E W H V U Y G N Y
```

Let us examine the individual and consolidated frequency tables for the first five columns.

TABLES

1.	X	I	W	M	F	V	S	D	Q	L	H	J	C
	卌		ǀǀǀ	ǀǀǀ		ǀǀ	ǀǀ	ǀǀ			ǀǀ	ǀǀ	

2.	R	W	H	V	P	M	F	T	E	N	B
	ǀǀǀǀ		ǀǀǀǀ	ǀǀ	ǀǀ	ǀǀǀǀ			ǀǀ	ǀǀǀǀ	

3.	B	P	W	R	E	J	N	V	M	C	X	G	L
			卌	卌 ǀ	ǀǀ		ǀǀǀ				ǀǀ		

4.	I	D	R	E	T	M	B	G	W	L	N	S
	ǀǀǀ			ǀǀǀǀ		ǀǀǀ	ǀǀ	卌	ǀǀ	ǀǀ		

5.	T	O	W	B	S	Z	J	P	I	L	U	M	V	X	F	A
			ǀǀǀ	ǀǀ			ǀǀ	卌		ǀǀ	ǀǀ					

1 & 2.	X	I	W	M	F	V	S	D	Q	L	H	J	C	R	P	T	E	N	B
	卌		ǀǀǀǀ	卌 ǀǀ	ǀǀ	ǀǀǀǀ	ǀǀ	ǀǀ			卌 ǀ	ǀǀ	·	ǀǀǀǀ	ǀǀ		ǀǀ	ǀǀǀǀ	

2 & 3.	R	W	H	V	P	M	F	T	E	N	B	J	C	X	G	L
	卌 卌	卌 ǀ	ǀǀǀǀ	ǀǀǀ	ǀǀǀ	卌			ǀǀǀǀ	卌 ǀǀ	ǀǀ			ǀǀ		

3 & 4.	B	P	W	R	E	J	N	V	M	C	X	G	L	I	D	T	S
	ǀǀǀ		卌 ǀǀ	卌 ǀǀ	卌 ǀ		ǀǀǀǀ		ǀǀǀǀ		ǀǀ	卌 ǀ	ǀǀǀ	ǀǀǀ			

4 & 5.	I	D	R	E	T	M	B	G	W	L	N	S	O	Z	J	P	U	V	X	F	A
	ǀǀǀǀ			ǀǀǀǀ	ǀǀ	ǀǀǀǀ	ǀǀǀǀ	卌	卌	ǀǀǀǀ		ǀǀ			ǀǀ	卌	ǀǀ				

1 & 2 & 3.	X	I	W	M	F	V	S	D	Q	L	H	J	C	R	P	T	E	N	B	G
	卌 ǀǀ		卌 ǀǀǀǀ	卌 ǀǀǀ	ǀǀ	卌	ǀǀ	ǀǀ		ǀǀ	卌 ǀ	ǀǀǀ	ǀǀ	卌 卌	ǀǀǀ		ǀǀǀǀ	卌 ǀǀ	ǀǀ	

2 & 3 & 4.	R	W	H	V	P	M	F	T	E	N	B	J	C	X	G	L	I	D	S
	卌 卌 ǀ	卌 ǀǀǀ	ǀǀǀǀ	ǀǀǀ	ǀǀǀ	卌 ǀǀǀ		ǀǀ	卌 ǀǀǀ	卌 ǀǀǀ	ǀǀǀǀ			ǀǀ	卌 ǀ	ǀǀǀ	ǀǀǀ		

3 & 4 & 5.	B	P	W	R	E	J	N	V	M	C	X	G	L	I	D	T	S	O	Z	U	F	A
	卌	卌 ǀ	卌 卌	卌 ǀǀ	卌 ǀ	ǀǀǀ	ǀǀǀǀ	ǀǀ	卌		ǀǀǀ	卌 ǀ	卌	ǀǀǀǀ		ǀǀ	ǀǀ			ǀǀ		

The first thing to do is to note and mark all recurrences; these have been indicated in the examples by bars over such recurrences.

An examination of the individual frequency tables shows that in the first column X, W, and M are the highest in frequency. Now if X is E, which is improbable, since E is not very high as an initial letter, then in the second column X should be high also, but since X does not appear in the second column, this assumption is not corroborated. The letters W or M may be E, and upon examination of the second column, it is seen that W occurs only once, while M occurs four times. We may assume therefore that M is E in columns 1 and 2. Now R is high in columns 2 and 3, and we may therefore assume R to be E in these two columns.

These values are substituted throughout the first three columns. In the fourth, seventh, and twenty-second messages the first three letters are E - E, with the first words of the fourth and twenty-second messages identical. The length of the word which recurs and the position of the E's suggest ENEMY. The frequency of V, which is assumed to be N, is good for this letter. Now the assumption of U for + gives us a clue to the lengths of other words, a clue of very great importance. The recurrences in messages 14, 16, and 19, are then noted. The frequency of X being high, in accordance with the frequency of initial letters,[1] X may be assumed to be T, and the words TRENCH and TRENCHES suggest themselves because of the indicated lengths and the positions of the high frequency letters. Note that N, which stands for R, is high in frequency and is combined as a digraph, NW, which equals RE, six times in columns 2, 3, and 4, and WG, occurring six times as a digraph, in columns 3 to 7, may well equal EN. In the first message we have TE as the beginning of a word. Now digraph RB (=E -) occurs in message eleven also (XTRB) and if we assume RB to equal EN, we would have TEN and TWENTY as the beginnings of these two messages. Note that in the case of the latter, U ends the word, which checks with a previous assumption.

In the seventh message we have MFRTWGOYU (=E - E - - - - -+). Now WG has been assumed to be EN, in messages 14, 16, and 19, and we may therefore assume this digraph to have the same values in the seventh message. E - E - EN - -+ suggests ELEVENTH. Messages 15 and 26 begin with the same word, represented by WHRLUSLU. Message 3 begins with the same two letters WH. A very probable beginning to fit these requirements is PR, which leads to the assumption of PREPARE for messages 15 and 26 and PROCEED for message 3. Corroboration is to be found in the frequency of digraph HR (=RE), four times. This gives us RE as the start of messages 17 and 23. The last E of PREPARE gives us L as the cipher equivalent of E in column 7. In the 18th message we have VENWJOU equals - - RE - -+. Now in message 7, O is equal to T and it may equal T in this case also, whereupon we would have - - RE - T+. In message 12 we would have - - RE - TH. The letter which precedes R is the same in both cases. The words which suggest themselves for trial are FIRE+TH - - - and DIRECT+. This would make the 6th message begin with DE. The 17th message begins HRXIMWGO for which we have RE - - - ENT. The word REGIMENT suggests itself for trial. In this M for M is corroborated by the M for M in the 4th and 22nd messages. The word may be REGIMENTAL because looking through the columns no other A's are seen, and this conflicts with the supposition that A equals +, whereas if the word really is REGIMENTAL, Z is +, and we have already indicated Z as + in the 3rd and 14th messages. Several other Z's also are seen in the adjacent columns. The 24th message begins -RTI, according to values secured from other places in the corresponding columns. The word

[1] See footnote to page 18.

ARTILLERY suggests itself. The check on the F (=L) is to be found in message 7. In like manner the initial words of the eighth and the twenty-third messages are assumed to be GERMAN and RETREAT respectively. The cipher letter S of the eighth message equaling G, the twenty-fifth message must also be assumed to start with G. From the nineteenth message NWG equals REN; hence we have GREN, which suggests GRENADE, or GRENADIER, or some similar term. The word SECTOR is found to be a probable beginning of the thirteenth message. The series of messages, now partially deciphered is as follows:

```
       1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
       __________
  1.   X  R  B  I  T  P  X  H  O  Y  L  N  W  C  F  Z  P  W  E  V  Y  D  T  C  R
       T  E  N  +
                T  H  +

  2.   I  W  P  I  O  Q  L  U  A  H  E  S  X  G  Q  L  X  K  I  L  B  O  D  F  T
          O     +        E  +
                T
       ____
  3.   W  H  W  D  W  W  R  Z  C  H  N  S  H  J  V  J  I  L  N  B  Z  C  M  W  W
       P  R  O  C  E  E  D

  4.   M  V  R  M  B  U  W  F  Z  J  J  H  E  Q  J  J  X  G  N  C  G  W  F  D  Y
       E  N  E  M  Y  +

  5.   F  P  E  R  W  S  B  U  H  Z  Y  S  L  D  P  K  T  P  I  L  X  B  M  J  Z
             T     E     Y  +

  6.   V  M  J  E  S  H  G  Z  Y  S  N  I  I  Y  B  C  N  B  Z  P  C  W  K  E  J
       D  E     T           +

  7.   M  F  R  T  W  G  O  Y  U  Y  R  E  K  W  C  T  L  Q  F  Z  H  O  G  G  D
       E  L  E  V  E  N  T  H  +

  8.   S  R  N  M  Z  G  U  T  I  S  L  F  U  Q  V  I  Q  U  Y  J  G  A  K  U  D
       G  E  R  M  A  N  +

  9.   D  M  V  B  J  N  O  Y  L  U  O  I  S  L  V  N  P  I  C  B  B  Z  C  M  U
       S  E  N  N                 +
                D

 10.   Q  M  M  G  P  X  H  S  F  C  O  K  K  T  O  C  V  L  O  K  A  M  M  T  L
          E        +
       _     _______
 11.   X  T  R  B  I  B  U  S  E  Y  D  F  Y  S  K  K  A  I  C  O  B  G  T  K  Y
       T  W  E  N  T  Y  +
          _______
 12.   L  E  N  W  P  O  Y  E  N  N  F  T  I  C  N  S  B  B  T  R  G  Q  R  L  O
       F  I  R  E  +  T  H

 13.   D  M  C  E  L  S  P  U  L  C  H  R  Y  S  S  H  Q  I  A  G  V  P  R  A  C
       S  E  C  T  O  R  +

       1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
       ________________
 14.   X  N  W  G  P  C  Z  I  S  I  Y  K  O  K  K  Y  I  I  J  Z  J  Y  O  R  U
       T  R  E  N  C  H  +

       ______________________
 15.   W  H  R  L  U  S  L  U  T  S  A  K  C  S  V  K  G  V  O  X  T  O  E  R  D
       P  R  E  P  A  R  E  +

       ______________________
 16.   X  N  W  G  P  C  N  F  F  X  U  V  K  D  G  U  T  I  M  X  E  R  E  H  G
       T  R  E  N  C  H  E  S  +
       ____
 17.   H  R  X  I  M  W  G  O  A  V  Z  Z  X  N  S  V  H  N  E  Y  Q  V  I  A  O
       R  E  G  I  M  E  N  T  A  L  +
          ____
 18.   V  E  N  W  J  O  U  A  E  T  Y  B  H  N  I  R  F  O  J  Y  I  V  U  A  J
       D  I  R  E  C  T  +  A
       _________________________
 19.   X  N  W  G  P  C  N  F  F  E  F  X  C  T  U  O  E  G  S  X  M  R  W  H  D
       T  R  E  N  C  H  E  S  +

 20.   J  B  G  N  V  I  I  O  H  M  Z  W  O  H  E  F  M  E  F  V  J  I  X  B  N

 21.   C  P  L  E  X  X  H  W  A  S  L  X  S  H  V  G  O  D  Y  C  N  W  I  C  R
                T
                I
       ________________
 22.   M  V  R  M  B  U  E  F  C  L  F  P  V  V  V  D  T  M  U  S  F  D  Y  L  B
       E  N  E  M  Y  +
       ____
 23.   H  R  E  S  L  A  T  Z  S  E  A  L  D  P  J  Q  P  O  S  B  Z  F  F  U  F
       R  E  T  R  E  A  T  +

 24.   J  H  X  E  F  M  R  N  V  P  S  T  E  N  A  D  L  D  E  Y  X  U  U  O  T
       A  R  T  I  L  L  E  R  Y  +
          ____
 25.   S  N  W  G  A  R  Y  N  I  A  O  X  C  J  S  E  N  P  V  U  K  T  N  Q  C
       G  R  E  N  A  D  E  +
                         I  E  R  +
       ______________________
 26.   W  H  R  L  U  S  L  U  Y  L  H  N  L  D  Q  D  E  W  H  V  U  Y  G  N  Y
       P  R  E  P  A  R  E  +
```

We now have sufficient probable values to attempt a reconstruction of the generating rectangle and the alphabets. We may not be able to do so, but it is possible that the tentative positions of letters may suggest values for some of the vacant spaces and may thus lead to the gradual decipherment.

Remembering the principles explained upon page 13, it will be seen that, from the partial decipherment already obtained, the following sequences are indicated, in which the dashes represent unknown letters:

Outer Alphabet	Inner Alphabet	
M-E	MR	E-Y
EO	RW	YC
OP	WL	X-I
PF	W-N	E-T
E-P	L-N	X-O
E-R	HN	C-P
R-G	NS	C-J
GT	SX	J-A
TI	XE	P-Z
YN	EI	U-Z
ND	IO	U-A
D-E	I-Y	ZA

Note the first few sequences given under the inner alphabet. It is evident that they may be consolidated into longer sequences by combining the individual sequences at the common letters. Thus, sequence MR can be combined with RW, the letter R being common to both pairs, making MRW. To the latter may be added L, given in the pair WL, making the sequence MRWL. Now the sequences W-N, and L-N, and the previous sequence MRWL show that a letter comes between W and N besides the letter L; and the sequence HN determines that H is the letter; this makes the sequence read MRWLHN. By continuing this process two fairly long sequences may be built up for the inner alphabet, and one for the outer alphabet, which sequences are then available for testing. They are as follows:

Outer Alphabet	Inner Alphabet
M-EOPFR-GTI	MRWLHNSXEIOTYC DJPUZA

By placing the sequence M-EOPFR-GTI upon one strip of cross-section paper and the sequence MRWLHNSXEIOTYC upon another, an attempt is made to corroborate such values as are already assigned and to secure further values. The first positions are thus:

```
Outer Alphabet—M-EOPFR-GTI
Inner Alphabet—  MRWLHNSXEIOTYC
```

Let us now attempt to add to these the values given by several of our tentatively deciphered words. For example, PROCEED adds the positions of Q and D, making the outer alphabet sequence read DMQEOPFR-GTI. The word GERMAN corroborates the placement of M between D and Q. TWENTY requires I to be one space removed from X in the inner alphabet, and SECTOR requires E to be the letter between these two, requirements which are justified and corroborated by the tentatively reconstructed partial sequences above. We may now join to the sequence of the outer alphabet the pair of letters YN given by our assumed sequences derived from the original decipherment. Thus:

```
Outer Alphabet—YNDMQEOPFR-GTI
Inner Alphabet—     MRWLHNSXEIOTYC
```

From these sequences we may attempt a direct reconstruction of the generating rectangles from which these alphabets have been derived. The process requires some ingenuity and the trials go much faster than the description. Taking the inner alphabet first, for example, we try to match sequences in sections such as might be produced by the use of a key word. Among other trials, the following looks most favorable:

```
-LE
-HI
MNO
RST
WXY
```

Noting a sequence given in the table of assumed sequences, viz., DJPUZA, we try to fit it into this tentative diagram. Thus:

```
-A-LE
D--HI
J-MNO
P-RST
U-WXY
Z
```

We may now assume the values suggested by the vacant spaces. The diagram is as follows:

```
-A-LE
DFGHI
JKMNO
PQRST
UVWXY
Z
```

The only values which have not been placed are B and C and we may make a guess at the key word CABLE and try out the alphabet which would be produced by it, by merely taking the successive columns in order. The alphabet is as follows:

```
C D J P U Z A F K Q V  B  G  M  R  W  L  H  N  S  X  E  I  O  T  Y
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

A trial of this alphabet brings out no inconsistencies and helps us to place additional values in our outer alphabet.

Trial of this alphabet on the partially deciphered messages results in the placing of the values of the outer alphabet as follows:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
+ S A - - - L - Y N  D  M  Q  E  O  P  F  R  -  G  T  I  H  -  -  -  -
```

A trial of these two alphabets on the second message produces the word HOSTILE immediately; and on the fifth message the trial results in the production of (B)ATTERY, which places B in the outer alphabet before Y. These two examples are sufficient to illustrate the process. The decipherer may then reconstruct the rectangle from which the outer alphabet was derived in the same way as before. It was found that the key word for the outer alphabet was SYNOPTIC and that the method of reading the columns was alternate vertical instead of simple vertical, as in the case of the inner alphabet. Even if the successive columns in the generating rectangle be taken in accordance with some key number, either independent of the key word used or based upon the same key word, the matching of sequences is not a difficult task. Only a little more ingenuity and care is required, but there is no doubt that the reconstruction is possible. Practice in such work is a great aid, and it has been found quite possible to reconstruct a generating rectangle from four or five letters, even when the most complicated method of taking the letters for the cipher alphabet has been employed. The plain text for the series of messages just deciphered is as follows:

```
 1. XRBITPXHOYLNWCFZPWEVYDTCR
    TENTH+REGIMENT+WILL+PREPA

 2. IWPIOQLUAHESXGQLXKILBODFT
    HOSTILE+AEROPLANE+OBSERVE

 3. WHWDWWRZCHNSHJVJILNBZCMWW
    PROCEED+IMMEDIATELY+TO+AS

 4. MVRMBUWFZJJHEQJJXGNCGWFDY
    ENEMY+MACHINE+GUN+LOCATED

 5. FPERWSBUHZYSLDPKTPILXBMJZ
    BATTERY+E+TENTH+FIELD+ART

 6. VMJESHGZYSNIIYBCNBZPCWKEJ
    DESTROY+TEMPORARY+TRESTLE

 7. MFRTWGOYUYREKWCTLQFZHOGGD
    ELEVENTH+INFANTRY+WILL+CO

 8. SRNMZGUTISLFUQVIQUYJGAKUD
    GERMAN+TRENCH+SECTOR+THRE

 9. DMVBJNOYLUOISLVNPICBBZCMU
    SEND+FIVE+GRENADIERS+TO+R

10. QMMGPXHSFCOKKTOCVLOKAMMTL
    NEED+REPAIRS+FOR+LEWIS+MA

11. XTRBIBUSEYDFYSKKAICOBGTKY
    TWENTY+PRIVATES+WERE+SEVE

12. LENWPOYENNFTICNSBBTRGQRLO
    FIRE+THREE+ROUNDS+EACH+AN

13. DMCELSPULCHRYSSHQIAGVPRAC
    SECTOR+SEVENTEEN+EVACUATE

14. XNWGPCZLSIYKOKKYIIJZJYORU
    TRENCH+MORTARS+REQUIRED+F

15. WHRLUSLUTSAKCSVKGVOXTOERD
    PREPARE+TO+ATTACK+ENEMY+E

16. XNWGPCNFFXUVKDGUTIMXEREHG
    TRENCHES+EVACUATED+BY+BAV

17. HRXIMWGOAVZZXNSVHNEYQVIAO
    REGIMENTAL+COMMANDER+SEVE

18. VENWJOUAETYBHNIRFOJYIVUAJ
    DIRECT+ARTILLERY+FIRE+THR

19. XNWGPCNFFEFXCTUOEGSXMRWHD
    TRENCHES+OCCUPIED+BY+SAXO

20. JBGNVIIOHMZWOHEFMEFVJIXBN
    AMMUNITION+DUMP+LOCATED+B

21. CPLEXXHWASLXSHVGODYCNWICR
    CAPTURED+ENEMY+AEROPLANE+

22. MVRMBUEFCLFPVVVDTMUSFDYLB
    ENEMY+RAID+HAS+RESULTED+I

23. HRESLATZSEALDPJQPOSBZFFUF
    RETREAT+OF+DIVISION+THIRT

24. JHXEFMRNVPSTENADLDEYXUUOT
    ARTILLERY+FIRE+INTERMITTE

25. SNWGARYNIAOXCJSENPVUKTNQC
    GRENADIER+REGIMENT+TWELVE

26. WHRLUSLUYLHNLDQDEWHVUYGNY
    PREPARE+IMMEDIATELY+TO+LE
```

In the case of only a few messages, perhaps five or six, in the same alphabets and key letter, a little experimentation, with no attempts whatsoever at decipherment, will often bring results when everything else has failed. By using as a basis the frequency tables for the individual columns, attempts should be made to find the successive encipherments of

E, or +. Often a sequence of four or five letters found in this manner will give a clue to the arrangement of the letters in the generating rectangle of the inner alphabet. If the latter can be reconstructed correctly, even in part, a great step forward has been made in the decipherment. The problem has thus been resolved into a case where only one of the alphabets is unknown; consequently the procedure from that point is comparatively easy and rapid. Take for example the first six messages in the series just discussed. From the frequency tables of combined columns, the cipher letters M, R, W, and L might readily be assumed to be the successive representatives of the text letter E or +, or both, and the sequence MRWL might be one of several tentative sequences to be tested. By experimenting with this sequence the following diagram would be found to be possible:

```
-L
--
M
R
W
```

To this could be added probable values as follows:

```
    (1)                    (2)                    (3)

---L-                  ---L-                  ---L-
-----      ⟶           DFG--      ⟶           DFGHI
--M--                  JKM--                  JKMNO
--R--                  PQR--                  PQRST
--W--                  UVW--                  UVWXY
                       Z                      Z
```

Comparison with the correct generating rectangle will show that the one built upon these four letters alone is nearly correct. By assuming only a few words based upon the positions of the E's, a partial decipherment can be obtained, and from that a reconstruction of the generating rectangle for the outer alphabet can be made.

A SINGLE MESSAGE

The solution of a series of messages has just been given. The solution of a single long message is also possible, by determining the cycles by the method given on page 14, writing out the message on lines of cross-section paper, and arranging them so as to bring the greatest number of recurrences in adjacent columns.

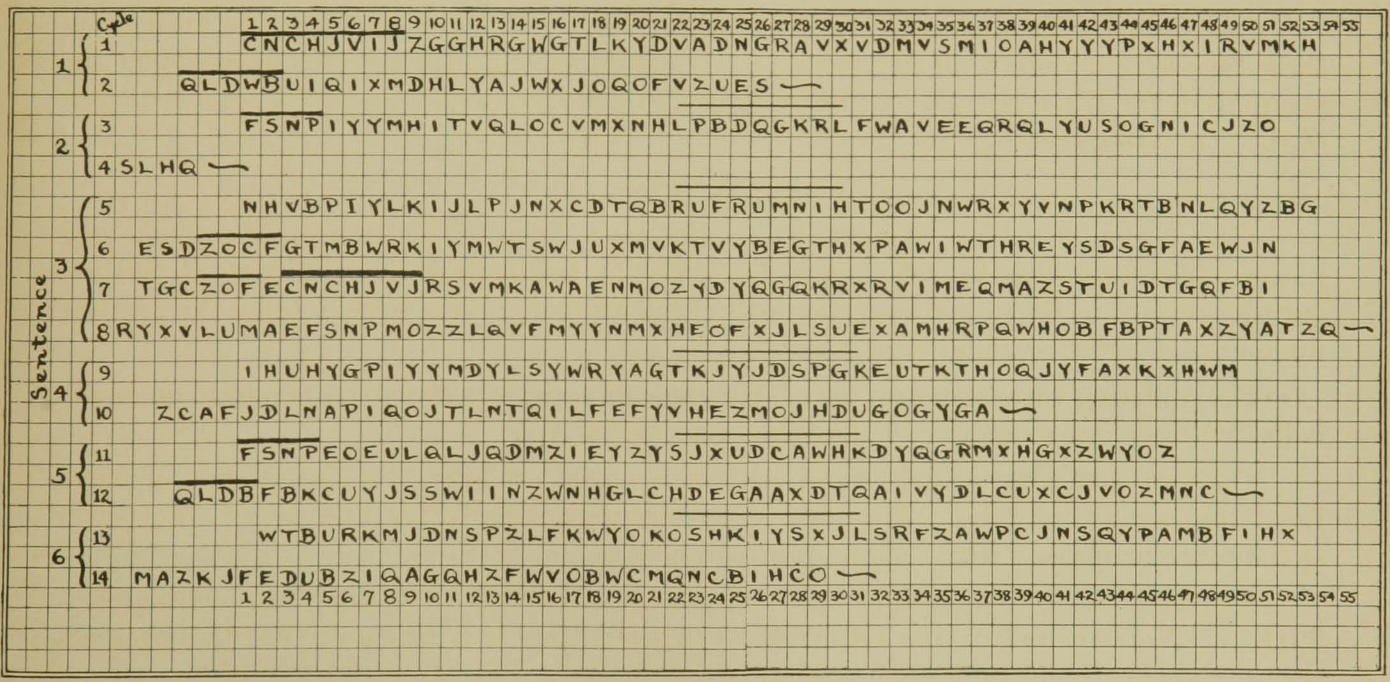
The following case is an example. The message, which is shown on the page opposite, is known to be one dealing with the submarine warfare.

The letters of this message have been rearranged according to the method outlined for determining the cycles. The recurrences are indicated by the lines above the corresponding recurrences. Fig. 7 shows the arrangement.

Now it is natural to assume that the polygraph FSNP, beginning two sentences is THE+. Note the polygraphs QLDWB and QLDBFB. It is probable that Q represents the + sign for it not only begins these two polygraphs but the last letter of the second sentence is Q which we are sure indicates the + sign. Assuming that B represents the +

MESSAGE

```
CNCHJ VIJZG GHRGW GTLKY DVAWN GRAVX VDMVS MIOAH YYYPX
HXIRV MKHQL DWBUI QIXMD HLYAJ WXJOQ OFVZU ES-FS NPIYY
MHITV QLOCV MXNHL PBDQG KRLFW AVEEQ RQLYU SOGNI CJZOS
LHQ-N HVBPI YLKIJ LPJNX CDTQB RUFRU MNIHI OOJNW RXYVN
PKRTB NLQYZ BGESD ZOCFG TMBWR KIYMW TSWJU XMVKT VYBEG
THXPA WIWTH REYSD SGFAE WJNTG CZOFE CNCHJ VJRSV MKAWA
ENMOZ YDYQG QKRXR VIMEQ MAZST UIDTG QFBIR YXVLU MAEFS
NPMOZ ZLQVF MYYNM XHEOF XJLSU EXAMH RPQWH OBFBP TAXZY
ATZQ- IHUHY GPIYY MDYLS YWRWA GTKJY JDSPG KEUTK THOQJ
YFAXK XHWMZ CAFJD LNAPI QOJTL NTQIL FEFYV HEZMO JHDUG
OGYGA -FSNP EOEUL QLJQD MZIEY ZYSJX UDCAW HKDYQ GRMXH
GXZWY OZQLD BFBKC UYJSS WIINZ WNHGL CHDEG AAXDT QAIVY
DLCUX CJVOZ MNCWT BURKM JDNSP ZLFKW YOKOS HKIYS XJLSR
FZAWP CJNSQ YPAMB FIHXM AZKJF EDUBZ IQAGQ HZFWV OBWCM
QNCBI HCO-
```



```
Sentence Cycle                     1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55
       1     1                     C  N  C  H  J  V  I  J  Z  G  G  H  R  G  W  G  T  L  K  Y  D  V  A  D  N  G  R  A  V  X  V  D  M  V  S  M  I  O  A  H  Y  Y  Y  P  X  H  X  I  R  V  M  K  H
             2           Q  L  D  W  B  U  I  Q  I  X  M  D  H  L  Y  A  J  W  X  J  O  Q  O  F  V  Z  U  E  S  —
       2     3                     F  S  N  P  I  Y  Y  M  H  I  T  V  Q  L  O  C  V  M  X  N  H  L  P  B  D  Q  G  K  R  L  F  W  A  V  E  E  Q  R  Q  L  Y  U  S  O  G  N  I  C  J  Z  O
             4     S  L  H  Q  —
       3     5                     N  H  V  B  P  I  Y  L  K  I  J  L  P  J  N  X  C  D  T  Q  B  R  U  F  R  U  M  N  I  H  T  O  O  J  N  W  R  X  Y  V  N  P  K  R  T  B  N  L  Q  Y  Z  B  G
             6        E  S  D  Z  O  C  F  G  T  M  B  W  R  K  I  Y  M  W  T  S  W  J  U  X  M  V  K  T  V  Y  B  E  G  T  H  X  P  A  W  I  W  T  H  R  E  Y  S  D  S  G  F  A  E  W  J  N
             7        T  G  C  Z  O  F  E  C  N  C  H  J  V  J  R  S  V  M  K  A  W  A  E  N  M  O  Z  Y  D  Y  Q  G  Q  K  R  X  R  V  I  M  E  Q  M  A  Z  S  T  U  I  D  T  G  Q  F  B  I
             8     R  Y  X  V  L  U  M  A  E  F  S  N  P  M  O  Z  Z  L  Q  V  F  M  Y  Y  N  M  X  H  E  O  F  X  J  L  S  U  E  X  A  M  H  R  P  Q  W  H  O  B  F  B  P  T  A  X  Z  Y  A  T  Z  Q  —
       4     9                     I  H  U  H  Y  G  P  I  Y  Y  M  D  Y  L  S  Y  W  R  Y  A  G  T  K  J  Y  J  D  S  P  G  K  E  U  T  K  T  H  O  Q  J  Y  F  A  X  K  X  H  W  M
            10           Z  C  A  F  J  D  L  N  A  P  I  Q  O  J  T  L  N  T  Q  I  L  F  E  F  Y  V  H  E  Z  M  O  J  H  D  U  G  O  G  Y  G  A  —
       5    11                     F  S  N  P  E  O  E  U  L  Q  L  J  Q  D  M  Z  I  E  Y  Z  Y  S  J  X  U  D  C  A  W  H  K  D  Y  Q  G  R  M  X  H  G  X  Z  W  Y  O  Z
            12              Q  L  D  B  F  B  K  C  U  Y  J  S  S  W  I  I  N  Z  W  N  H  G  L  C  H  D  E  G  A  A  X  D  T  Q  A  I  V  Y  D  L  C  U  X  C  J  V  O  Z  M  N  C  —
       6    13                        W  T  B  U  R  K  M  J  D  N  S  P  Z  L  F  K  W  Y  O  K  O  S  H  K  I  Y  S  X  J  L  S  R  F  Z  A  W  P  C  J  N  S  Q  Y  P  A  M  B  F  I  H  X
            14        M  A  Z  K  J  F  E  D  U  B  Z  I  Q  A  G  Q  H  Z  F  W  V  O  B  W  C  M  Q  N  C  B  I  H  C  O  —
                                   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55
```

FIG. 7. SHOWING THE SINGLE LONG MESSAGE SEPARATED INTO ITS CONSTITUENT CYCLES

sign, the word may be either a two-letter one, which could have an additional letter at the end, such as for example AN and ANY, or it could be a three-letter one, with the same sort of a possibility, such as THE and THIS or THAT. If the words are THE and THAT, then since BFB would represent AT+ it would mean that in the outer alphabet the letter A would follow the + sign, a condition of high probability if the columns of the generating rectangle had been taken in accordance with the numerical key determined by the key word.

Now note the polygraphs CNCHJVIJ and CNCHJVJ. We may assume that N represents E, because it has been assumed to be E in the words THE and it occurs seven times in the columns adjacent to this column. Now since it has been assumed that the sequence of the outer alphabet begins + A, then it may well be that in this case also the J represents A and +, making these two polygraphs as follows:

```
CNCHJVIJ                   CNCHJVJ
-E--A--+                   -E--A-+
```

Considering the nature of the message, among the words which suggest themselves the words GERMANS (this word was later found to be GERMANY) and GERMAN might fit nicely. If so, then a probable word to precede the latter would be THE.

Let us now collate all the data that is possible in order to attempt a reconstruction of the generating rectangle.

The sequences which may be assumed from the tentatively deciphered material are these:

Outer alphabet	Inner alphabet
+A	F-N
RG	WN
	LF
	P-J
	BP
	C-E
	CQE
	EB
	Z-F
	DS
	OD

Consolidation of the several sequences indicated under the inner alphabet results as follows:

```
CQEBP-JZLFWN     ........     ODS
```

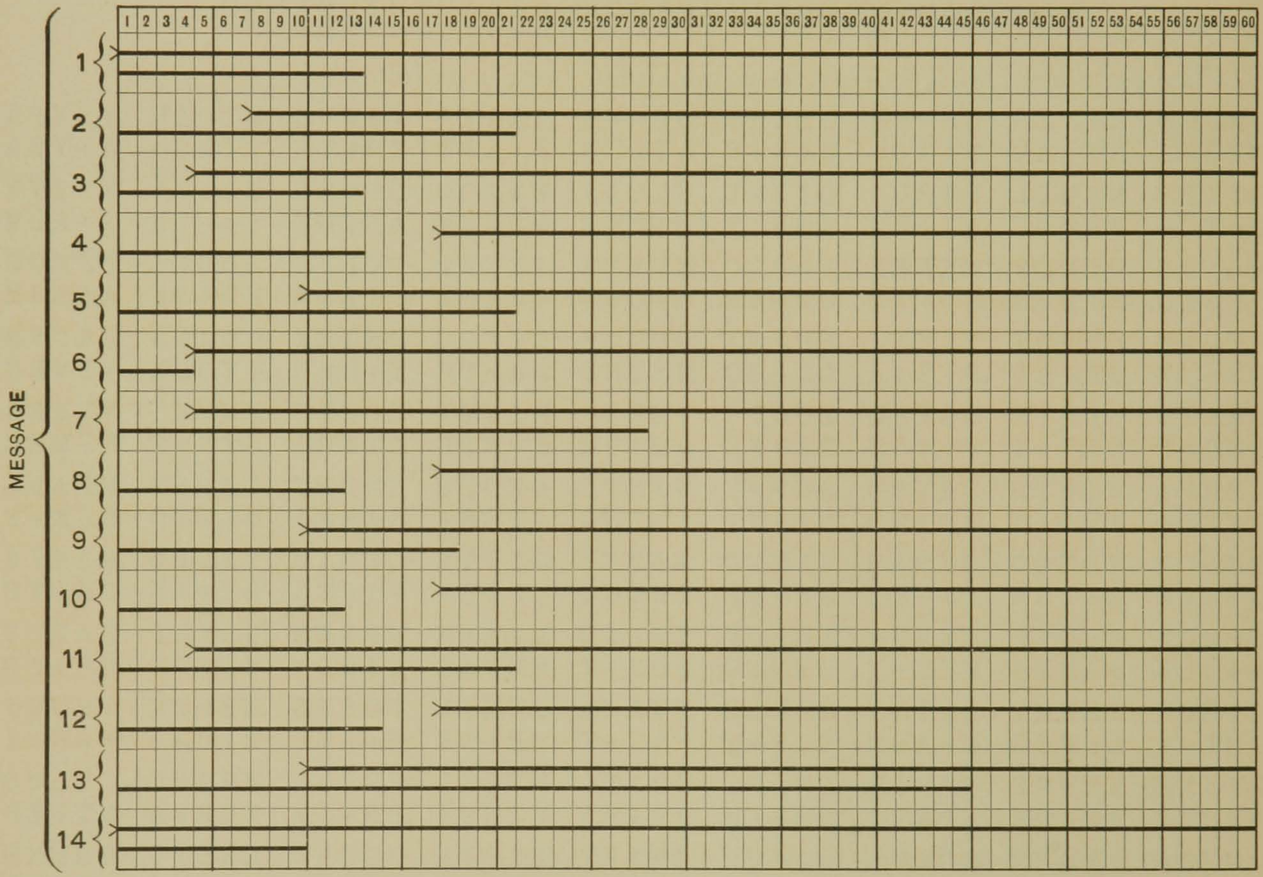
A few experiments with these sequences for the inner alphabet leads to the assumption of a rectangle of two rows of nine letters and one of seven. After some trials of key words like EVALUTION (from *evaluation*), and EVOLUTIN (from *evolution*), the word REVOLUTIN (from *revolution*) suggests itself. A trial of this alphabet furnishes a check upon the material already deciphered and soon suggests new values. For example, the fifth sentence is found to begin thus: THE + GERMAN + GOVERNMENT. Enough has been said in the preceding pages to make further explanation unnecessary. From the new values, an attempt is made to reconstruct the generating rectangle for the outer alphabet with the result that it is soon found to be AMERICAN. The entire message may now be solved with ease. The two generating rectangles and the alphabets which were derived from them, by taking the columns in accordance with the numerical key based upon the same key words, are as follows:

```
1537426                  619538724
AMERICN                  REVOLUTIN
BDFGHJK                  ABCDFGHJK
LOPQSTU                  MPQSWXYZ
VWXYZ

                 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
Outer alphabet:  + A B L V C J T E F  P  X  I  H  S  Z  M  D  O  W  N  K  U  R  G  Q  Y
Inner alphabet:  E B P I J Z L F W N  K  O  D  S  R  A  M  T  H  Y  U  G  X  V  C  Q
                 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The plain text, with its corresponding cipher text, is as follows:

```
CNCHJ VIJZG GHRGW GTLKY DVAWN GRAVX VDMVS MIOAH YYYPX
GERMA NY+AD MITS+ HER+F AILUR E+AFT ER+TR YING+ A+YEA

HXIRV MKHQL DWBUI QIXMD HLYAJ WXJOQ OFVZU ES-FS NPIYY
R+TO+ WIN+T HE+WA R+WIT H+HER +SUBM ARINE S+-TH E+ADM

MHITV QLOCV MXNHL PBDQG KRLFW AVEEQ RQLYU SOGNI CJZOS
ISSIO N+COM ES+FR OM+HE R+OWN +EXPE RTS+A ND+ST ATESM

LHQ-N HVBPI YLKIJ LPJNX CDTQB RUFRU MNIHI OOJNW RXYVN
EN+-F OR+AB OVE+A LL+CO NTINU ES+TH E+NEW +YORK +EVEN

PKRTB NLQYZ BGESD ZOCFG TMBWR KIYMW TSWJU XMVKT VYBEG
ING+P OST+I T+COM ES+FR OM+TH E+MIL ITARI STS+T HEMSE

THXPA WIWTH REYSD SGFAE WJNTG CZOFE CNCHJ VJRSV MKAWA
LVES+ WHO+A RE+NO W+INV ITING +THE+ GERMA N+PEO PLE+T

ENMOZ YDYQG QKRXR VIMEQ MAZST UIDTG QFBIR YXVLU MAEFS
O+TAK E+THE IR+EY ES+PE ERING +FOR+ VICTO RY+FR OM+TH

NPMOZ ZLQVF MYYNM XHEOF XJLSU EXAMH RPQWH OBFBP TAXZY
E+SEA +AND+ FIX+T HEM+U PON+T HE+AL LIED+ WESTE RN+FR

ATZQ- IHUHY GPIYY MDYLS YWRWA GTKJY JDSPG KEUTK THOQJ
ONT+- LONDO N+ADM ITS+T HAT+T HE+NE W+AME RICAN +ANTI

YFAXK XHWMZ CAFJD LNAPI QOJTL NTQIL FEFYV HEZMO JHDUG
+SUBM ARINE +DEVI CES+A RE+HA VING+ AN+IM PORTA NT+EF

OGYGA -FSNP EOEUL QLJQD MZIEY ZYSJX UDCAW HKDYQ GRMXH
FECT+ -THE+ GERMA N+GOV ERNME NT+DE CREED +ON+J ANUAR

GXZWY OZQLD BFBKC UYJSS WIINZ WNHGL CHDEG AAXDT QAIVY
Y+FIR ST+TH AT+FR OM+FE BRUAR Y+FIR ST+SE A+TRA FFIC+

DLCUX CJVOZ MNCWT BURKM JDNSP ZLFKW YOKOS HKIYS XJLSR
WILL+ BE+ST OPPED +WITH +EVER Y+AVA ILABL E+WEA PON+A

FZAWP CJNSQ YPAMB FIHXM AZKJF EDUBZ IQAGQ HZFWV OBWCM
ND+WI THOUT +FURT HER+N OTICE +IN+V ARIOU S+BLO CKADE

QNCBI HCO-
D+ZON ES+-
```

On page 8 it was stated that the analysis with regard to the Wheatstone cipher, to the effect that the system involves two keys, (1) the disposition of the letters of the cryptographic alphabet, and (2) the starting point, was correct. We may therefore amend this statement by saying that the foregoing modification adds a third key to the system which complicates the case considerably; but notwithstanding, a single message of sufficient length may be solved. As to the key concerned with the starting point, it is certainly true that this might constitute an important safeguard; yet, given a series of short messages, perhaps fifty of them in the same alphabets, but in different key letters (i. e., different starting points) it would be possible to arrange the messages in the same way that the cycles constituting a single long message are arranged. The solution would be somewhat easier because considerable help would be furnished by the clues offered by the initial words, clues which may be applied to the corresponding sections of the cycles above and below the places where the initial words occur. A diagrammatic sketch of such a condition would be as follows:



Here the section included by columns 5-10 would be aided by the tentative decipherment of the initial words of the third, sixth, seventh, and eleventh messages; the section included by columns 10-15 would be aided in a like manner by the initial words of the fifth, ninth, and thirteenth messages, etc.

In conclusion it may be said that the chief advantages of this system are (1) its simplicity of operation and (2) its adaptability; the chief disadvantages are (1) the relatively low degree of safety afforded, and (2) the possibilities of errors, the effect of which are progressive and which may cause considerable confusion.

III. A MULTIPLEX ALPHABET SYSTEM[1]

1. THE APPARATUS

In 1891, Commandant Bazeries, a noted French cipher expert, invented a rather ingenious mechanical enciphering device, called the "Cylindrical Cryptograph," the principles of which are worthy of study.

Fig. 8 illustrates the apparatus. A description of it, taken from Bazeries' work,[2] is as follows:

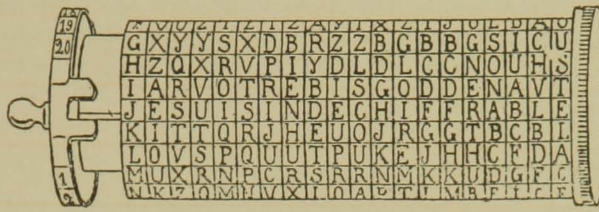

19
20
1
G X Y Y S X D B R Z Z B G B B G S I C U
H Z Q X R V P I Y D L D L C C N O U H S
I A R V O T R E B I S G O D D E N A V T
J E S U I S I N D E C H I F F R A B L E
K I T T Q R J H E U O J R G G T B C B I
L O V S P Q U U T P U K E J H H C F D A
M U X R N P C R S R R N M K K U D G F C

Fig. 8

The apparatus consists of the following parts:

1. A cylindrical body, terminated at one extremity by a disk permanently fixed to the cylinder and bearing an indicator in the shape of a forked finger; at the other extremity by a milled disk, which screws onto the cylinder.

2. Twenty alphabets, each of twenty-five letters (Latin Script) in the form of rings which encircle the cylinder, the sequence in each alphabet being different from that in all the other alphabets. Each one bears a number on one side.

3. A stop-pin, the head of which can be screwed into the fixed disk, and the stem of which, partially sunk into a groove running longitudinally on the cylinder, fits into notches on the inner side of the alphabet-rings, which notches correspond in position with the letters on the outer side.

The Key.—This is secured from the order in which the alphabet rings are placed on the cylinder. This order is derived from a word which is repeated until there is a total of twenty letters. To transcribe this word into numbers, a figure 1 is written beneath the letter which comes first in the normal alphabet; if it is repeated the second time it becomes number 2, a third time, number 3, etc. Then the letter which comes next in the normal alphabet is numbered in sequence, etc., until all the letters have been numbered. The following example illustrates the process:

Key-word—	B	A	T	A	I	L	L	O	N
	II	I	VII	(I)	III	IV	(IV)	VI	V

Here the roman numbers indicate the relative positions of the letters of this key-word as regards their order in the normal alphabet.

Numerical Transformation	B	A	T	A	I	L	L	O	N	B	A	T	A	I	L	L	O	N	B	A
	6	1	19	2	9	11	12	17	15	7	3	20	4	10	13	14	18	16	8	5

Setting the apparatus according to the key, that is, arranging the various alphabet rings in accordance with the succession of numbers given by this numerical key, the successive rings are so adjusted

[1] This particular system has been referred to by us, as a matter of convenience, as the Star Cipher.

[2] Les Chiffres Secrets Dévoilés, Paris, 1901, pages 250-261.

> in relation to each other as to spell out in the line indicated by the forked finger the first twenty letters of the plain text. The successive rings are fixed one after the other during the process by pushing the stop-pin forward and thus through each ring as it comes into position. The cipher line is one single line taken from among the other horizontal lines. This operation is repeated for the next twenty letters and so on until the entire message has been enciphered. The process of decipherment is simply the reverse of the process of encipherment. The first series of twenty cipher letters being brought on the line opposite the indicator, the successive horizontal lines are inspected and the line containing the plain text will be found immediately, because it will be the only one which presents an assemblage of letters forming intelligible words.
>
> *
>
> The cylindrical cryptograph inaugurates a new method in cryptography. The principle is the following: the simultaneous employment of a multiplicity of alphabets for the encipherment of one and the same dispatch. The apparatus does not need to be kept in concealment, since it does not betray the secret, on condition of course that it be taken apart. The operation of it is simple and rapid and the indecipherability absolute. There is nothing kept secret except the key-word.
>
> *
>
> The number of interchangeable alphabets being 20, the number of combinations is given by the formula of permutations which can be made with 20 different objects, and is as follows: $1\times2\times3\times4\times5\times6\times7\times8\times9\times10\times11\times12\times13\times14\times15\times16\times17\times18\times19\times20=$ approximately two quintillions (2,000,000,000,000,000,000).

Bazeries goes on to say that since there are 25 combinations in each alphabet, the true number of combinations is 2 quintillions raised to the 25th power. But he is quite willing to stop at the 2 quintillions post!

> A strong-box having four alphabets of 25 letters gives as the number of combinations $25^4=390{,}625$. In comparing the security of such a strong-box with that of the cylindrical cryptograph, the reader can ascertain that it is 5 trillion times as easy to open a strong-box of which one does not know the combination, as to decipher a cryptogram made by means of the cylindrical cryptograph if one does not possess the key word.

Truly these statements sound staggering and should be enough to discourage any attempts at solving such an impregnable system. But the long experience of decipherers has taught them that such statements usually cloak a complexity which is only superficial. We shall see the very different conclusions which another cipher expert reached with respect to Bazeries' system.

The French cipher expert De Viaris[1] has given a very ingenious method for solving a single message enciphered by means of such a system, and it is thought that an exposition of the method would be desirable for the use of students who do not have access to the original and who would be desirous of experimenting with such a system without going through the labor of compiling the necessary tables.

The method discussed below has been based directly upon the description given by this decipherer and a few short cuts have been developed which seem worthy of incorporation with the principles laid down by him. In order to illustrate the method, a series of

[1] L'Art de Dèchiffrer les Depêches Secrèts, Paris, 1893 and 1895, pp. 50-52; 99-109.

mixed alphabets, arranged by Colonel Parker Hitt, given in Fig. 9 on page 40, will be used. Since ordinary sliding strips bearing double alphabets will produce the same results as single alphabets mounted upon wheels, and since in decipherment the several alphabets must be capable of being quickly and easily rearranged, they were written on cross-section paper, numbered, and then mounted upon strips of wood fourteen inches long, one-half inch wide, and one-fourth inch thick.

Two basic assumptions will be made:

(1) The enemy has possession of the apparatus, along with a knowledge of all the details of the system, a premise which has been granted since the time of Kerckhoffs, who included the condition stated above in the enumeration of his requirements of field ciphers.

(2) The apparatus is so arranged that the same number of alphabets is used invariably. Accordingly, if the system comprises a total of twenty-five mixed alphabets, the apparatus is such that all twenty-five alphabets must be used every time.

Granting the first assumption, the only requisite to the decipherment of a message is the compilation of a series of *Synoptic Tables.*[1] Briefly, these tables are merely the tabulated record of the quadricular or square tables which result when all the cipher alphabets are arranged or adjusted so that any given letter of the normal alphabet can be read all the way across. When all the alphabets are "set" so that all the A's, for example, are brought into one horizontal line, the synoptic table for the letter A results, from which can be ascertained what letters will represent A in any given horizontal line. There will be generated in an alphabet of twenty-six letters, twenty-five such horizontal lines, and for this reason, each horizontal line is called a *generatrix.*

In his exposition of the method of solution, De Viaris states that he asked Bazeries first to give him a message and to indicate the generatrix number for each cipher line. This message he deciphered. Then he asked Bazeries for another message and requested that he be told a single word in it. The decipherer was also successful in this case. Finally, he was given three messages with only the information that they were all in the same key. De Viaris succeeded in solving these also.

Since these three examples represent a series of cases of increasing complexity, the same method of exposition will be used here, inasmuch as they afford a clarity of illustration such as is best suited to the purpose in hand.

[1] All the synoptic tables, alphabetically arranged, will be found on page 59 ff.

ALPHABETS FOR THE STAR CIPHER

A	X	Q	J	X	H	F	C	G	D	B	W	M	Y	P	L	O	E	U	I	X	S	N	T	R	0
E	U	V	K	Z	N	T	D	B	F	C	G	P	L	W	M	Y	I	A	O	Z	V	R	H	S	1
I	A	O	Q	J	R	H	S	C	G	D	B	F	M	Y	P	L	W	E	U	J	X	Q	N	T	2
O	E	U	I	K	S	N	T	R	B	F	C	G	D	L	W	M	Y	P	A	K	Z	V	K	H	3
U	I	A	O	E	T	R	H	S	N	G	D	B	F	C	Y	P	L	W	M	Q	J	X	Q	J	4
H	O	E	U	I	L	S	N	T	R	A	F	C	G	D	V	W	M	Y	P	V	K	Z	V	K	5
N	T	I	A	O	M	Y	R	H	S	E	U	D	B	F	X	Q	P	L	W	B	Q	J	X	Q	6
R	H	S	E	U	P	L	W	N	T	I	A	O	C	G	Z	V	K	M	Y	C	G	K	Z	V	7
S	N	T	R	A	W	M	Y	P	H	O	E	U	I	B	J	X	Q	J	L	D	B	F	J	X	8
T	R	H	S	N	Y	P	L	W	M	U	I	A	O	E	K	Z	V	K	Z	F	C	G	D	Z	9
B	S	N	T	R	A	W	M	Y	P	Q	O	E	U	I	Q	J	X	Q	J	G	D	B	F	C	10
C	G	R	H	S	E	U	P	L	W	V	K	I	A	O	H	K	Z	V	K	L	F	C	G	D	11
D	B	F	N	T	I	A	O	M	Y	X	Q	J	E	U	N	T	J	X	Q	M	Y	D	B	F	12
F	C	G	D	H	O	E	U	I	L	Z	V	K	Z	A	R	H	S	Z	V	P	L	W	C	G	13
G	D	B	F	C	U	I	A	O	E	J	X	Q	J	X	S	N	T	R	X	W	M	Y	P	B	14
L	F	C	G	D	K	O	E	U	I	K	Z	V	K	Z	T	R	H	S	N	Y	P	L	W	M	15
M	Y	D	B	F	Q	J	I	A	O	H	J	X	Q	J	B	S	N	T	R	A	W	M	Y	P	16
P	L	W	C	G	V	K	Z	E	U	N	T	Z	V	K	C	G	R	H	S	E	U	P	L	W	17
W	M	Y	P	B	X	Q	J	X	A	R	H	S	X	Q	D	B	F	N	T	I	A	O	M	Y	18
Y	P	L	W	M	Z	V	K	Z	V	S	N	T	R	V	F	C	G	D	H	O	E	U	I	L	19
J	W	M	Y	P	J	X	Q	J	X	T	R	H	S	N	G	D	B	F	C	U	I	A	O	E	20
K	Z	P	L	W	B	Z	V	K	Z	L	S	N	T	R	A	F	C	G	D	H	O	E	U	I	21
Q	J	X	M	Y	C	G	X	Q	J	M	Y	R	H	S	E	U	D	B	F	N	T	I	A	O	22
V	K	Z	V	L	D	B	F	V	K	P	L	W	N	T	I	A	O	C	G	R	H	S	E	U	23
X	Q	J	X	Q	F	C	G	D	Q	W	M	Y	P	H	O	E	U	I	B	S	N	T	R	A	24
Z	V	K	Z	V	G	D	B	F	C	Y	P	L	W	M	U	I	A	O	E	T	R	H	S	N	25
A	X	Q	J	X	H	F	C	G	D	B	W	M	Y	P	L	O	E	U	I	X	S	N	T	R	0
E	U	V	K	Z	N	T	D	B	F	C	G	P	L	W	M	Y	I	A	O	Z	V	R	H	S	1
I	A	O	Q	J	R	H	S	C	G	D	B	F	M	Y	P	L	W	E	U	J	X	Q	N	T	2
O	E	U	I	K	S	N	T	R	B	F	C	G	D	L	W	M	Y	P	A	K	Z	V	K	H	3
U	I	A	O	E	T	R	H	S	N	G	D	B	F	C	Y	P	L	W	M	Q	J	X	Q	J	4
H	O	E	U	I	L	S	N	T	R	A	F	C	G	D	V	W	M	Y	P	V	K	Z	V	K	5
N	T	I	A	O	M	Y	R	H	S	E	U	D	B	F	X	Q	P	L	W	B	Q	J	X	Q	6
R	H	S	E	U	P	L	W	N	T	I	A	O	C	G	Z	V	K	M	Y	C	G	K	Z	V	7
S	N	T	R	A	W	M	Y	P	H	O	E	U	I	B	J	X	Q	J	L	D	B	F	J	X	8
T	R	H	S	N	Y	P	L	W	M	U	I	A	O	E	K	Z	V	K	Z	F	C	G	D	Z	9
B	S	N	T	R	A	W	M	Y	P	Q	O	E	U	I	Q	J	X	Q	J	G	D	B	F	C	10
C	G	R	H	S	E	U	P	L	W	V	K	I	A	O	H	K	Z	V	K	L	F	C	G	D	11
D	B	F	N	T	I	A	O	M	Y	X	Q	J	E	U	N	T	J	X	Q	M	Y	D	B	F	12
F	C	G	D	H	O	E	U	I	L	Z	V	K	Z	A	R	H	S	Z	V	P	L	W	C	G	13
G	D	B	F	C	U	I	A	O	E	J	X	Q	J	X	S	N	T	R	X	W	M	Y	P	B	14
L	F	C	G	D	K	O	E	U	I	K	Z	V	K	Z	T	R	H	S	N	Y	P	L	W	M	15
M	Y	D	B	F	Q	J	I	A	O	H	J	X	Q	J	B	S	N	T	R	A	W	M	Y	P	16
P	L	W	C	G	V	K	Z	E	U	N	T	Z	V	K	C	G	R	H	S	E	U	P	L	W	17
W	M	Y	P	B	X	Q	J	X	A	R	H	S	X	Q	D	B	F	N	T	I	A	O	M	Y	18
Y	P	L	W	M	Z	V	K	Z	V	S	N	T	R	V	F	C	G	D	H	O	E	U	I	L	19
J	W	M	Y	P	J	X	Q	J	X	T	R	H	S	N	G	D	B	F	C	U	I	A	O	E	20
K	Z	P	L	W	B	Z	V	K	Z	L	S	N	T	R	A	F	C	G	D	H	O	E	U	I	21
Q	J	X	M	Y	C	G	X	Q	J	M	Y	R	H	S	E	U	D	B	F	N	T	I	A	O	22
V	K	Z	V	L	D	B	F	V	K	P	L	W	N	T	I	A	O	C	G	R	H	S	E	U	23
X	Q	J	X	Q	F	C	G	D	Q	W	M	Y	P	H	O	E	U	I	B	S	N	T	R	A	24
Z	V	K	Z	V	G	D	B	F	C	Y	P	L	W	M	U	I	A	O	E	T	R	H	S	N	25
★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

Fig. 9

2. SOLUTION OF A MESSAGE WHEN THE GENERATRICES USED ARE KNOWN TO THE DECIPHERER

The following message has been enciphered on this system for the purpose of illustrating certain principles which will be used in solving such a message:

MESSAGE

	Column—	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15	16 17 18 19 20	21 22 23 24 25
Generatrix—	7.	DSGDX	KUCPW	YRZJF	GSGQX	VWNJG
"	12.	KGNVR	WQFKI	NDDIZ	TGRFA	GYEPS
"	18.	XEBBG	KVILF	ZDYXF	SQXXL	CSXDV
"	6.	BGVQC	EVNWP	OWKEH	SPYLT	INYGX
"	9.	KGOOS	ACPCA	OGXTO	JXKXT	ZLGIK
"	8.	DPIOS	IOSGQ	HQVAN	VDZXC	VBXEJ
"	14.	NZNRE	CYLQT	SAEPZ	TMTKC	HYFZV
"	11.	DWXAR	VIZEX	NNEJD	IPHFD	KPOQT
"	19.	INCQJ	OTBPX	BMMGP	VPZXW	LRFKG
"	20.	AVXJT	MZKDG	QNMGQ	VCVWO	UKNDZ
"	5.	RGPZM	QWWYB	VVZNK	U	

For the sake of clearness of exposition let us study the five adjacent columns, numbers 10 to 14, of this message, together with their accompanying plain text. They are as follows:

		Column—10 11 12 13 14
		ERETH
Generatrix—	7.	WYRZJ
		HAVEB
"	12.	INDDI
		MBARD
"	18.	FZDYX
		EPREL
"	6.	POWKE
		NTHEA
"	9.	AOGXT
		EDIED
"	8.	QHQVA
		EANDT
"	14.	TSAEP
		AVEBE
"	11.	XNNEJ
		RPOSE
"	19.	XBMMG
		ANDRA
"	20.	GQNMG
		HEENE
"	5.	BVVZN

If we desire to determine which particular alphabet of the twenty-five was used to encipher the first column of this series of five, we could do so by means of the synoptic tables. We wish to know, for example, what alphabet will produce for the plain-text letters, in this column at the generatrix indicated, the cipher letters which represent them. We refer to the synoptic table for E, which is the first letter in the column; looking on the 7th generatrix we search for the letter W, which represents this plain-text letter, and we find that this cipher letter will be produced by alphabets 16, 17, and 20. We then refer to the synoptic table for H, the second letter in this column, and find that the cipher letter I will be produced on the 12th generatrix by alphabets 6, 7, 8, 14, 15, 16, 17, and 18. A table such as the following results, when this is done for all the letters in this column:

TABLE 1

Column 10

Generatrix	Plain text	Cipher text	Alphabets indicated
7	E	W	16, 17, 20
12	H	I	6, 7, 8, 14, 15, 16, 17, 18
18	M	F	3, 4, 6, 7, 10, 16, 17, 20, 23, 24
6	E	P	16, 17, 18, 20
9	N	A	6, 7, 8, 9, 16, 17, 18, 19
8	E	Q	17, 18, 19
14	E	T	7, 8, 9, 11, 15, 17, 18, 19
11	A	X	16, 17, 18, 19, 20
19	R	X	15, 16, 17, 18
20	A	G	12, 13, 14, 15, 17, 18, 19, 20, 21
5	H	B	1, 2, 3, 4, 5, 16, 17, 18, 19, 20

Now let us make a frequency table of the alphabets which are indicated in order to find the one which is indicated the most frequently.

TABLE 2

Alphabet —	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Frequency—	|	|	||	||	|	|||	||||	|||	||	|	|	|	|	||	||||	𝍸 |||	𝍸 𝍸 |	𝍸 ||||	𝍸 |	𝍸 |	|		|	|	

The frequency table shows that alphabet 17 is indicated the most frequently. In fact it is indicated just as many times as there are letters in the column, viz., 11 times. By means of this method, then, we have determined which of the possible twenty-five alphabets will best meet the requirements of the given column of plain text, cipher text, and generatrix numbers. In other words, we have determined which alphabet was used to encipher this column, and the reason why this alphabet was indicated 11 times is clear.

Had we known only the equivalents of the letter E, and compiled our table upon them, it would have been as follows:

TABLE 3

Alphabet —	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Frequency—							|	|	|		|				|	||	||||	|||	||	||					

We still could pick out alphabet 17 as the probable one which was used.

Now if we had supposed that this column consisted exclusively of E's, the table would be as follows:

TABLE 4

Column 10

Generatrix	Plain text	Cipher text	Alphabets indicated
7	E	W	16, 17, 20
12	E	I	———
18	E	F	13, 14, 18, 19, 21, 22, 25
6	E	P	16, 17, 18, 20
9	E	A	———
8	E	Q	17, 18, 19
14	E	T	7, 8, 9, 11, 15, 17, 18, 19
11	E	X	———
19	E	X	———
20	E	G	———
5	E	B	———

TABLE 5

Alphabet —	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Frequency—							|	|	|		|		|	|	|	||	||||	||||	|||	||	|	|			|

Since on referring to the synoptic table for letter E, the 12th generatrix, cipher letter I does not appear, we indicate this in our table by a dash, meaning that there is no alphabet which will produce the cipher letter I for the plain-text letter E at the 12th generatrix. In reality it means that this letter represents a letter other than E. The same may be said with reference to the other dashes in this table.

Note now that alphabets 17 and 18 are the most frequent. Examination of these two alphabets will show that they resemble each other very closely, and one will do almost as well as the other in this case. Experiment would soon disclose that alphabet 17 is the correct one. The nature of such experiment will be given below.

It is seen therefore that by merely assuming the entire column to consist exclusively of E's, we could determine which alphabet was used to encipher this column. Now since the letter E composes approximately 14% of English text, we could assume this to be true in any message on this system for the sake of trying the preceding method of determining the alphabets applying to each column of the message. After the determination of each alphabet we can proceed to find out for each column the correct plain-text letters which correspond to the cipher letters, by merely counting back on each alphabet the indicated number of spaces from the cipher letters, which will thus give the plain-text letters concerned. For example, having determined that the correct alphabet applying to column 10 is number 17, we count back 7 letters from cipher letter W and find that the plain-text letter concerned is E; likewise we count back 12 letters from cipher letter I and find that the plain-text letter concerned is H, etc.

We do this for each letter and for each column and set the results together. Often it will be found that no alphabet is repeated sufficiently to justify its selection for experiment. It means, therefore, that in the column concerned there were no E's, or perhaps only one or two. The procedure very frequently results in the choosing of an alphabet which proves on trial to be incorrect. But the majority of the results will be correct and will produce skeleton words in which the errors resulting from a faulty choice of alphabets will be noted very easily, and the values which are wanting may be filled in from the context. The tables and data for the other four columns in our series of five adjacent ones in the example, are as follows:

TABLE 6

Column 11

Generatrix	Plain text assumed to be	Cipher text	Alphabets indicated
7	E	Y	———
12	E	N	———
18	E	Z	2, 3, 4
6	E	O	———
9	E	O	———
8	E	H	———
14	E	S	———
11	E	N	11, 12, 13, 14, 15
19	E	B	———
20	E	Q	5
5	E	V	10, 11, 12, 13, 14

Column 12

Generatrix	Plain text assumed to be	Cipher text	Alphabets indicated
7	E	R	14
12	E	D	6, 7, 8, 10, 24
18	E	D	———
6	E	W	———
9	E	G	7, 8, 9
8	E	Q	17, 18, 19
14	E	A	——
11	E	N	11, 12, 13, 14, 15
19	E	M	———
20	E	N	———
5	E	V	10, 11, 12, 13, 14

Column 13

Generatrix	Plain text assumed to be	Cipher text	Alphabets indicated
7	E	Z	10, 11, 12, 13
12	E	D	6, 7, 8, 10, $\underline{24}$
18	E	Y	1, 5
6	E	K	$\underline{24}$
9	E	X	21, 22, 23, $\underline{24}$
8	E	V	22, 23, $\underline{24}$
14	E	E	———
11	E	E	———
19	E	M	———
20	E	M	———
5	E	Z	———

Column 14

7	E	J	15
12	E	I	———
18	E	X	———
6	E	E	———
9	E	T	12, 13, 14
8	E	A	———
14	E	P	———
11	E	J	20, $\underline{21}$, 22, 23, 24
19	E	G	12, 13, 14, 17, 18, 19, $\underline{21}$, 25
20	E	G	———
5	E	N	1, 2, 3, 4, 5, $\underline{21}$, 22, 23, 24, 25

The alphabets which are indicated a sufficient number of times to justify experiment have been underlined in the tables, and those which may be tentatively assigned to the columns concerned on the basis of such selection, are as follows:

Column	—	10	11	12	13	14
Alphabet	—	17	—	14	24	21

It is seen that in the case of column 11 no alphabet can be selected as probable from frequency alone. Setting together the results of the other four columns, however, the requirements of the context soon determine what letters must be represented. From this the correct alphabet can be found by referring again to the synoptic tables.

Thus, the alphabets applying to columns 10, 12, 13, and 14 having been determined, we proceed to find the correct plain-text letters in each column. They are as follows:

	Column	10	11	12	13	14
Line No. 1,	Generatrix 7	W	Y	R	Z	J
		E	-	E	T	H
2,	" 12	I	N	D	D	I
		H	-	V	E	B
3,	" 18	F	Z	D	Y	X
		M	-	A	R	D
4,	" 6	P	O	W	K	E
		E	-	R	E	L
5,	" 9	A	O	G	X	T
		N	-	H	E	A
6,	" 8	Q	H	Q	V	A
		E	-	I	E	D
7,	" 14	T	S	A	E	P
		E	-	N	D	T
8,	" 11	X	N	N	E	J
		A	-	E	B	E
9,	" 19	X	B	M	M	G
		R	-	O	S	E
10.	" 20	G	Q	N	M	G
		A	-	D	R	A
11,	" 5	B	V	V	Z	N
		H	-	E	N	E

In the 5th line the polygraph AOGX is N-HE, which suggests that the words may be ON THE or IN THE. Likewise trigraphs SAE in the 7th line, and GQN in the 10th line suggest AND. The synoptic tables are consulted to find an alphabet which will produce the appropriate plain-text letters from the given cipher letters on the indicated generatrices, and it is found that alphabet 10 will not only produce the desired letters, but will give good combinations everywhere else in this same column. We have thus determined from context the correct alphabet applying to this column.

When four or five alphabets are in juxtaposition, reference is made to the cipher text on each line, and the generatrices for each line being given, parts of words to the right or left are completed, which in turn will add to the alphabets already determined. For example:

Take the five columns of cipher letters on either side of the columns already deciphered in the example above. They are as follows:

Column			5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Line 1,	Generatrix—	7	X	K	U	C	P	W	Y	R	Z	J	F	G	S	G	Q
								E	R	E	T	H					
2,	"	12	R	W	Q	F	K	I	N	D	D	I	Z	T	G	R	F
								H	A	V	E	B					
3,	"	18	G	K	V	I	L	F	Z	D	Y	X	F	S	Q	X	X
								M	B	A	R	D					
4,	"	6	C	E	V	N	W	P	O	W	K	E	H	S	P	Y	L
								E	P	R	E	L					
5,	"	9	S	A	C	P	C	A	O	G	X	T	O	J	X	K	X
								N	T	H	E	A					
6,	"	8	S	I	O	S	G	Q	H	Q	V	A	N	V	D	Z	X
								E	D	I	E	D					
7,	"	14	E	C	Y	L	Q	T	S	A	E	P	Z	T	M	T	K
								E	A	N	D	T					
8,	"	11	R	V	I	Z	E	X	N	N	E	J	D	I	P	H	F
								A	V	E	B	E					
9,	"	19	J	O	T	B	P	X	B	M	M	G	P	V	P	Z	X
								R	P	O	S	E					
10,	"	20	T	M	Z	K	D	G	Q	N	M	G	Q	V	C	V	W
								A	N	D	R	A					
11,	"	5	M	Q	W	W	Y	B	V	V	Z	N	K	U			
								H	E	E	N	E					

In the 3rd line the word BOMBARDMENT is suggested. If this word is correct then the digraph IL represents BO and the polygraph FSQX represents MENT. We search, therefore, by means of the synoptic tables for the alphabets which will produce these cipher letters for the assumed plain-text letters at the generatrix indicated, viz., 18. The alphabets which are indicated are as follows:

TABLE 7

Column	8	9	10	11	12	13	14	15	16	17	18
Plain text	B	O	M	B	A	R	D	M	E	N	T
Cipher	I	L	F	Z	D	Y	X	F	S	Q	X
Alphabets indicated on the 18th generatrix.	1	6	17	10	14	24	21	3	6	17	11
	2	7						4	7	18	
	3	13	These have already been determined and fixed for these positions.					6	10	19	
		14						7	16		
		15						10	17		
		21						16	20		
		22						17			
								20			
								23			
								24			

From among the possibilities for these letters we may eliminate at once those alphabets which have already been assigned to the deciphered columns 10, 11, 12, 13, 14. This will eliminate alphabets 14 and 21 from the possibilities of column 9, alphabets 10, 17, and 24 from the possibilities of column 15, etc.

We put together the combination of alphabets 1· 6· 17· 10· 14· 24· 21· 3· 7· 18· 11 for example, which will produce the word BOMBARDMENT on the third line, 18th generatrix, and set them to the corresponding section of cipher letters on the 1st line and look for the plain text on the 7th generatrix. If this combination results in the addition of good letters to the already deciphered text here, and also when it is applied to several other places within these same columns, we may assume that we have found the correct one. If it does not, we experiment further and try to eliminate such alphabets as do not add to the results until the correct alphabets are found. In this manner the entire message is finally solved.

This method of decipherment is only of theoretical or pedagogical importance[1] because it is dependent upon the knowledge of the generatrices used, a condition which would rarely, if ever, happen in actual practice. Hence a method is necessary for solving a message when the generatrices used are not known.

3. SOLUTION OF A MESSAGE WHEN ONE WORD CONTAINED IN THE DISPATCH IS KNOWN OR SUSPECTED BY THE DECIPHERER

MESSAGE

```
WDGQE EDZLV HUOJW MZIWV WGOXK
LETII CYUPX HSEXV DGAPR NEGND
MYHVQ JGQUD JBFGD WFKOC VLLGX
YQNAO MTACD ZVZOR QZIAF KGSUG
LMIMK GWQPP LOTQU QVTZU NWBZC
BMZDX MPEVY XLQVP BATYK FCTQK
EPFTW AVPQM KOKTK FLFKY UGLPK
RYKUW TKQYY DFNGW SLCTT WXMKJ
QBQJW KXVBN VZLRX QVLWO OSTPX
NZYZF KCRAT L
```

Suppose it is known that the message above contains the word AMERICAN. Now it is, of course, not known where this word occurs, nor on which one of the possible twenty-five generatrices it has been enciphered. These two things must be determined. We may begin by assuming that the word has been enciphered on the 10th generatrix. The reason one might profitably start the search with the 10th generatrix is that in practice it is better not to use the first three or four generatrices immediately above or below the line of plain-text; by beginning with the 10th, therefore, and working backward and forward one generatrix at a time, this kind of a systematic search is likely to lead to results more quickly than if

[1] It is true that we have been able occasionally to determine the generatrices which were used by fitting the frequency tables for the successive horizontal lines in a message to frequency tables based upon the cipher equivalents of ETOANIRSHD *for each generatrix*. That is, a series of 25 frequency tables, one for each generatrix, for the letters ETOANIRSHD was made. Then by attempting to fit the frequency table for a single horizontal line of a message to these tables, it was often possible to pick out the most probable generatrix which might apply to this particular line. This process when applied throughout the successive lines of a message would enable the decipherer to select the most probable generatrices for all the lines and from there on the process would be the same as described above.

random generatrices are tried. The first step is to make a table showing the possible equivalents for the letters of this assumed word if it has been enciphered on the 10th generatrix. This is done as follows:

Examine the A synoptic table, the 10th generatrix, and it will be found that the only letters which can represent A for all twenty-five alphabets are B, J, G, K, T, V, and X. Examine the M synoptic table, 10th generatrix, and it will be found that the only letters which can represent M for all twenty-five alphabets are A, K, Q, V, E, H, X, N.

This is done for the rest of the letters of the assumed word, and a table like the following results:

TABLE 8

Plain text	A	M	E	R	I	C	A	N
Possible cipher equivalents on the 10th generatrix.	B	A	C	P	D	K	B	M
	J	K	B	I	C	Q	J	E
	G	Q	Q	D	V	M	G	C
	K	V	H	C	N	V	K	B
	T	E	V	J	X	X	T	Z
	V	H	X		Z	E	V	
	X	X	Z		J		X	
		N	J		K			

Search is then made in the cipher text for a sequence of eight letters of which the first (which would represent A) will be any one of the series of possible equivalents given for A in Table 8; the second (which would represent M) will be any one of the series of possible equivalents given for M in Table 8, etc. In short, if a group of eight letters representing any of the multitude of possible combinations offered by Table 8 can be found, this group may be the word AMERICAN, enciphered on the 10th generatrix.

If no such group is found in the 10th generatrix, it becomes necessary to make a similar search on another generatrix, say the 9th, or the 11th, etc., until a possible place has been found. The possibilities of prolonged experimenting in this particular justify the assertion of De Viaris that in case of urgency twenty secretaries might be employed simultaneously, in order to reduce the tedium and burden of the search!

When a possible sequence has been located it becomes necessary for the decipherer to find the combination of alphabets which will apply to that particular portion of cipher text. The difficulties for the decipherer now actually begin in the case of the particular alphabets under discussion.

In this case, the group sought will be found in the 11th generatrix, the 4th line of the text, the group ZVZORQZI.

By consulting the synoptic tables we find that the alphabets, which will produce the combinations of cipher letters ZVZORQZI for the word AMERICAN on the 11th generatrix, are as follows:

TABLE 9

Plain text	A	M	E	R	I	C	A	N
Cipher text	Z	V	Z	O	R	Q	Z	I
Possible alphabets indicated on the 11th generatrix.	21	6	16	6	11	1	21	6
	22	7	17	7	12	2	22	7
	23	8	18	9	13	3	23	8
	24	9	19	10	14	4	24	10
	25			13	15		25	14
				16				16
				17				17
				19				18
				20				20

Now the total number of combinations which is possible, given the indicated assortment of alphabets, is represented by the product of 5×4×4×9×5×4×5×9=648,000.

Any one of these combinations will produce for the word AMERICAN, on the 11th generatrix, the cipher group ZVZORQZI; *but there is only one combination which will decipher the entire corresponding section above and below this portion of the cipher text,* and this combination must be found. It is clear that we could try out one after the other the combinations offered, setting the alphabets together and applying them to corresponding portions of the cipher text above and below the place where AMERICAN has been found, rejecting such as do not give us any possible reading on any generatrix; but it would take many hours of tedious trials to find the correct combination by such experiment, inasmuch as the number of combinations possible from the many alphabets indicated is almost unlimited. We will therefore have recourse to some further step to simplify the procedure. This represents our first addition to the methods of De Viaris.

On the same theory, as stated on page 43, that a line of English text will consist of approximately 14% of E's, it is likewise true that, to a greater degree, the same line will contain the letters ETOANIRSHDLC because these compose approximately 85% of English text. Having ascertained that the word AMERICAN was probably enciphered on the 11th generatrix, reference is next made to the synoptic tables for the letters ETOANIRSHDLC for this generatrix and a table is the result, as follows:

TABLE 10

Plain text	E	T	O	A	N	I	R	S	H	D	L	C
Possible cipher equivalents on the 11th generatrix.	D	J	G	C	P	F	W	Y	M	V	A	Q
	P	L	Y	M	V	W	X	Z	Q	X	Q	V
	C	K	F	B	I	D	O	U	E	W	E	P
	N	A	S	X	X	R	Z	J	V	O	X	I
	Z	B	K	H	D	J	F	G	C	Z	H	X
	J	G	Q	Z	C	K	D	F	B	J	N	Z
	K		V			Q				K	J	J
										S		R

The decipherer then turns to the line in which his tentatively deciphered word appears and writes beneath each undeciphered letter the possible plain-text letters which it might represent, as shown by Table 11.

The result in this case is as follows:

TABLE 11

Generatrix—11.	Y	Q	N	A	O	M	T	A	C	D	Z	V	Z	O	R	Q	Z	I	A	F	K	G	S	U	G
	O	O	E	T	R	A		T	E	E	A	M	E	R	I	C	A	N	T	O	O	T	O	S	T
	S	I	M	L	D	H		L	N	I									L	I	D	O	D		O
		H	L						H	R										R	E	S			S
		L							A	N										S	T				
		C																			I				

The alert decipherer will detect with little effort the words THE AMERICAN TROO(P) S, and at the left HELD. This leaves a two-letter word between HELD and THE, and the one that is most probable is BY. If so the line would read as follows:

—HELD (BY) THE AMERICAN TROO(P)S—

In this procedure, it will of course often happen that a correct letter is not indicated as in the case of the letters P, B, and Y, since our table 10 considers only the high-frequency letters; but in the majority of cases skeletons of words will result, which can be built up by the suggestions offered.

A table is then constructed showing the alphabets which are indicated for each letter of the deciphered line. It is as follows:

TABLE 12

Position—	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Possible alphabets indicated for each position on the basis of the single line of decipherment.	—	5	11	1	8	6	16	7	11	1	21	6	16	6	11	1	21	6	7	11	16	1	21	6	—
			12	2	21	7	17	8	12	2	22	7	17	7	12	2	22	7	8	12	17	3	22	8	
			13	3	22	8	18	9	13	3	23	8	18	9	13	3	23	8	9	14		4	24	9	
			14	4	24	9	19	10	14	5	24	9	19	10	14	4	24	10	10	15		5	25	10	
			15	5	25	16	20	11			25			13	15		25	14	11					12	
						17		17						16				16	17					16	
						18		18						17				17	18					18	
						19		19						19				18	19					19	
								20						20				20	20					20	

Now any combination of the alphabets given in this table will produce this line of deciphered text on the 11th generatrix, but it is necessary to find *one* combination, from among the vast number of possible combinations, which will decipher *all* the lines of cipher text. Obviously it would require much time if the mere process of experiment and elimination is applied. It is possible, however, to find the correct sequence for small sections, where only two or three possibilities are offered at most, as in the sections covering positions 2, 3, 4, and 5, or 20, 21, 22, and 23. The decipherer should therefore attempt to do so, and in some cases, much progress can be made; but since in no case is the generatrix number indicated, such work is largely one requiring a great amount of time and labor. Accordingly, some principles must be found for simplifying the subsequent decipherment. These principles, which represent our second contribution to the method of De Viaris, are the result of certain definite relations which result from the use of a key word to determine the sequence of alphabets, or in other words, from the use of a numerical key derived from a key word.

4. METHOD FOR THE RECONSTRUCTION OF A NUMERICAL KEY DERIVED FROM A KEY WORD

The following short cut was found to simplify the work enormously and to eliminate considerable experimentation. It is based, as stated above, upon the numerical relations which obtain among the series of alphabets when a key word has been used as the basis for the sequence of the alphabets. Let us consider the following example of a numerical key derived from a key word, carefully noting the numerical relations:

```
 1  2  3  4  5  6  7  8  9    10 11 12 13 14 15 16 17 18    19 20 21 22 23 24 25
 R  I  V  E  R  B  A  N  K     R  I  V  E  R  B  A  N  K     R  I  V  E  R  B  A
17 10 23  7 18  4  1 15 13    19 11 24  8 20  5  2 16 14    21 12 25  9 22  6  3
```

This key sequence consists of two complete periods and one incomplete, which for convenience will be denoted as *key word lengths*.

Consider the letter A. It is found three times in this case, occupying positions 7, 16, and 25, indicated by 1, 2, and 3 respectively. Now as regards the relative positions occupied by A in each length of key, all three of them occupy similar positions which may be termed homologous. That is, in this example, position 7 is homologous with position 16, and with position 25, and we may say that the *homolog* of A in the 7th position is A in the 16th or 25th positions. Now if the position numbers of any two homologs be considered, it will be found that their difference is equal to the number of letters in the key word. For example, in the case of the letter A, the difference between 7, the position number of the first A, and 16, the position number of its homolog, the second A, is 9. The number of letters in the key word is 9. Likewise, the difference between the position number of the second A, 16, and its homolog, the third A, 25, is 9.

Now the fact that in the numerical key homologs receive numbers in sequence, affords an external indication of the presence of homologs, which enables us to locate them, and thus to determine the number of letters in the key word. For example, given the alphabet numbers 15 and 16, occupying positions 8 and 17 respectively in the illustration above, we simply find the difference between 17 and 8, and this gives us 9 as the number of letters in the key word.

The exception to the rule, viz., that the difference in position numbers of two alphabet numbers in sequence is equal to the number of letters in the key word, is found in the case of a repeated letter within one length of key word. Since two repeated letters within one length of key word receive numbers in sequence, then although the numerical relation of homologs pointed out above still holds true, yet the rule with respect to the two alphabet numbers in sequence does not hold strictly true.

Note, for example the letter R in the illustration. The positions occupied by the successive R's are as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
R				R					R				R					R				R		
17				18					19				20					21				22		
I*a*				II*a*					I*b*				II*b*					I*c*				II*c*		

Here the successive R's have been indicated by the roman numerals. Now I*a*, I*b*, and I*c* are homologs, as likewise are II*a*, II*b*, and II*c*.

I*a* receives the number	17	II*a* receives the number	18
I*b* " " "	19	II*b* " " "	20
I*c* " " "	21	II*c* " " "	22

Here, then, homologs receive such numbers as are within 1 of being sequent. If this letter occurred three times within one length of key word, the homologs would receive numbers such as would be within 2 of being sequent. With the mental reservation then that repeated letters, which may be designated for convenience as *analogs*, occasion this exception to the general rule, the decipherer may proceed on the assumption that two numbers in sequence, when not too close to each other, in most cases represent homologs. If the length of the key word can be determined from unrepeated letters, the presence of repeated letters constitutes an aid to decipherment. A repeated letter in the key word may offer obstacles at first, but once located, assists rather than hinders the solution.

Once the length of the key word is found, divide the series of numbers into lengths corresponding to the length of the key. Note above that at intervals of nine spaces, the numbers of the alphabets follow in numerical sequence as a result of this numerical relation of homologs. For example:

Intervals:	1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9
Alphabets:	7 – – – – – – – – – 8	4 – – – – – – – – – 5	10 – – – – – – – – – 11
"	8 – – – – – – – – – 9	5 – – – – – – – – – 6	11 – – – – – – – – – 12

Note further that the numerical relation between any two alphabet numbers which apply to (1) two unrepeated letters in one key word length is exactly the same as that between their homologs in another key word length; (2) two repeated letters in one key word length is also exactly the same as that between their homologs in another key word length; (3) one repeated and one unrepeated letter in one key word length is not the same as that between their homologs in another key word length, but decreases regularly by arithmetical progression. Examples of these three cases as exhibited in the illustration above are as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
17		23		18		1		13	19		24		20		2		14	21		25		22		3

Case (1) Letter V	Case (2) Letter R	Case (3) Letters R and V
1st length; 23 – 1 = 22	1st length; 17 + 1 = 18	1st length; 17 + 6 = 23
2nd " ; 24 – 2 = 22	2nd " ; 19 + 1 = 20	2nd " ; 19 + 5 = 24
3rd " ; 25 – 3 = 22	3rd " ; 21 + 1 = 22	3rd " ; 21 + 4 = 25

Another important principle which follows from these mathematical relations is that in most cases, sequences such as 5·4, or 9·8, or in other words, cases where two numbers are in reversed normal sequence, are impossible. This follows because the letters in the key word are numbered in sequence in accordance with their positions in the normal alphabet and except in the case of a very long key word, the homolog of the letter which takes the number 4, for example, would be 5, so that number 5 could not possibly appear immediately before 4, but must appear in the second length of key. Sequences like 5· 17· 4, or 12· 10, however, are not only possible but frequent. Note the sequences 15· 13 and 16· 14 in the illustration above.

From the principles given above, it is possible to reconstruct completely the whole sequence of a numerical key, given only a few of the alphabets and their positions. Take the following example:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:			11	1	12	5	8	19																	

Here only six adjacent alphabet numbers and their positions are given, yet it is possible to find the entire sequence from these alone. Let us first find the length of the key word. From the position of alphabet 1, it is seen immediately that the key word cannot be shorter than four letters, for alphabet 1 must be found in the first length or period of the key sequence. Now the key word cannot be four letters in length because if it were then alphabet 2 would have to fall in position 8, which is already assigned to alphabet 19. We shall make a trial therefore on the basis of a five-letter key word.

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	4	7	11	1	12	5	8	19																	

Now the homolog of position 7 on the basis of a five-letter key word is the position 2, hence alphabet 7 is tentatively assigned to position 2; by the same reasoning, alphabet 5 is assigned to position 1. Note now that the two homologous positions 3 and 8 are assigned to 11 and 19 respectively, which is impossible, since homologous positions must bear numbers in sequence or in the case of repeated letters, one or two numbers removed from each other.

Hence, a five-letter key word is not correct, and we begin again on the basis of a six-letter key word.

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	7	18	11	1	12	5	8	19	13	2	14	6	9	20	15	3	16	7	10	21	17	4	18	8	11

Note the conflicts in the sequence as determined on the basis of a six-letter word: Alphabets 7, 8, and 11 appear twice, alphabets 22 to 25 are missing. Evidently a six-letter key word is incorrect.

On the basis of a seven-letter key word a complete sequence may be attained in which no inconsistencies appear, in which all the mathematical conditions are fully complied with, and which may therefore]be taken to be correct. It is as follows:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	18	22	11	1	12	5	8	19	23	13	2	14	6	9	20	24	15	3	16	7	10	21	25	17	4

Let us now apply these principles to the solution of the case under discussion. The sequence given on page 51 is repeated below:

TABLE 12

Position—	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Possible alphabets indicated for each position on the basis of the single line of decipherment.	–	5	11	1	8	6	16	7	11	1	21	6	16	6	11	1	21	6	7	11	16	1	21	6	—
			12	2	21	7	17	8	12	2	22	7	17	7	12	2	22	7	8	12	17	3	22	8	
			13	3	22	8	18	9	13	3	23	8	18	9	13	3	23	8	9	14		4	24	9	
			14	4	24	9	19	10	14	5	24	9	19	10	14	4	24	10	10	15		5	25	10	
			15	5	25	16	20	11			25			13	15		25	14	11					12	
						17		17						16				16	17					16	
						18		18						17				17	18					18	
						19		19						19				18	19					19	
								20						20				20	20					20	

The only alphabet which is fixed is alphabet 5, for position 2. We may eliminate 5 from all other positions immediately. In doing so we notice that under position 22 the possibilities left are alphabets 1, 3, and 4. Now alphabet 1 is hardly possible for this position, so that we may eliminate it immediately, also, leaving alphabets 3 and 4 as the only possibilities. Looking through the various columns to find the possible positions for the homologs of 3 or 4, viz.: 1 and 2, we find that only under positions 4, 10, and 16 are there any possibilities. The difference between these numbers, 4, 10, and 16 is 6, and it points, therefore, to a six-letter key word. We divide up the series into six-letter lengths, therefore, and assign alphabets 1, 2, 3, and 4 to positions 4, 10, 16, and 22 respectively, as meeting the requirements. Now alphabet 5 is fixed for position 2, and on looking for columns containing possible homologs of this alphabet, we note that position 6 may contain an analog of alphabet 5; that positions 8 and 12 may contain another set of analogs, which would be homologous with the first set; that positions 14 and 18, 20 and 24, form two more sets of analogs. The positions may be those of repeated letters, therefore, and would be as follows:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:		5				6		7				8		9				10		11				12	

By experiment it will be found that this is, in fact, the only arrangement which fulfills the mathematical requirements of the sequence and will conform to the possibilities indicated in the given series.

We may, therefore, consider these alphabets as fixed for the positions indicated and proceed to eliminate them as possibilities from all other positions. This leaves alphabets 13 or 14 for position 3, and since 15 is not given as a possibility for the first homolog of position 3, namely 9, alphabet 13 is fixed for position 3, alphabets 14, 15, and 16 are fixed for the homologous positions 9, 15, and 21 respectively.

The alphabets which still remain unassigned are 17 to 25; the positions which as yet are undetermined are 1, 5, 7, 11, 13, 17, 19, 23, and 25; and the partially reconstructed sequence is now as follows:

TABLE 13

Position —	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabets indicated.	–	5	13	1	21	6	17	7	14	2	21	8	17	9	15	3	21	10	17	11	16	4	21	12	—
					22		18				22		18				22		18				22		
					24		19				23		19				23		19				24		
					25		20				24						24		20				25		
											25						25								

Now alphabet 17 will have to be found within the first six positions, since alphabet 16 is placed in the final length of key word. Alphabet 17 is found as a possibility in position 6 only, which has already been assigned to alphabet 6. Hence, the only remaining possibility for alphabet 17 is position 1, which so far has remained blank. If this position is correct, alphabet 18 should be found in position 7, and alphabets 19 and 20 in positions 13 and 19, respectively. Upon inspection all conditions meet the requirements, and in addition fix position 25 for alphabet 21. The sequence now stands thus:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	17	5	13	1		6	18	7	14	2		8	19	9	15	3		10	20	11	16	4		12	21

Enough of the procedure has been shown to demonstrate the method. The sequence can now be completed very rapidly. The final sequence is found to be as follows:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	17	5	13	1	22	6	18	7	14	2	23	8	19	9	15	3	24	10	20	11	16	4	25	12	21

The solution of the message may now be completed as easily by the decipherer as by the intended recipient. It is as follows:

```
WDGQE  EDZLV  HUOJW  MZIWV  WGOXK
EARLY  THISM  ORNIN  GTHEG  ERMAN

LETII  CYUPX  HSEXV  DGAPR  NEGND
SBOMB  ARDED  WITHG  ASSHE  LLSAN

MYHVQ  JGQUD  JBFGD  WFKOC  VLLGX
DHIGH  EXPLO  SIVES  THETR  ENCHE

YQNAO  MTACD  ZVZOR  QZIAF  KGSUG
SHELD  BYTHE  AMERI  CANTR  OOPST

LMIMK  GWQPP  LOTQU  QVTZU  NWBZC
HEREW  ASNOI  NFANT  RYACT  IONWI

BMZDX  MPEVY  XLQVP  BATYK  FCTQK
THINT  HELAS  TTWEN  TYFOU  RHOUR

EPFTW  AVPQM  KOKTK  FLFKY  UGLPK
STHEB  RITIS  HHAVE  ADVAN  CEDTH

RYKUW  TKQYY  DFNGW  SLCTT  WXMKJ
EIRFR  ONTOV  ERAWI  DTHOF  NEARL

QBQJW  KXVBN  VZLRX  QVLWO  OSTPX
YHALF  AMILE  TOADE  PTHOF  FOURH

NZYZF  KCRAT  L
UNDRE  DYARD  S
```

5. SOLUTION OF A MESSAGE WHEN THE DECIPHERER HAS NO KNOWLEDGE OF ANY WORD IN THE MESSAGE

The length of the message will suggest to the decipherer the wisdom or otherwise of searching for the terminations ordinarily found in plain text, whether it be English, Spanish, French, or German; or of short and very common words such as OF THE, AND THE, TO THE, BY THE, etc., in English; in Spanish, PARA QUE, DE QUE, AMENTE, MIENDO, etc. A very important feature of this sort of guesswork is the knowledge of the source of the message to be deciphered, or the parties between whom the message passed. If a word of six or seven letters, or more, be guessed correctly, the solution of the problem is at hand.

6. RECOVERY OF A KEY WORD GIVEN THE NUMERICAL KEY DERIVED FROM IT

It is often desirable to determine from the sequence of numerical equivalents the key word which was used to generate the numerical key, in order that clues as to future key words may be had.

By the exercise of some ingenuity, this can be done by the method given by De Viaris.

Given the following sequence, let us try to recover the key word:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	4	7	16	1	19	22	12	8	14	23	5	9	17	2	20	24	13	10	15	25	6	11	18	3	21

The first thing to do is to find the length of key word, by means of the principles given on pages 52-54. In this case, it will be found to be 10 and we will therefore divide the sequence into 10 letter lengths.

Under each number place a series of three or four letters such as are probable from the indications given by that number, with respect to the normal alphabet sequence. It is not necessary to consider more than one length of key word. Thus:

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alphabet Indicated:	4	7	16	1	19	22	12	8	14	23															
Possible Letter Equivalents.	B	C	M	$\underline{A}$	Q	Q	I	C	M	Q															
	C	D	N	B	$\underline{R}$	R	L	D	$\underline{N}$	R															
	$\underline{D}$	$\underline{E}$	O	C	S	S	$\underline{M}$	$\underline{E}$	O	S															
			$\underline{P}$		T	$\underline{T}$	N		P	$\underline{T}$															

Alphabets number 7 and 8 and 22 and 23 occupying homologous positions 2 and 8 and 6 and 10, respectively, represent repeated letters and must be either vowels or high consonants, if the word is a common English word. A trial of various possibilities, soon discloses the word DEPARTMENT.

By the exercise of ingenuity and patience the key word may be recovered in almost every case. Sometimes a basic word varied by the date is used, and when once discovered is of course a great aid in the decipherment of subsequent messages in the same cipher. Key phrases may be recovered by the same method, though the process is long and difficult.

In the case of the two messages given in sections 1 and 2, the key words were BELGIUM and SENATE, respectively.

It may be of interest to add, paradoxical as it may seem, that, as regards the nature of the alphabets used in such a system, the more dissimilar the individual alphabets are, that is, *the more mixed they are*, the easier it is to solve a message, when once a single word has been located. The alphabets used in this exposition bear certain relations to each other which enable the person using the system to reproduce them from memory. Note the repetition of sequences such as AEIOU, BCDF, NHRST, etc. The result is that even when a possible word has been located the number of alphabets which will produce the word is very great, so that considerable experiment must be resorted to in order that the correct combination may be found. This is because on many alphabets the sequences are so nearly alike that, given a letter E, for example, there may be ten different alphabets which will produce the same cipher letter on the same generatrix of E. The same is true as regards all the other letters of the alphabet. In a system similar to this one, however, where all the alphabets are so mixed that any two sequences rarely bear even a remote resemblance, when once a word has been located, the alphabets which apply are very limited in number, and the correct combination may be found with comparative ease. The combinations are tried out on the corresponding portions of cipher text above and below the deciphered word and their correctness thus tested. It is true, however, that in the former case the number of possible places where an assumed word may be found is smaller than in the latter case.

The weakness of such a system is that of using a key word to determine the sequence of the alphabets, a sequence which may be worked out mathematically, when a single word has been placed in the message. On the other hand, when such a system is used in connection with a purely random choice of alphabets (or its equivalent), the great number of alphabets resulting from the placing of a word, necessitates long and tedious experiment, in such a case, before the correct combination is found.

In conclusion, it may be said that this system, although superficially it appears to combine the most desirable elements of a cipher as regards secrecy and practicability, yet it will not withstand assault by the modern methods. Modifications of the original method of enciphering, however, have been proposed, which may have the result of materially increasing the safety and desirability of the system.

Synoptic Tables for the Star Cipher

SYNOPTIC TABLE OF THE LETTER A

	ALPHABET																								
GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
1	E	E	E	E	N	E	E	E	E	V	E	E	E	E	X	E	E	E	E	M	E	E	E	E	N
2	I	I	I	R	R	I	I	I	X	X	I	I	I	Z	Z	I	I	I	P	P	I	I	I	R	R
3	O	O	S	S	S	O	O	Z	Z	Z	O	O	J	J	J	O	O	W	W	W	O	O	S	S	S
4	U	T	T	T	T	U	J	J	J	J	U	K	K	K	K	U	Y	Y	Y	Y	U	T	T	T	T
5	H	H	H	H	H	K	K	K	K	K	Q	Q	Q	Q	Q	L	L	L	L	L	H	H	H	H	H
6	N	N	N	N	C	Q	Q	Q	Q	Q	V	V	V	V	V	M	M	M	M	Z	N	N	N	N	J
7	R	R	R	D	D	V	V	V	V	C	X	X	X	X	N	P	P	P	J	J	R	R	R	K	K
8	S	S	F	F	F	X	X	X	D	D	Z	Z	Z	R	R	W	W	K	K	K	S	S	Q	Q	Q
9	T	G	G	G	G	Z	Z	F	F	F	J	J	S	S	S	Y	Q	Q	Q	Q	T	V	V	V	V
10	B	B	B	B	B	J	G	G	G	G	K	T	T	T	T	V	V	V	V	V	X	X	X	X	X
11	C	C	C	C	M	B	B	B	B	B	H	H	H	H	H	X	X	X	X	X	Z	Z	Z	Z	Z
12	D	D	D	P	P	C	C	C	C	N	N	N	N	N	M	Z	Z	Z	Z	N	J	J	J	J	C
13	F	F	W	W	W	D	D	D	R	R	R	R	R	P	P	J	J	J	R	R	K	K	K	D	D
14	G	Y	Y	Y	Y	F	F	S	S	S	S	S	W	W	W	K	K	S	S	S	Q	Q	F	F	F
15	L	L	L	L	L	G	T	T	T	T	T	Y	Y	Y	Y	Q	T	T	T	T	V	G	G	G	G
16	M	M	M	M	Q	H	H	H	H	H	L	L	L	L	L	H	H	H	H	H	B	B	B	B	B
17	P	P	P	V	V	N	N	N	N	M	M	M	M	M	C	N	N	N	N	C	C	C	C	C	M
18	W	W	X	X	X	R	R	R	P	P	P	P	P	D	D	R	R	R	D	D	D	D	D	P	P
19	Y	Z	Z	Z	Z	S	S	W	W	W	W	W	F	F	F	S	S	F	F	F	F	F	W	W	W
20	J	J	J	J	J	T	Y	Y	Y	Y	Y	G	G	G	G	T	G	G	G	G	G	Y	Y	Y	Y
21	K	K	K	K	K	L	L	L	L	L	B	B	B	B	B	B	B	B	B	B	L	L	L	L	L
22	Q	Q	Q	Q	E	M	M	M	M	E	C	C	C	C	E	C	C	C	C	E	M	M	M	M	E
23	V	V	V	I	I	P	P	P	I	I	D	D	D	I	I	D	D	D	I	I	P	P	P	I	I
24	X	X	O	O	O	W	W	O	O	O	F	F	O	O	O	F	F	O	O	O	W	W	O	O	O
25	Z	U	U	U	U	Y	U	U	U	U	G	U	U	U	U	G	U	U	U	U	Y	U	U	U	U

SYNOPTIC TABLE OF THE LETTER
B

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	0
1	C	C	C	C	M	C	C	C	C	N	C	C	C	C	E	C	C	C	C	E	C	C	C	C	M	1
2	D	D	D	P	P	D	D	D	R	R	D	D	D	I	I	D	D	D	I	I	D	D	D	P	P	2
3	F	F	W	W	W	F	F	S	S	S	F	F	O	O	O	F	F	O	O	O	F	F	W	W	W	3
4	G	Y	Y	Y	Y	G	T	T	T	T	G	U	U	U	U	G	U	U	U	U	G	Y	Y	Y	Y	4
5	L	L	L	L	L	H	H	H	H	H	A	A	A	A	A	A	A	A	A	A	L	L	L	L	L	5
6	M	M	M	M	Q	N	N	N	N	M	E	E	E	E	X	E	E	E	E	M	M	M	M	M	E	6
7	P	P	P	V	V	R	R	R	P	P	I	I	I	Z	Z	I	I	I	P	P	P	P	P	I	I	7
8	W	W	X	X	X	S	S	W	W	W	O	O	J	J	J	O	O	W	W	W	W	W	O	O	O	8
9	Y	Z	Z	Z	Z	T	Y	Y	Y	Y	U	K	K	K	K	U	Y	Y	Y	Y	Y	U	U	U	U	9
10	J	J	J	J	J	L	L	L	L	L	Q	Q	Q	Q	Q	L	L	L	L	L	A	A	A	A	A	10
11	K	K	K	K	K	M	M	M	M	E	V	V	V	V	V	M	M	M	M	Z	E	E	E	E	N	11
12	Q	Q	Q	Q	E	P	P	P	I	I	X	X	X	X	N	P	P	P	J	J	I	I	I	R	R	12
13	V	V	V	I	I	W	W	O	O	O	Z	Z	Z	R	R	W	W	K	K	K	O	O	S	S	S	13
14	X	X	O	O	O	Y	U	U	U	U	J	J	S	S	S	Y	Q	Q	Q	Q	U	T	T	T	T	14
15	Z	U	U	U	U	A	A	A	A	A	K	T	T	T	T	V	V	V	V	V	H	H	H	H	H	15
16	A	A	A	A	A	E	E	E	E	V	H	H	H	H	H	X	X	X	X	X	N	N	N	N	J	16
17	E	E	E	E	N	I	I	I	X	X	N	N	N	N	M	Z	Z	Z	Z	N	R	R	R	K	K	17
18	I	I	I	R	R	O	O	Z	Z	Z	R	R	R	P	P	J	J	J	R	R	S	S	Q	Q	Q	18
19	O	O	S	S	S	U	J	J	J	J	S	S	W	W	W	K	K	S	S	S	T	V	V	V	V	19
20	U	T	T	T	T	K	K	K	K	K	T	Y	Y	Y	Y	Q	T	T	T	T	X	X	X	X	X	20
21	H	H	H	H	H	Q	Q	Q	Q	Q	L	L	L	L	L	H	H	H	H	H	Z	Z	Z	Z	Z	21
22	N	N	N	N	C	V	V	V	V	C	M	M	M	M	C	N	N	N	N	C	J	J	J	J	C	22
23	R	R	R	D	D	X	X	X	D	D	P	P	P	D	D	R	R	R	D	D	K	K	K	D	D	23
24	S	S	F	F	F	Z	Z	F	F	F	W	W	F	F	F	S	S	F	F	F	Q	Q	F	F	F	24
25	T	G	G	G	G	J	G	G	G	G	Y	G	G	G	G	T	G	G	G	G	V	G	G	G	G	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

SYNOPTIC TABLE OF THE LETTER

C

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	0
1	D	D	D	P	D	D	D	D	R	D	D	D	D	I	D	D	D	D	I	D	D	D	D	P	D	1
2	F	F	W	W	F	F	F	S	S	F	F	F	O	O	F	F	F	O	O	F	F	F	W	W	F	2
3	G	Y	Y	Y	G	G	T	T	T	G	G	U	U	U	G	G	U	U	U	G	G	Y	Y	Y	G	3
4	L	L	L	L	B	H	H	H	H	B	A	A	A	A	B	A	A	A	A	B	L	L	L	L	B	4
5	M	M	M	M	M	N	N	N	N	N	E	E	E	E	E	E	E	E	E	E	M	M	M	M	M	5
6	P	P	P	V	P	R	R	R	P	R	I	I	I	Z	I	I	I	I	P	I	P	P	P	I	P	6
7	W	W	X	X	W	S	S	W	W	S	O	O	J	J	O	O	O	W	W	O	W	W	O	O	W	7
8	Y	Z	Z	Z	Y	T	Y	Y	Y	T	U	K	K	K	U	U	Y	Y	Y	U	Y	U	U	U	Y	8
9	J	J	J	J	L	L	L	L	L	H	Q	Q	Q	Q	A	L	L	L	L	A	A	A	A	A	L	9
10	K	K	K	K	Q	M	M	M	M	M	V	V	V	V	X	M	M	M	M	M	E	E	E	E	E	10
11	Q	Q	Q	Q	V	P	P	P	I	P	X	X	X	X	Z	P	P	P	J	P	I	I	I	R	I	11
12	V	V	V	I	X	W	W	O	O	W	Z	Z	Z	R	J	W	W	K	K	W	O	O	S	S	O	12
13	X	X	O	O	Z	Y	U	U	U	Y	J	J	S	S	K	Y	Q	Q	Q	Y	U	T	T	T	U	13
14	Z	U	U	U	J	A	A	A	A	L	K	T	T	T	Q	V	V	V	V	L	H	H	H	H	A	14
15	A	A	A	A	K	E	E	E	E	E	H	H	H	H	V	X	X	X	X	Z	N	N	N	N	N	15
16	E	E	E	E	E	I	I	I	X	I	N	N	N	N	N	Z	Z	Z	Z	J	R	R	R	K	R	16
17	I	I	I	R	I	O	O	Z	Z	O	R	R	R	P	R	J	J	J	R	K	S	S	Q	Q	S	17
18	O	O	S	S	O	U	J	J	J	U	S	S	W	W	S	K	K	S	S	Q	T	V	V	V	T	18
19	U	T	T	T	U	K	K	K	K	A	T	Y	Y	Y	T	Q	T	T	T	V	X	X	X	X	H	19
20	H	H	H	H	A	Q	Q	Q	Q	V	L	L	L	L	H	H	H	H	H	X	Z	Z	Z	Z	J	20
21	N	N	N	N	N	V	V	V	V	X	M	M	M	M	M	N	N	N	N	N	J	J	J	J	K	21
22	R	R	R	D	R	X	X	X	D	Z	P	P	P	D	P	R	R	R	D	R	K	K	K	D	Q	22
23	S	S	F	F	S	Z	Z	F	F	J	W	W	F	F	W	S	S	F	F	S	Q	Q	F	F	V	23
24	T	G	G	G	T	J	G	G	G	K	Y	G	G	G	Y	T	G	G	G	T	V	G	G	G	X	24
25	B	B	B	B	H	B	B	B	B	Q	B	B	B	B	L	B	B	B	B	H	B	B	B	B	Z	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER
D

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	0
1	F	F	W	F	F	F	F	S	F	F	F	F	O	F	F	F	F	O	F	F	F	F	W	F	F	1
2	G	Y	Y	G	G	G	T	T	G	G	G	U	U	G	G	G	U	U	G	G	G	Y	Y	G	G	2
3	L	L	L	B	B	H	H	H	B	B	A	A	A	B	B	A	A	A	B	B	L	L	L	B	B	3
4	M	M	M	C	M	N	N	N	C	N	E	E	E	C	E	E	E	E	C	E	M	M	M	C	M	4
5	P	P	P	P	P	R	R	R	R	R	I	I	I	I	I	I	I	I	I	I	P	P	P	P	P	5
6	W	W	X	W	W	S	S	W	S	S	O	O	J	O	O	O	O	W	O	O	W	W	O	W	W	6
7	Y	Z	Z	Y	Y	T	Y	Y	T	T	U	K	K	U	U	U	Y	Y	U	U	Y	U	U	Y	Y	7
8	J	J	J	L	L	L	L	L	H	H	Q	Q	Q	A	A	L	L	L	A	A	A	A	A	L	L	8
9	K	K	K	M	Q	M	M	M	N	M	V	V	V	E	X	M	M	M	E	M	E	E	E	M	E	9
10	Q	Q	Q	V	V	P	P	P	P	P	X	X	X	Z	Z	P	P	P	P	P	I	I	I	I	I	10
11	V	V	V	X	X	W	W	O	W	W	Z	Z	Z	J	J	W	W	K	W	W	O	O	S	O	O	11
12	X	X	O	Z	Z	Y	U	U	Y	Y	J	J	S	K	K	Y	Q	Q	Y	Y	U	T	T	U	U	12
13	Z	U	U	J	J	A	A	A	L	L	K	T	T	Q	Q	V	V	V	L	L	H	H	H	A	A	13
14	A	A	A	K	K	E	E	E	M	E	H	H	H	V	V	X	X	X	M	Z	N	N	N	E	N	14
15	E	E	E	Q	E	I	I	I	I	I	N	N	N	X	N	Z	Z	Z	J	J	R	R	R	R	R	15
16	I	I	I	I	I	O	O	Z	O	O	R	R	R	R	R	J	J	J	K	K	S	S	Q	S	S	16
17	O	O	S	O	O	U	J	J	U	U	S	S	W	S	S	K	K	S	Q	Q	T	V	V	T	T	17
18	U	T	T	U	U	K	K	K	A	A	T	Y	Y	T	T	Q	T	T	V	V	X	X	X	H	H	18
19	H	H	H	A	A	Q	Q	Q	E	V	L	L	L	H	H	H	H	H	X	X	Z	Z	Z	N	J	19
20	N	N	N	E	N	V	V	V	X	X	M	M	M	N	M	N	N	N	Z	N	J	J	J	K	K	20
21	R	R	R	R	R	X	X	X	Z	Z	P	P	P	P	P	R	R	R	R	R	K	K	K	Q	Q	21
22	S	S	F	S	S	Z	Z	F	J	J	W	W	F	W	W	S	S	F	S	S	Q	Q	F	V	V	22
23	T	G	G	T	T	J	G	G	K	K	Y	G	G	Y	Y	T	G	G	T	T	V	G	G	X	X	23
24	B	B	B	H	H	B	B	B	Q	Q	B	B	B	L	L	B	B	B	H	H	B	B	B	Z	Z	24
25	C	C	C	N	C	C	C	C	V	C	C	C	C	M	C	C	C	C	N	C	C	C	C	J	C	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

SYNOPTIC TABLE OF THE LETTER E

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	0
1	I	I	I	R	I	I	I	I	X	I	I	I	I	Z	I	I	I	I	P	I	I	I	I	R	I	1
2	O	O	S	S	O	O	O	Z	Z	O	O	O	J	J	O	O	O	W	W	O	O	O	S	S	O	2
3	U	T	T	T	U	U	J	J	J	U	U	K	K	K	U	U	Y	Y	Y	U	U	T	T	T	U	3
4	H	H	H	H	A	K	K	K	K	A	Q	Q	Q	Q	A	L	L	L	L	A	H	H	H	H	A	4
5	N	N	N	N	N	Q	Q	Q	Q	V	V	V	V	V	X	M	M	M	M	M	N	N	N	N	N	5
6	R	R	R	D	R	V	V	V	V	X	X	X	X	X	Z	P	P	P	J	P	R	R	R	K	R	6
7	S	S	F	F	S	X	X	X	D	Z	Z	Z	Z	R	J	W	W	K	K	W	S	S	Q	Q	S	7
8	T	G	G	G	T	Z	Z	F	F	J	J	J	S	S	K	Y	Q	Q	Q	Y	T	V	V	V	T	8
9	B	B	B	B	H	J	G	G	G	K	K	T	T	T	Q	V	V	V	V	L	X	X	X	X	H	9
10	C	C	C	C	C	B	B	B	B	Q	H	H	H	H	V	X	X	X	X	Z	Z	Z	Z	Z	J	10
11	D	D	D	P	D	C	C	C	C	C	N	N	N	N	N	Z	Z	Z	Z	J	J	J	J	J	K	11
12	F	F	W	W	F	D	D	D	R	D	R	R	R	P	R	J	J	J	R	K	K	K	K	D	Q	12
13	G	Y	Y	Y	G	F	F	S	S	F	S	S	W	W	S	K	K	S	S	Q	Q	Q	F	F	V	13
14	L	L	L	L	B	G	T	T	T	G	T	Y	Y	Y	T	Q	T	T	T	V	V	G	G	G	X	14
15	M	M	M	M	M	H	H	H	H	B	L	L	L	L	H	H	H	H	H	X	B	B	B	B	Z	15
16	P	P	P	V	P	N	N	N	N	N	M	M	M	M	M	N	N	N	N	N	C	C	C	C	C	16
17	W	W	X	X	W	R	R	R	P	R	P	P	P	D	P	R	R	R	D	R	D	D	D	P	D	17
18	Y	Z	Z	Z	Y	S	S	W	W	S	W	W	F	F	W	S	S	F	F	S	F	F	W	W	F	18
19	J	J	J	J	L	T	Y	Y	Y	T	Y	G	G	G	Y	T	G	G	G	T	G	Y	Y	Y	G	19
20	K	K	K	K	Q	L	L	L	L	H	B	B	B	B	L	B	B	B	B	H	L	L	L	L	B	20
21	Q	Q	Q	Q	V	M	M	M	M	M	C	C	C	C	C	C	C	C	C	C	M	M	M	M	M	21
22	V	V	V	I	X	P	P	P	I	P	D	D	D	I	D	D	D	D	I	D	P	P	P	I	P	22
23	X	X	O	O	Z	W	W	O	O	W	F	F	O	O	F	F	F	O	O	F	W	W	O	O	W	23
24	Z	U	U	U	J	Y	U	U	U	Y	G	U	U	U	G	G	U	U	U	G	Y	U	U	U	Y	24
25	A	A	A	A	K	A	A	A	A	L	A	A	A	A	B	A	A	A	A	B	A	A	A	A	L	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER

F

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
1	G	Y	G	G	G	G	T	G	G	G	G	U	G	G	G	G	U	G	G	G	G	Y	G	G	G
2	L	L	B	B	B	H	H	B	B	B	A	A	B	B	B	A	A	B	B	B	L	L	B	B	B
3	M	M	C	C	M	N	N	C	C	N	E	E	C	C	E	E	E	C	C	E	M	M	C	C	M
4	P	P	D	P	P	R	R	D	R	R	I	I	D	I	I	I	I	D	I	I	P	P	D	P	P
5	W	W	W	W	W	S	S	S	S	S	O	O	O	O	O	O	O	O	O	O	W	W	W	W	W
6	Y	Z	Y	Y	Y	T	Y	T	T	T	U	K	U	U	U	U	Y	U	U	U	Y	U	Y	Y	Y
7	J	J	L	L	L	L	L	H	H	H	Q	Q	A	A	A	L	L	A	A	A	A	A	L	L	L
8	K	K	M	M	Q	M	M	N	N	M	V	V	E	E	X	M	M	E	E	M	E	E	M	M	E
9	Q	Q	P	V	V	P	P	R	P	P	X	X	I	Z	Z	P	P	I	P	P	I	I	P	I	I
10	V	V	X	X	X	W	W	W	W	W	Z	Z	J	J	J	W	W	W	W	W	O	O	O	O	O
11	X	X	Z	Z	Z	Y	U	Y	Y	Y	J	J	K	K	K	Y	Q	Y	Y	Y	U	T	U	U	U
12	Z	U	J	J	J	A	A	L	L	L	K	T	Q	Q	Q	V	V	L	L	L	H	H	A	A	A
13	A	A	K	K	K	E	E	M	M	E	H	H	V	V	V	X	X	M	M	Z	N	N	E	E	N
14	E	E	Q	Q	E	I	I	P	I	I	N	N	X	X	N	Z	Z	P	J	J	R	R	I	R	R
15	I	I	V	I	I	O	O	O	O	O	R	R	Z	R	R	J	J	K	K	K	S	S	S	S	S
16	O	O	O	O	O	U	J	U	U	U	S	S	S	S	S	K	K	Q	Q	Q	T	V	T	T	T
17	U	T	U	U	U	K	K	A	A	A	T	Y	T	T	T	Q	T	V	V	V	X	X	H	H	H
18	H	H	A	A	A	Q	Q	E	E	V	L	L	H	H	H	H	H	X	X	X	Z	Z	N	N	J
19	N	N	E	E	N	V	V	I	X	X	M	M	N	N	M	N	N	Z	Z	N	J	J	R	K	K
20	R	R	I	R	R	X	X	Z	Z	Z	P	P	R	P	P	R	R	J	R	R	K	K	Q	Q	Q
21	S	S	S	S	S	Z	Z	J	J	J	W	W	W	W	W	S	S	S	S	S	Q	Q	V	V	V
22	T	G	T	T	T	J	G	K	K	K	Y	G	Y	Y	Y	T	G	T	T	T	V	G	X	X	X
23	B	B	H	H	H	B	B	Q	Q	Q	B	B	L	L	L	B	B	H	H	H	B	B	Z	Z	Z
24	C	C	N	N	C	C	C	V	V	C	C	C	M	M	C	C	C	N	N	C	C	C	J	J	C
25	D	D	R	D	D	D	D	X	D	D	D	D	P	D	D	D	D	R	D	D	D	D	K	D	D

E F G H I J K L M N O P Q R S T U V W X Y Z

SYNOPTIC TABLE OF THE LETTER
G

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	0
1	L	B	B	B	B	H	B	B	B	B	A	B	B	B	B	A	B	B	B	B	L	B	B	B	B	1
2	M	C	C	C	M	N	C	C	C	N	E	C	C	C	E	E	C	C	C	E	M	C	C	C	M	2
3	P	D	D	P	P	R	D	D	R	R	I	D	D	I	I	I	D	D	I	I	P	D	D	P	P	3
4	W	F	W	W	W	S	F	S	S	S	O	F	O	O	O	O	F	O	O	O	W	F	W	W	W	4
5	Y	Y	Y	Y	Y	T	T	T	T	T	U	U	U	U	U	U	U	U	U	U	Y	Y	Y	Y	Y	5
6	J	L	L	L	L	L	H	H	H	H	Q	A	A	A	A	L	A	A	A	A	A	L	L	L	L	6
7	K	M	M	M	Q	M	N	N	N	M	V	E	E	E	X	M	E	E	E	M	E	M	M	M	E	7
8	Q	P	P	V	V	P	R	R	P	P	X	I	I	Z	Z	P	I	I	P	P	I	P	P	I	I	8
9	V	W	X	X	X	W	S	W	W	W	Z	O	J	J	J	W	O	W	W	W	O	W	O	O	O	9
10	X	Z	Z	Z	Z	Y	Y	Y	Y	Y	J	K	K	K	K	Y	Y	Y	Y	Y	U	U	U	U	U	10
11	Z	J	J	J	J	A	L	L	L	L	K	Q	Q	Q	Q	V	L	L	L	L	H	A	A	A	A	11
12	A	K	K	K	K	E	M	M	M	E	H	V	V	V	V	X	M	M	M	Z	N	E	E	E	N	12
13	E	Q	Q	Q	E	I	P	P	I	I	N	X	X	X	N	Z	P	P	J	J	R	I	I	R	R	13
14	I	V	V	I	I	O	W	O	O	O	R	Z	Z	R	R	J	W	K	K	K	S	O	S	S	S	14
15	O	X	O	O	O	U	U	U	U	U	S	J	S	S	S	K	Q	Q	Q	Q	T	T	T	T	T	15
16	U	U	U	U	U	K	A	A	A	A	T	T	T	T	T	Q	V	V	V	V	X	H	H	H	H	16
17	H	A	A	A	A	Q	E	E	E	V	L	H	H	H	H	H	X	X	X	X	Z	N	N	N	J	17
18	N	E	E	E	N	V	I	I	X	X	M	N	N	N	M	N	Z	Z	Z	N	J	R	R	K	K	18
19	R	I	I	R	R	X	O	Z	Z	Z	P	R	R	P	P	R	J	J	R	R	K	S	Q	Q	Q	19
20	S	O	S	S	S	Z	J	J	J	J	W	S	W	W	W	S	K	S	S	S	Q	V	V	V	V	20
21	T	T	T	T	T	J	K	K	K	K	Y	Y	Y	Y	Y	T	T	T	T	T	V	X	X	X	X	21
22	B	H	H	H	H	B	Q	Q	Q	Q	B	L	L	L	L	B	H	H	H	H	B	Z	Z	Z	Z	22
23	C	N	N	N	C	C	V	V	V	C	C	M	M	M	C	C	N	N	N	C	C	J	J	J	C	23
24	D	R	R	D	D	D	X	X	D	D	D	P	P	D	D	D	R	R	D	D	D	K	K	D	D	24
25	F	S	F	F	F	F	Z	F	F	F	F	W	F	F	F	F	S	F	F	F	F	Q	F	F	F	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

SYNOPTIC TABLE OF THE LETTER H

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	0
1	N	N	N	N	C	N	N	N	N	M	N	N	N	N	M	N	N	N	N	C	N	N	N	N	J	1
2	R	R	R	D	D	R	R	R	P	P	R	R	R	P	P	R	R	R	D	D	R	R	R	K	K	2
3	S	S	F	F	F	S	S	W	W	W	S	S	W	W	W	S	S	F	F	F	S	S	Q	Q	Q	3
4	T	G	G	G	G	T	Y	Y	Y	Y	T	Y	Y	Y	Y	T	G	G	G	G	T	V	V	V	V	4
5	B	B	B	B	B	L	L	L	L	L	L	L	L	L	L	B	B	B	B	B	X	X	X	X	X	5
6	C	C	C	C	M	M	M	M	M	E	M	M	M	M	C	C	C	C	C	E	Z	Z	Z	Z	Z	6
7	D	D	D	P	P	P	P	P	I	I	P	P	P	D	D	D	D	D	I	I	J	J	J	J	C	7
8	F	F	W	W	W	W	W	O	O	O	W	W	F	F	F	F	F	O	O	O	K	K	K	D	D	8
9	G	Y	Y	Y	Y	Y	U	U	U	U	Y	G	G	G	G	G	U	U	U	U	Q	Q	F	F	F	9
10	L	L	L	L	L	A	A	A	A	A	B	B	B	B	B	A	A	A	A	A	V	G	G	G	G	10
11	M	M	M	M	Q	E	E	E	E	V	C	C	C	C	E	E	E	E	E	M	B	B	B	B	B	11
12	P	P	P	V	V	I	I	I	X	X	D	D	D	I	I	I	I	I	P	P	C	C	C	C	M	12
13	W	W	X	X	X	O	O	Z	Z	Z	F	F	O	O	O	O	O	W	W	W	D	D	D	P	P	13
14	Y	Z	Z	Z	Z	U	J	J	J	J	G	U	U	U	U	U	Y	Y	Y	Y	F	F	W	W	W	14
15	J	J	J	J	J	K	K	K	K	K	A	A	A	A	A	L	L	L	L	L	G	Y	Y	Y	Y	15
16	K	K	K	K	K	Q	Q	Q	Q	Q	E	E	E	E	X	M	M	M	M	Z	L	L	L	L	L	16
17	Q	Q	Q	Q	E	V	V	V	V	C	I	I	I	Z	Z	P	P	P	J	J	M	M	M	M	E	17
18	V	V	V	I	I	X	X	X	D	D	O	O	J	J	J	W	W	K	K	K	P	P	P	I	I	18
19	X	X	O	O	O	Z	Z	F	F	F	U	K	K	K	K	Y	Q	Q	Q	Q	W	W	O	O	O	19
20	Z	U	U	U	U	J	G	G	G	G	Q	Q	Q	Q	Q	V	V	V	V	V	Y	U	U	U	U	20
21	A	A	A	A	A	B	B	B	B	B	V	V	V	V	V	X	X	X	X	X	A	A	A	A	A	21
22	E	E	E	E	N	C	C	C	C	N	X	X	X	X	N	Z	Z	Z	Z	N	E	E	E	E	N	22
23	I	I	I	R	R	D	D	D	R	R	Z	Z	Z	R	R	J	J	J	R	R	I	I	I	R	R	23
24	O	O	S	S	S	F	F	S	S	S	J	J	S	S	S	K	K	S	S	S	O	O	S	S	S	24
25	U	T	T	T	T	G	T	T	T	T	K	T	T	T	T	Q	T	T	T	T	U	T	T	T	T	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER I

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	0
1	O	O	S	O	O	O	O	Z	O	O	O	O	J	O	O	O	O	W	O	O	O	O	S	O	O	1
2	U	T	T	U	U	U	J	J	U	U	U	K	K	U	U	U	Y	Y	U	U	U	T	T	U	U	2
3	H	H	H	A	A	K	K	K	A	A	Q	Q	Q	A	A	L	L	L	A	A	H	H	H	A	A	3
4	N	N	N	E	N	Q	Q	Q	E	V	V	V	V	E	X	M	M	M	E	M	N	N	N	E	N	4
5	R	R	R	R	R	V	V	V	X	X	X	X	X	Z	Z	P	P	P	P	P	R	R	R	R	R	5
6	S	S	F	S	S	X	X	X	Z	Z	Z	Z	Z	J	J	W	W	K	W	W	S	S	Q	S	S	6
7	T	G	G	T	T	Z	Z	F	J	J	J	J	S	K	K	Y	Q	Q	Y	Y	T	V	V	T	T	7
8	B	B	B	H	H	J	G	G	K	K	K	T	T	Q	Q	V	V	V	L	L	X	X	X	H	H	8
9	C	C	C	N	C	B	B	B	Q	Q	H	H	H	V	V	X	X	X	M	Z	Z	Z	Z	N	J	9
10	D	D	D	D	D	C	C	C	V	C	N	N	N	X	N	Z	Z	Z	J	J	J	J	J	K	K	10
11	F	F	W	F	F	D	D	D	D	D	R	R	R	R	R	J	J	J	K	K	K	K	K	Q	Q	11
12	G	Y	Y	G	G	F	F	S	F	F	S	S	W	S	S	K	K	S	Q	Q	Q	Q	F	V	V	12
13	L	L	L	B	B	G	T	T	G	G	T	Y	Y	T	T	Q	T	T	V	V	V	G	G	X	X	13
14	M	M	M	C	M	H	H	H	B	B	L	L	L	H	H	H	H	H	X	X	B	B	B	Z	Z	14
15	P	P	P	P	P	N	N	N	C	N	M	M	M	N	M	N	N	N	Z	N	C	C	C	J	C	15
16	W	W	X	W	W	R	R	R	R	R	P	P	P	P	P	R	R	R	R	R	D	D	D	D	D	16
17	Y	Z	Z	Y	Y	S	S	W	S	S	W	W	F	W	W	S	S	F	S	S	F	F	W	F	F	17
18	J	J	J	L	L	T	Y	Y	T	T	Y	G	G	Y	Y	T	G	G	T	T	G	Y	Y	G	G	18
19	K	K	K	M	Q	L	L	L	H	H	B	B	B	L	L	B	B	B	H	H	L	L	L	B	B	19
20	Q	Q	Q	V	V	M	M	M	N	M	C	C	C	M	C	C	C	C	N	C	M	M	M	C	M	20
21	V	V	V	X	X	P	P	P	P	P	D	D	D	D	D	D	D	D	D	D	P	P	P	P	P	21
22	X	X	O	Z	Z	W	W	O	W	W	F	F	O	F	F	F	F	O	F	F	W	W	O	W	W	22
23	Z	U	U	J	J	Y	U	U	Y	Y	G	U	U	G	G	G	U	U	G	G	Y	U	U	Y	Y	23
24	A	A	A	K	K	A	A	A	L	L	A	A	A	B	B	A	A	A	B	B	A	A	A	L	L	24
25	E	E	E	Q	E	E	E	E	M	E	E	E	E	C	E	E	E	E	C	E	E	E	E	M	E	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER
J

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	J	0
1	K	K	K	K	K	B	K	K	K	K	K	T	K	K	K	K	K	S	K	K	K	K	K	D	K	1
2	Q	Q	Q	Q	E	C	Q	Q	Q	Q	H	H	Q	Q	Q	Q	T	T	Q	Q	Q	Q	F	F	Q	2
3	V	V	V	I	I	D	V	V	V	C	N	N	V	V	V	H	H	H	V	V	V	G	G	G	V	3
4	X	X	O	O	O	F	X	X	D	D	R	R	X	X	N	N	N	N	X	X	B	B	B	B	X	4
5	Z	U	U	U	U	G	Z	F	F	F	S	S	Z	R	R	R	R	R	Z	N	C	C	C	C	Z	5
6	A	A	A	A	A	H	G	G	G	G	T	Y	S	S	S	S	S	F	R	R	D	D	D	P	C	6
7	E	E	E	E	N	N	B	B	B	B	L	L	T	T	T	T	G	G	S	S	F	F	W	W	D	7
8	I	I	I	R	R	R	C	C	C	N	M	M	H	H	H	B	B	B	T	T	G	Y	Y	Y	F	8
9	O	O	S	S	S	S	D	D	R	R	P	P	N	N	M	C	C	C	H	H	L	L	L	L	G	9
10	U	T	T	T	T	T	F	S	S	S	W	W	R	P	P	D	D	D	N	C	M	M	M	M	B	10
11	H	H	H	H	H	L	T	T	T	T	Y	G	W	W	W	F	F	O	D	D	P	P	P	I	M	11
12	N	N	N	N	C	M	H	H	H	H	B	B	Y	Y	Y	G	U	U	F	F	W	W	O	O	P	12
13	R	R	R	D	D	P	N	N	N	M	C	C	L	L	L	A	A	A	G	G	Y	U	U	U	W	13
14	S	S	F	F	F	W	R	R	P	P	D	D	M	M	C	E	E	E	B	B	A	A	A	A	Y	14
15	T	G	G	G	G	Y	S	W	W	W	F	F	P	D	D	I	I	I	C	E	E	E	E	E	L	15
16	B	B	B	B	B	A	Y	Y	Y	Y	G	U	F	F	F	O	O	W	I	I	I	I	I	R	E	16
17	C	C	C	C	M	E	L	L	L	L	A	A	G	G	G	U	Y	Y	O	O	O	O	S	S	I	17
18	D	D	D	P	P	I	M	M	M	E	E	E	B	B	B	L	L	L	U	U	U	T	T	T	O	18
19	F	F	W	W	W	O	P	P	I	I	I	I	C	C	E	M	M	M	A	A	H	H	H	H	U	19
20	G	Y	Y	Y	Y	U	W	O	O	O	O	O	D	I	I	P	P	P	E	M	N	N	N	N	A	20
21	L	L	L	L	L	K	U	U	U	U	U	K	O	O	O	W	W	K	P	P	R	R	R	K	N	21
22	M	M	M	M	Q	Q	A	A	A	A	Q	Q	U	U	U	Y	Q	Q	W	W	S	S	Q	Q	R	22
23	P	P	P	V	V	V	E	E	E	V	V	V	A	A	A	V	V	V	Y	Y	T	V	V	V	S	23
24	W	W	X	X	X	X	I	I	X	X	X	X	E	E	X	X	X	X	L	L	X	X	X	X	T	24
25	Y	Z	Z	Z	Z	Z	O	Z	Z	Z	Z	Z	I	Z	Z	Z	Z	Z	M	Z	Z	Z	Z	Z	H	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

I J K L M N O P Q R S T U V W X Y Z

SYNOPTIC TABLE OF THE LETTER
K

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K
1	Q	Q	Q	Q	E	Q	Q	Q	Q	Q	H	Q	Q	Q	Q	Q	T	Q	Q	Q	Q	Q	F	Q	Q
2	V	V	V	I	I	V	V	V	V	C	N	V	V	V	V	H	H	V	V	V	V	G	G	V	V
3	X	X	O	O	O	X	X	X	D	D	R	X	X	X	N	N	N	X	X	X	B	B	B	X	X
4	Z	U	U	U	U	Z	Z	F	F	F	S	Z	Z	R	R	R	R	Z	Z	N	C	C	C	Z	Z
5	A	A	A	A	A	J	G	G	G	G	T	J	S	S	S	S	S	J	R	R	D	D	D	J	C
6	E	E	E	E	N	B	B	B	B	B	L	T	T	T	T	T	G	S	S	S	F	F	W	D	D
7	I	I	I	R	R	C	C	C	C	N	M	H	H	H	H	B	B	T	T	T	G	Y	Y	F	F
8	O	O	S	S	S	D	D	D	R	R	P	N	N	N	M	C	C	H	H	H	L	L	L	G	G
9	U	T	T	T	T	F	F	S	S	S	W	R	R	P	P	D	D	N	N	C	M	M	M	B	B
10	H	H	H	H	H	G	T	T	T	T	Y	S	W	W	W	F	F	R	D	D	P	P	P	C	M
11	N	N	N	N	C	H	H	H	H	H	B	Y	Y	Y	Y	G	U	F	F	F	W	W	O	P	P
12	R	R	R	D	D	N	N	N	N	M	C	L	L	L	L	A	A	G	G	G	Y	U	U	W	W
13	S	S	F	F	F	R	R	R	P	P	D	M	M	M	C	E	E	B	B	B	A	A	A	Y	Y
14	T	G	G	G	G	S	S	W	W	W	F	P	P	D	D	I	I	C	C	E	E	E	E	L	L
15	B	B	B	B	B	T	Y	Y	Y	Y	G	W	F	F	F	O	O	D	I	I	I	I	I	M	E
16	C	C	C	C	M	L	L	L	L	L	A	G	G	G	G	U	Y	O	O	O	O	O	S	I	I
17	D	D	D	P	P	M	M	M	M	E	E	B	B	B	B	L	L	U	U	U	U	T	T	O	O
18	F	F	W	W	W	P	P	P	I	I	I	C	C	C	E	M	M	A	A	A	H	H	H	U	U
19	G	Y	Y	Y	Y	W	W	O	O	O	O	D	D	I	I	P	P	E	E	M	N	N	N	A	A
20	L	L	L	L	L	Y	U	U	U	U	U	F	O	O	O	W	W	I	P	P	R	R	R	E	N
21	M	M	M	M	Q	A	A	A	A	A	Q	U	U	U	U	Y	Q	W	W	W	S	S	Q	R	R
22	P	P	P	V	V	E	E	E	E	V	V	A	A	A	A	V	V	Y	Y	Y	T	V	V	S	S
23	W	W	X	X	X	I	I	I	X	X	X	E	E	E	X	X	X	L	L	L	X	X	X	T	T
24	Y	Z	Z	Z	Z	O	O	Z	Z	Z	Z	I	I	Z	Z	Z	Z	M	M	Z	Z	Z	Z	H	H
25	J	J	J	J	J	U	J	J	J	J	J	O	J	J	J	J	J	P	J	J	J	J	J	N	J

SYNOPTIC TABLE OF THE LETTER
L

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	0
1	M	M	M	M	Q	M	M	M	M	E	M	M	M	M	C	M	M	M	M	Z	M	M	M	M	E	1
2	P	P	P	V	V	P	P	P	I	I	P	P	P	D	D	P	P	P	J	J	P	P	P	I	I	2
3	W	W	X	X	X	W	W	O	O	O	W	W	F	F	F	W	W	K	K	K	W	W	O	O	O	3
4	Y	Z	Z	Z	Z	Y	U	U	U	U	Y	G	G	G	G	Y	Q	Q	Q	Q	Y	U	U	U	U	4
5	J	J	J	J	J	A	A	A	A	A	B	B	B	B	B	V	V	V	V	V	A	A	A	A	A	5
6	K	K	K	K	K	E	E	E	E	V	C	C	C	C	E	X	X	X	X	X	E	E	E	E	N	6
7	Q	Q	Q	Q	E	I	I	I	X	X	D	D	D	I	I	Z	Z	Z	Z	N	I	I	I	R	R	7
8	V	V	V	I	I	O	O	Z	Z	Z	F	F	O	O	O	J	J	J	R	R	O	O	S	S	S	8
9	X	X	O	O	O	U	J	J	J	J	G	U	U	U	U	K	K	S	S	S	U	T	T	T	T	9
10	Z	U	U	U	U	K	K	K	K	K	A	A	A	A	A	Q	T	T	T	T	H	H	H	H	H	10
11	A	A	A	A	A	Q	Q	Q	Q	Q	E	E	E	E	X	H	H	H	H	H	N	N	N	N	J	11
12	E	E	E	E	N	V	V	V	V	C	I	I	I	Z	Z	N	N	N	N	C	R	R	R	K	K	12
13	I	I	I	R	R	X	X	X	D	D	O	O	J	J	J	R	R	R	D	D	S	S	Q	Q	Q	13
14	O	O	S	S	S	Z	Z	F	F	F	U	K	K	K	K	S	S	F	F	F	T	V	V	V	V	14
15	U	T	T	T	T	J	G	G	G	G	Q	Q	Q	Q	Q	T	G	G	G	G	X	X	X	X	X	15
16	H	H	H	H	H	B	B	B	B	B	V	V	V	V	V	B	B	B	B	B	Z	Z	Z	Z	Z	16
17	N	N	N	N	C	C	C	C	C	N	X	X	X	X	N	C	C	C	C	E	J	J	J	J	C	17
18	R	R	R	D	D	D	D	D	R	R	Z	Z	Z	R	R	D	D	D	I	I	K	K	K	D	D	18
19	S	S	F	F	F	F	F	S	S	S	J	J	S	S	S	F	F	O	O	O	Q	Q	F	F	F	19
20	T	G	G	G	G	G	T	T	T	T	K	T	T	T	T	G	U	U	U	U	V	G	G	G	G	20
21	B	B	B	B	B	H	H	H	H	H	H	H	H	H	H	A	A	A	A	A	B	B	B	B	B	21
22	C	C	C	C	M	N	N	N	N	M	N	N	N	N	M	E	E	E	E	M	C	C	C	C	M	22
23	D	D	D	P	P	R	R	R	P	P	R	R	R	P	P	I	I	I	P	P	D	D	D	P	P	23
24	F	F	W	W	W	S	S	W	W	W	S	S	W	W	W	O	O	W	W	W	F	F	W	W	W	24
25	G	Y	Y	Y	Y	T	Y	Y	Y	Y	T	Y	Y	Y	Y	U	Y	Y	Y	Y	G	Y	Y	Y	Y	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

K L M N O P Q R S T U V W X Y Z

SYNOPTIC TABLE OF THE LETTER M

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	0
1	P	P	P	V	P	P	P	P	I	P	P	P	P	D	P	P	P	P	J	P	P	P	P	I	P	1
2	W	W	X	X	W	W	W	O	O	W	W	W	F	F	W	W	W	K	K	W	W	W	O	O	W	2
3	Y	Z	Z	Z	Y	Y	U	U	U	Y	Y	G	G	G	Y	Y	Q	Q	Q	Y	Y	U	U	U	Y	3
4	J	J	J	J	L	A	A	A	A	L	B	B	B	B	L	V	V	V	V	L	A	A	A	A	L	4
5	K	K	K	K	Q	E	E	E	E	E	C	C	C	C	C	X	X	X	X	Z	E	E	E	E	E	5
6	Q	Q	Q	Q	V	I	I	I	X	I	D	D	D	I	D	Z	Z	Z	Z	J	I	I	I	R	I	6
7	V	V	V	I	X	O	O	Z	Z	O	F	F	O	O	F	J	J	J	R	K	O	O	S	S	O	7
8	X	X	O	O	Z	U	J	J	J	U	G	U	U	U	G	K	K	S	S	Q	U	T	T	T	U	8
9	Z	U	U	U	J	K	K	K	K	A	A	A	A	A	B	Q	T	T	T	V	H	H	H	H	A	9
10	A	A	A	A	K	Q	Q	Q	Q	V	E	E	E	E	E	H	H	H	H	X	N	N	N	N	N	10
11	E	E	E	E	E	V	V	V	V	X	I	I	I	Z	I	N	N	N	N	N	R	R	R	K	R	11
12	I	I	I	R	I	X	X	X	D	Z	O	O	J	J	O	R	R	R	D	R	S	S	Q	Q	S	12
13	O	O	S	S	O	Z	Z	F	F	J	U	K	K	K	U	S	S	F	F	S	T	V	V	V	T	13
14	U	T	T	T	U	J	G	G	G	K	Q	Q	Q	Q	A	T	G	G	G	T	X	X	X	X	H	14
15	H	H	H	H	A	B	B	B	B	Q	V	V	V	V	X	B	B	B	B	H	Z	Z	Z	Z	J	15
16	N	N	N	N	N	C	C	C	C	C	X	X	X	X	Z	C	C	C	C	C	J	J	J	J	K	16
17	R	R	R	D	R	D	D	D	R	D	Z	Z	Z	R	J	D	D	D	I	D	K	K	K	D	Q	17
18	S	S	F	F	S	F	F	S	S	F	J	J	S	S	K	F	F	O	O	F	Q	Q	F	F	V	18
19	T	G	G	G	T	G	T	T	T	G	K	T	T	T	Q	G	U	U	U	G	V	G	G	G	X	19
20	B	B	B	B	H	H	H	H	H	B	H	H	H	H	V	A	A	A	A	B	B	B	B	B	Z	20
21	C	C	C	C	C	N	N	N	N	N	N	N	N	N	N	E	E	E	E	E	C	C	C	C	C	21
22	D	D	D	P	D	R	R	R	P	R	R	R	R	P	R	I	I	I	P	I	D	D	D	P	D	22
23	F	F	W	W	F	S	S	W	W	S	S	S	W	W	S	O	O	W	W	O	F	F	W	W	F	23
24	G	Y	Y	Y	G	T	Y	Y	Y	T	T	Y	Y	Y	T	U	Y	Y	Y	U	G	Y	Y	Y	G	24
25	L	L	L	L	B	L	L	L	L	H	L	L	L	L	H	L	L	L	L	A	L	L	L	L	B	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

SYNOPTIC TABLE OF THE LETTER

N

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	0
1	R	R	R	D	R	R	R	R	P	R	R	R	R	P	R	R	R	R	D	R	R	R	R	K	R	1
2	S	S	F	F	S	S	S	W	W	S	S	S	W	W	S	S	S	F	F	S	S	S	Q	Q	S	2
3	T	G	G	G	T	T	Y	Y	Y	T	T	Y	Y	Y	T	T	G	G	G	T	T	V	V	V	T	3
4	B	B	B	B	H	L	L	L	L	H	L	L	L	L	H	B	B	B	B	H	X	X	X	X	H	4
5	C	C	C	C	C	M	M	M	M	M	M	M	M	M	M	C	C	C	C	C	Z	Z	Z	Z	J	5
6	D	D	D	P	D	P	P	P	I	P	P	P	P	D	P	D	D	D	I	D	J	J	J	J	K	6
7	F	F	W	W	F	W	W	O	O	W	W	W	F	F	W	F	F	O	O	F	K	K	K	D	Q	7
8	G	Y	Y	Y	G	Y	U	U	U	Y	Y	G	G	G	Y	G	U	U	U	G	Q	Q	F	F	V	8
9	L	L	L	L	B	A	A	A	A	L	B	B	B	B	L	A	A	A	A	B	V	G	G	G	X	9
10	M	M	M	M	M	E	E	E	E	E	C	C	C	C	C	E	E	E	E	E	B	B	B	B	Z	10
11	P	P	P	V	P	I	I	I	X	I	D	D	D	I	D	I	I	I	P	I	C	C	C	C	C	11
12	W	W	X	X	W	O	O	Z	Z	O	F	F	O	O	F	O	O	W	W	O	D	D	D	P	D	12
13	Y	Z	Z	Z	Y	U	J	J	J	U	G	U	U	U	G	U	Y	Y	Y	U	F	F	W	W	F	13
14	J	J	J	J	L	K	K	K	K	A	A	A	A	A	B	L	L	L	L	A	G	Y	Y	Y	G	14
15	K	K	K	K	Q	Q	Q	Q	Q	V	E	E	E	E	E	M	M	M	M	M	L	L	L	L	B	15
16	Q	Q	Q	Q	V	V	V	V	V	X	I	I	I	Z	I	P	P	P	J	P	M	M	M	M	M	16
17	V	V	V	I	X	X	X	X	D	Z	O	O	J	J	O	W	W	K	K	W	P	P	P	I	P	17
18	X	X	O	O	Z	Z	Z	F	F	J	U	K	K	K	U	Y	Q	Q	Q	Y	W	W	O	O	W	18
19	Z	U	U	U	J	J	G	G	G	K	Q	Q	Q	Q	A	V	V	V	V	L	Y	U	U	U	Y	19
20	A	A	A	A	K	B	B	B	B	Q	V	V	V	V	X	X	X	X	X	Z	A	A	A	A	L	20
21	E	E	E	E	E	C	C	C	C	C	X	X	X	X	Z	Z	Z	Z	Z	J	E	E	E	E	E	21
22	I	I	I	R	I	D	D	D	R	D	Z	Z	Z	R	J	J	J	J	R	K	I	I	I	R	I	22
23	O	O	S	S	O	F	F	S	S	F	J	J	S	S	K	K	K	S	S	Q	O	O	S	S	O	23
24	U	T	T	T	U	G	T	T	T	G	K	T	T	T	Q	Q	T	T	T	V	U	T	T	T	U	24
25	H	H	H	H	A	H	H	H	H	B	H	H	H	H	V	H	H	H	H	X	H	H	H	H	A	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

M N O P Q R S T U V W X Y Z

SYNOPTIC TABLE OF THE LETTER

O

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
1	U	T	U	U	U	U	J	U	U	U	U	K	U	U	U	U	Y	U	U	U	U	T	U	U	U
2	H	H	A	A	A	K	K	A	A	A	Q	Q	A	A	A	L	L	A	A	A	H	H	A	A	A
3	N	N	E	E	N	Q	Q	E	E	V	V	V	E	E	X	M	M	E	E	M	N	N	E	E	N
4	R	R	I	R	R	V	V	I	X	X	X	X	I	Z	Z	P	P	I	P	P	R	R	I	R	R
5	S	S	S	S	S	X	X	Z	Z	Z	Z	Z	J	J	J	W	W	W	W	W	S	S	S	S	S
6	T	G	T	T	T	Z	Z	J	J	J	J	J	K	K	K	Y	Q	Y	Y	Y	T	V	T	T	T
7	B	B	H	H	H	J	G	K	K	K	K	T	Q	Q	Q	V	V	L	L	L	X	X	H	H	H
8	C	C	N	N	C	B	B	Q	Q	Q	H	H	V	V	V	X	X	M	M	Z	Z	Z	N	N	J
9	D	D	R	D	D	C	C	V	V	C	N	N	X	X	N	Z	Z	P	J	J	J	J	R	K	K
10	F	F	F	F	F	D	D	X	D	D	R	R	Z	R	R	J	J	K	K	K	K	K	Q	Q	Q
11	G	Y	G	G	G	F	F	F	F	F	S	S	S	S	S	K	K	Q	Q	Q	Q	Q	V	V	V
12	L	L	B	B	B	G	T	G	G	G	T	Y	T	T	T	Q	T	V	V	V	V	G	X	X	X
13	M	M	C	C	M	H	H	B	B	B	L	L	H	H	H	H	H	X	X	X	B	B	Z	Z	Z
14	P	P	D	P	P	N	N	C	C	N	M	M	N	N	M	N	N	Z	Z	N	C	C	J	J	C
15	W	W	W	W	W	R	R	D	R	R	P	P	R	P	P	R	R	J	R	R	D	D	K	D	D
16	Y	Z	Y	Y	Y	S	S	S	S	S	W	W	W	W	W	S	S	S	S	S	F	F	F	F	F
17	J	J	L	L	L	T	Y	T	T	T	Y	G	Y	Y	Y	T	G	T	T	T	G	Y	G	G	G
18	K	K	M	M	Q	L	L	H	H	H	B	B	L	L	L	B	B	H	H	H	L	L	B	B	B
19	Q	Q	P	V	V	M	M	N	N	M	C	C	M	M	C	C	C	N	N	C	M	M	C	C	M
20	V	V	X	X	X	P	P	R	P	P	D	D	P	D	D	D	D	R	D	D	P	P	D	P	P
21	X	X	Z	Z	Z	W	W	W	W	W	F	F	F	F	F	F	F	F	F	F	W	W	W	W	W
22	Z	U	J	J	J	Y	U	Y	Y	Y	G	U	G	G	G	G	U	G	G	G	Y	U	Y	Y	Y
23	A	A	K	K	K	A	A	L	L	L	A	A	B	B	B	A	A	B	B	B	A	A	L	L	L
24	E	E	Q	Q	E	E	E	M	M	E	E	E	C	C	E	E	E	C	C	E	E	E	M	M	E
25	I	I	V	I	I	I	I	P	I	I	I	I	D	I	I	I	I	D	I	I	I	I	P	I	I

SYNOPTIC TABLE OF THE LETTER P

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	0
1	W	W	X	W	W	W	W	O	W	W	W	W	F	W	W	W	W	K	W	W	W	W	O	W	W	1
2	Y	Z	Z	Y	Y	Y	U	U	Y	Y	Y	G	G	Y	Y	Y	Q	Q	Y	Y	Y	U	U	Y	Y	2
3	J	J	J	L	L	A	A	A	L	L	B	B	B	L	L	V	V	V	L	L	A	A	A	L	L	3
4	K	K	K	M	Q	E	E	E	M	E	C	C	C	M	C	X	X	X	M	Z	E	E	E	M	E	4
5	Q	Q	Q	V	V	I	I	I	I	I	D	D	D	D	D	Z	Z	Z	J	J	I	I	I	I	I	5
6	V	V	V	X	X	O	O	Z	O	O	F	F	O	F	F	J	J	J	K	K	O	O	S	O	O	6
7	X	X	O	Z	Z	U	J	J	U	U	G	U	U	G	G	K	K	S	Q	Q	U	T	T	U	U	7
8	Z	U	U	J	J	K	K	K	A	A	A	A	A	B	B	Q	T	T	V	V	H	H	H	A	A	8
9	A	A	A	K	K	Q	Q	Q	E	V	E	E	E	C	E	H	H	H	X	X	N	N	N	E	N	9
10	E	E	E	Q	E	V	V	V	X	X	I	I	I	I	I	N	N	N	Z	N	R	R	R	R	R	10
11	I	I	I	I	I	X	X	X	Z	Z	O	O	J	O	O	R	R	R	R	R	S	S	Q	S	S	11
12	O	O	S	O	O	Z	Z	F	J	J	U	K	K	U	U	S	S	F	S	S	T	V	V	T	T	12
13	U	T	T	U	U	J	G	G	K	K	Q	Q	Q	A	A	T	G	G	T	T	X	X	X	H	H	13
14	H	H	H	A	A	B	B	B	Q	Q	V	V	V	E	X	B	B	B	H	H	Z	Z	Z	N	J	14
15	N	N	N	E	N	C	C	C	V	C	X	X	X	Z	Z	C	C	C	N	C	J	J	J	K	K	15
16	R	R	R	R	R	D	D	D	D	D	Z	Z	Z	J	J	D	D	D	D	D	K	K	K	Q	Q	16
17	S	S	F	S	S	F	F	S	F	F	J	J	S	K	K	F	F	O	F	F	Q	Q	F	V	V	17
18	T	G	G	T	T	G	T	T	G	G	K	T	T	Q	Q	G	U	U	G	G	V	G	G	X	X	18
19	B	B	B	H	H	H	H	H	B	B	H	H	H	V	V	A	A	A	B	B	B	B	B	Z	Z	19
20	C	C	C	N	C	N	N	N	C	N	N	N	N	X	N	E	E	E	C	E	C	C	C	J	C	20
21	D	D	D	D	D	R	R	R	R	R	R	R	R	R	R	I	I	I	I	I	D	D	D	D	D	21
22	F	F	W	F	F	S	S	W	S	S	S	S	W	S	S	O	O	W	O	O	F	F	W	F	F	22
23	G	Y	Y	G	G	T	Y	Y	T	T	T	Y	Y	T	T	U	Y	Y	U	U	G	Y	Y	G	G	23
24	L	L	L	B	B	L	L	L	H	H	L	L	L	H	H	L	L	L	A	A	L	L	L	B	B	24
25	M	M	M	C	M	M	M	M	N	M	M	M	M	N	M	M	M	M	E	M	M	M	M	C	M	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

SYNOPTIC TABLE OF THE LETTER

Q

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q
1	V	V	V	I	V	V	V	V	V	C	V	V	V	V	V	H	V	V	V	V	V	G	V	V	V
2	X	X	O	O	X	X	X	X	D	D	X	X	X	X	N	N	X	X	X	X	B	B	X	X	X
3	Z	U	U	U	Z	Z	Z	F	F	F	Z	Z	Z	R	R	R	Z	Z	Z	N	C	C	Z	Z	Z
4	A	A	A	A	J	J	G	G	G	G	J	J	S	S	S	S	J	J	R	R	D	D	J	J	C
5	E	E	E	E	K	B	B	B	B	B	K	T	T	T	T	T	K	S	S	S	F	F	K	D	D
6	I	I	I	R	E	C	C	C	C	N	H	H	H	H	H	B	T	T	T	T	G	Y	F	F	F
7	O	O	S	S	I	D	D	D	R	R	N	N	N	N	M	C	H	H	H	H	L	L	G	G	G
8	U	T	T	T	O	F	F	S	S	S	R	R	R	P	P	D	N	N	N	C	M	M	B	B	B
9	H	H	H	H	U	G	T	T	T	T	S	S	W	W	W	F	R	R	D	D	P	P	C	C	M
10	N	N	N	N	A	H	H	H	H	H	T	Y	Y	Y	Y	G	S	F	F	F	W	W	D	P	P
11	R	R	R	D	N	N	N	N	N	M	L	L	L	L	L	A	G	G	G	G	Y	U	W	W	W
12	S	S	F	F	R	R	R	R	P	P	M	M	M	M	C	E	B	B	B	B	A	A	Y	Y	Y
13	T	G	G	G	S	S	S	W	W	W	P	P	P	D	D	I	C	C	C	E	E	E	L	L	L
14	B	B	B	B	T	T	Y	Y	Y	Y	W	W	F	F	F	O	D	D	I	I	I	I	M	M	E
15	C	C	C	C	H	L	L	L	L	L	Y	G	G	G	G	U	F	O	O	O	O	O	P	I	I
16	D	D	D	P	C	M	M	M	M	E	B	B	B	B	B	L	U	U	U	U	U	T	O	O	O
17	F	F	W	W	D	P	P	P	I	I	C	C	C	C	E	M	A	A	A	A	H	H	U	U	U
18	G	Y	Y	Y	F	W	W	O	O	O	D	D	D	I	I	P	E	E	E	M	N	N	A	A	A
19	L	L	L	L	G	Y	U	U	U	U	F	F	O	O	O	W	I	I	P	P	R	R	E	E	N
20	M	M	M	M	B	A	A	A	A	A	G	U	U	U	U	Y	O	W	W	W	S	S	I	R	R
21	P	P	P	V	M	E	E	E	E	V	A	A	A	A	A	V	Y	Y	Y	Y	T	V	S	S	S
22	W	W	X	X	P	I	I	I	X	X	E	E	E	E	X	X	L	L	L	L	X	X	T	T	T
23	Y	Z	Z	Z	W	O	O	Z	Z	Z	I	I	I	Z	Z	Z	M	M	M	Z	Z	Z	H	H	H
24	J	J	J	J	Y	U	J	J	J	J	O	O	J	J	J	J	P	P	J	J	J	J	N	N	J
25	K	K	K	K	L	K	K	K	K	K	U	K	K	K	K	K	W	K	K	K	K	K	R	K	K

SYNOPTIC TABLE OF THE LETTER

R

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	0
1	S	S	F	S	S	S	S	W	S	S	S	S	W	S	S	S	S	F	S	S	S	S	Q	S	S	1
2	T	G	G	T	T	T	Y	Y	T	T	T	Y	Y	T	T	T	G	G	T	T	T	V	V	T	T	2
3	B	B	B	H	H	L	L	L	H	H	L	L	L	H	H	B	B	B	H	H	X	X	X	H	H	3
4	C	C	C	N	C	M	M	M	N	M	M	M	M	N	M	C	C	C	N	C	Z	Z	Z	N	J	4
5	D	D	D	D	D	P	P	P	P	P	P	P	P	P	P	D	D	D	D	D	J	J	J	K	K	5
6	F	F	W	F	F	W	W	O	W	W	W	W	F	W	W	F	F	O	F	F	K	K	K	Q	Q	6
7	G	Y	Y	G	G	Y	U	U	Y	Y	Y	G	G	Y	Y	G	U	U	G	G	Q	Q	F	V	V	7
8	L	L	L	B	B	A	A	A	L	L	B	B	B	L	L	A	A	A	B	B	V	G	G	X	X	8
9	M	M	M	C	M	E	E	E	M	E	C	C	C	M	C	E	E	E	C	E	B	B	B	Z	Z	9
10	P	P	P	P	P	I	I	I	I	I	D	D	D	D	D	I	I	I	I	I	C	C	C	J	C	10
11	W	W	X	W	W	O	O	Z	O	O	F	F	O	F	F	O	O	W	O	O	D	D	D	D	D	11
12	Y	Z	Z	Y	Y	U	J	J	U	U	G	U	U	G	G	U	Y	Y	U	U	F	F	W	F	F	12
13	J	J	J	L	L	K	K	K	A	A	A	A	A	B	B	L	L	L	A	A	G	Y	Y	G	G	13
14	K	K	K	M	Q	Q	Q	Q	E	V	E	E	E	C	E	M	M	M	E	M	L	L	L	B	B	14
15	Q	Q	Q	V	V	V	V	V	X	X	I	I	I	I	I	P	P	P	P	P	M	M	M	C	M	15
16	V	V	V	X	X	X	X	X	Z	Z	O	O	J	O	O	W	W	K	W	W	P	P	P	P	P	16
17	X	X	O	Z	Z	Z	Z	F	J	J	U	K	K	U	U	Y	Q	Q	Y	Y	W	W	O	W	W	17
18	Z	U	U	J	J	J	G	G	K	K	Q	Q	Q	A	A	V	V	V	L	L	Y	U	U	Y	Y	18
19	A	A	A	K	K	B	B	B	Q	Q	V	V	V	E	X	X	X	X	M	Z	A	A	A	L	L	19
20	E	E	E	Q	E	C	C	C	V	C	X	X	X	Z	Z	Z	Z	Z	J	J	E	E	E	M	E	20
21	I	I	I	I	I	D	D	D	D	D	Z	Z	Z	J	J	J	J	J	K	K	I	I	I	I	I	21
22	O	O	S	O	O	F	F	S	F	F	J	J	S	K	K	K	K	S	Q	Q	O	O	S	O	O	22
23	U	T	T	U	U	G	T	T	G	G	K	T	T	Q	Q	Q	T	T	V	V	U	T	T	U	U	23
24	H	H	H	A	A	H	H	H	B	B	H	H	H	V	V	H	H	H	X	X	H	H	H	A	A	24
25	N	N	N	E	N	N	N	N	C	N	N	N	N	X	N	N	N	N	Z	N	N	N	N	E	N	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER

S

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
1	T	G	T	T	T	T	Y	T	T	T	T	Y	T	T	T	T	G	T	T	T	T	V	T	T	T
2	B	B	H	H	H	L	L	H	H	H	L	L	H	H	H	B	B	H	H	H	X	X	H	H	H
3	C	C	N	N	C	M	M	N	N	M	M	M	N	N	M	C	C	N	N	C	Z	Z	N	N	J
4	D	D	R	D	D	P	P	R	P	P	P	P	R	P	P	D	D	R	D	D	J	J	R	K	K
5	F	F	F	F	F	W	W	W	W	W	W	W	W	W	W	F	F	F	F	F	K	K	Q	Q	Q
6	G	Y	G	G	G	Y	U	Y	Y	Y	Y	G	Y	Y	Y	G	U	G	G	G	Q	Q	V	V	V
7	L	L	B	B	B	A	A	L	L	L	B	B	L	L	L	A	A	B	B	B	V	G	X	X	X
8	M	M	C	C	M	E	E	M	M	E	C	C	M	M	C	E	E	C	C	E	B	B	Z	Z	Z
9	P	P	D	P	P	I	I	P	I	I	D	D	P	D	D	I	I	D	I	I	C	C	J	J	C
10	W	W	W	W	W	O	O	O	O	O	F	F	F	F	F	O	O	O	O	O	D	D	K	D	D
11	Y	Z	Y	Y	Y	U	J	U	U	U	G	U	G	G	G	U	Y	U	U	U	F	F	F	F	F
12	J	J	L	L	L	K	K	A	A	A	A	A	B	B	B	L	L	A	A	A	G	Y	G	G	G
13	K	K	M	M	Q	Q	Q	E	E	V	E	E	C	C	E	M	M	E	E	M	L	L	B	B	B
14	Q	Q	P	V	V	V	V	I	X	X	I	I	D	I	I	P	P	I	P	P	M	M	C	C	M
15	V	V	X	X	X	X	X	Z	Z	Z	O	O	O	O	O	W	W	W	W	W	P	P	D	P	P
16	X	X	Z	Z	Z	Z	Z	J	J	J	U	K	U	U	U	Y	Q	Y	Y	Y	W	W	W	W	W
17	Z	U	J	J	J	J	G	K	K	K	Q	Q	A	A	A	V	V	L	L	L	Y	U	Y	Y	Y
18	A	A	K	K	K	B	B	Q	Q	Q	V	V	E	E	X	X	X	M	M	Z	A	A	L	L	L
19	E	E	Q	Q	E	C	C	V	V	C	X	X	I	Z	Z	Z	Z	P	J	J	E	E	M	M	E
20	I	I	V	I	I	D	D	X	D	D	Z	Z	J	J	J	J	J	K	K	K	I	I	P	I	I
21	O	O	O	O	O	F	F	F	F	F	J	J	K	K	K	K	K	Q	Q	Q	O	O	O	O	O
22	U	T	U	U	U	G	T	G	G	G	K	T	Q	Q	Q	Q	T	V	V	V	U	T	U	U	U
23	H	H	A	A	A	H	H	B	B	B	H	H	V	V	V	H	H	X	X	X	H	H	A	A	A
24	N	N	E	E	N	N	N	C	C	N	N	N	X	X	N	N	N	Z	Z	N	N	N	E	E	N
25	R	R	I	R	R	R	R	D	R	R	R	R	Z	R	R	R	R	J	R	R	R	R	I	R	R

SYNOPTIC TABLE OF THE LETTER
T

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	0
1	B	H	H	H	H	L	H	H	H	H	L	H	H	H	H	B	H	H	H	H	X	H	H	H	H	1
2	C	N	N	N	C	M	N	N	N	M	M	N	N	N	M	C	N	N	N	C	Z	N	N	N	J	2
3	D	R	R	D	D	P	R	R	P	P	P	R	R	P	P	D	R	R	D	D	J	R	R	K	K	3
4	F	S	F	F	F	W	S	W	W	W	W	S	W	W	W	F	S	F	F	F	K	S	Q	Q	Q	4
5	G	G	G	G	G	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	G	G	G	G	G	Q	V	V	V	V	5
6	L	B	B	B	B	A	L	L	L	L	B	L	L	L	L	A	B	B	B	B	V	X	X	X	X	6
7	M	C	C	C	M	E	M	M	M	E	C	M	M	M	C	E	C	C	C	E	B	Z	Z	Z	Z	7
8	P	D	D	P	P	I	P	P	I	I	D	P	P	D	D	I	D	D	I	I	C	J	J	J	C	8
9	W	F	W	W	W	O	W	O	O	O	F	W	F	F	F	O	F	O	O	O	D	K	K	D	D	9
10	Y	Y	Y	Y	Y	U	U	U	U	U	G	G	G	G	G	U	U	U	U	U	F	Q	F	F	F	10
11	J	L	L	L	L	K	A	A	A	A	A	B	B	B	B	L	A	A	A	A	G	G	G	G	G	11
12	K	M	M	M	Q	Q	E	E	E	V	E	C	C	C	E	M	E	E	E	M	L	B	B	B	B	12
13	Q	P	P	V	V	V	I	I	X	X	I	D	D	I	I	P	I	I	P	P	M	C	C	C	M	13
14	V	W	X	X	X	X	O	Z	Z	Z	O	F	O	O	O	W	O	W	W	W	P	D	D	P	P	14
15	X	Z	Z	Z	Z	Z	J	J	J	J	U	U	U	U	U	Y	Y	Y	Y	Y	W	F	W	W	W	15
16	Z	J	J	J	J	J	K	K	K	K	Q	A	A	A	A	V	L	L	L	L	Y	Y	Y	Y	Y	16
17	A	K	K	K	K	B	Q	Q	Q	Q	V	E	E	E	X	X	M	M	M	Z	A	L	L	L	L	17
18	E	Q	Q	Q	E	C	V	V	V	C	X	I	I	Z	Z	Z	P	P	J	J	E	M	M	M	E	18
19	I	V	V	I	I	D	X	X	D	D	Z	O	J	J	J	J	W	K	K	K	I	P	P	I	I	19
20	O	X	O	O	O	F	Z	F	F	F	J	K	K	K	K	K	Q	Q	Q	Q	O	W	O	O	O	20
21	U	U	U	U	U	G	G	G	G	G	K	Q	Q	Q	Q	Q	V	V	V	V	U	U	U	U	U	21
22	H	A	A	A	A	H	B	B	B	B	H	V	V	V	V	H	X	X	X	X	H	A	A	A	A	22
23	N	E	E	E	N	N	C	C	C	N	N	X	X	X	N	N	Z	Z	Z	N	N	E	E	E	N	23
24	R	I	I	R	R	R	D	D	R	R	R	Z	Z	R	R	R	J	J	R	R	R	I	I	R	R	24
25	S	O	S	S	S	S	F	S	S	S	S	J	S	S	S	S	K	S	S	S	S	O	S	S	S	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER U

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0
1	H	A	A	A	A	K	A	A	A	A	Q	A	A	A	A	L	A	A	A	A	H	A	A	A	A	1
2	N	E	E	E	N	Q	E	E	E	V	V	E	E	E	X	M	E	E	E	M	N	E	E	E	N	2
3	R	I	I	R	R	V	I	I	X	X	X	I	I	Z	Z	P	I	I	P	P	R	I	I	R	R	3
4	S	O	S	S	S	X	O	Z	Z	Z	Z	O	J	J	J	W	O	W	W	W	S	O	S	S	S	4
5	T	T	T	T	T	Z	J	J	J	J	J	K	K	K	K	Y	Y	Y	Y	Y	T	T	T	T	T	5
6	B	H	H	H	H	J	K	K	K	K	K	Q	Q	Q	Q	V	L	L	L	L	X	H	H	H	H	6
7	C	N	N	N	C	B	Q	Q	Q	Q	H	V	V	V	V	X	M	M	M	Z	Z	N	N	N	J	7
8	D	R	R	D	D	C	V	V	V	C	N	X	X	X	N	Z	P	P	J	J	J	R	R	K	K	8
9	F	S	F	F	F	D	X	X	D	D	R	Z	Z	R	R	J	W	K	K	K	K	S	Q	Q	Q	9
10	G	G	G	G	G	F	Z	F	F	F	S	J	S	S	S	K	Q	Q	Q	Q	Q	V	V	V	V	10
11	L	B	B	B	B	G	G	G	G	G	T	T	T	T	T	Q	V	V	V	V	V	X	X	X	X	11
12	M	C	C	C	M	H	B	B	B	B	L	H	H	H	H	H	X	X	X	X	B	Z	Z	Z	Z	12
13	P	D	D	P	P	N	C	C	C	N	M	N	N	N	M	N	Z	Z	Z	N	C	J	J	J	C	13
14	W	F	W	W	W	R	D	D	R	R	P	R	R	P	P	R	J	J	R	R	D	K	K	D	D	14
15	Y	Y	Y	Y	Y	S	F	S	S	S	W	S	W	W	W	S	K	S	S	S	F	Q	F	F	F	15
16	J	L	L	L	L	T	T	T	T	T	Y	Y	Y	Y	Y	T	T	T	T	T	G	G	G	G	G	16
17	K	M	M	M	Q	L	H	H	H	H	B	L	L	L	L	B	H	H	H	H	L	B	B	B	B	17
18	Q	P	P	V	V	M	N	N	N	M	C	M	M	M	C	C	N	N	N	C	M	C	C	C	M	18
19	V	W	X	X	X	P	R	R	P	P	D	P	P	D	D	D	R	R	D	D	P	D	D	P	P	19
20	X	Z	Z	Z	Z	W	S	W	W	W	F	W	F	F	F	F	S	F	F	F	W	F	W	W	W	20
21	Z	J	J	J	J	Y	Y	Y	Y	Y	G	G	G	G	G	G	G	G	G	G	Y	Y	Y	Y	Y	21
22	A	K	K	K	K	A	L	L	L	L	A	B	B	B	B	A	B	B	B	B	A	L	L	L	L	22
23	E	Q	Q	Q	E	E	M	M	M	E	E	C	C	C	E	E	C	C	C	E	E	M	M	M	E	23
24	I	V	V	I	I	I	P	P	I	I	I	D	D	I	I	I	D	D	I	I	I	P	P	I	I	24
25	O	X	O	O	O	O	W	O	O	O	O	F	O	O	O	O	F	O	O	O	O	W	O	O	O	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER
V

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	0
1	X	X	O	X	X	X	X	X	D	X	X	X	X	X	N	X	X	X	X	X	B	X	X	X	X	1
2	Z	U	U	Z	Z	Z	Z	F	F	Z	Z	Z	Z	R	R	Z	Z	Z	Z	N	C	Z	Z	Z	Z	2
3	A	A	A	J	J	J	G	G	G	J	J	J	S	S	S	J	J	J	R	R	D	J	J	J	C	3
4	E	E	E	K	K	B	B	B	B	K	K	T	T	T	T	K	K	S	S	S	F	K	K	D	D	4
5	I	I	I	Q	E	C	C	C	C	Q	H	H	H	H	H	Q	T	T	T	T	G	Q	F	F	F	5
6	O	O	S	I	I	D	D	D	R	C	N	N	N	N	M	H	H	H	H	H	L	G	G	G	G	6
7	U	T	T	O	O	F	F	S	S	D	R	R	R	P	P	N	N	N	N	C	M	B	B	B	B	7
8	H	H	H	U	U	G	T	T	T	F	S	S	W	W	W	R	R	R	D	D	P	C	C	C	M	8
9	N	N	N	A	A	H	H	H	H	G	T	Y	Y	Y	Y	S	S	F	F	F	W	D	D	P	P	9
10	R	R	R	E	N	N	N	N	N	B	L	L	L	L	L	T	G	G	G	G	Y	F	W	W	W	10
11	S	S	F	R	R	R	R	R	P	N	M	M	M	M	C	B	B	B	B	B	A	Y	Y	Y	Y	11
12	T	G	G	S	S	S	S	W	W	R	P	P	P	D	D	C	C	C	C	E	E	L	L	L	L	12
13	B	B	B	T	T	T	Y	Y	Y	S	W	W	F	F	F	D	D	D	I	I	I	M	M	M	E	13
14	C	C	C	H	H	L	L	L	L	T	Y	G	G	G	G	F	F	O	O	O	O	P	P	I	I	14
15	D	D	D	N	C	M	M	M	M	H	B	B	B	B	B	G	U	U	U	U	U	W	O	O	O	15
16	F	F	W	D	D	P	P	P	I	M	C	C	C	C	E	A	A	A	A	A	H	U	U	U	U	16
17	G	Y	Y	F	F	W	W	O	O	P	D	D	D	I	I	E	E	E	E	M	N	A	A	A	A	17
18	L	L	L	G	G	Y	U	U	U	W	F	F	O	O	O	I	I	I	P	P	R	E	E	E	N	18
19	M	M	M	B	B	A	A	A	A	Y	G	U	U	U	U	O	O	W	W	W	S	I	I	R	R	19
20	P	P	P	C	M	E	E	E	E	L	A	A	A	A	A	U	Y	Y	Y	Y	T	O	S	S	S	20
21	W	W	X	P	P	I	I	I	X	E	E	E	E	E	X	L	L	L	L	L	X	T	T	T	T	21
22	Y	Z	Z	W	W	O	O	Z	Z	I	I	I	I	Z	Z	M	M	M	M	Z	Z	H	H	H	H	22
23	J	J	J	Y	Y	U	J	J	J	O	O	O	J	J	J	P	P	P	J	J	J	N	N	N	J	23
24	K	K	K	L	L	K	K	K	K	U	U	K	K	K	K	W	W	K	K	K	K	R	R	K	K	24
25	Q	Q	Q	M	Q	Q	Q	Q	Q	A	Q	Q	Q	Q	Q	Y	Q	Q	Q	Q	Q	S	Q	Q	Q	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

U V W X Y Z

SYNOPTIC TABLE OF THE LETTER
W

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	W	0
1	Y	Z	Y	Y	Y	Y	U	Y	Y	Y	Y	G	Y	Y	Y	Y	Q	Y	Y	Y	Y	U	Y	Y	Y	1
2	J	J	L	L	L	A	A	L	L	L	B	B	L	L	L	V	V	L	L	L	A	A	L	L	L	2
3	K	K	M	M	Q	E	E	M	M	E	C	C	M	M	C	X	X	M	M	Z	E	E	M	M	E	3
4	Q	Q	P	V	V	I	I	P	I	I	D	D	P	D	D	Z	Z	P	J	J	I	I	P	I	I	4
5	V	V	X	X	X	O	O	O	O	O	F	F	F	F	F	J	J	K	K	K	O	O	O	O	O	5
6	X	X	Z	Z	Z	U	J	U	U	U	G	U	G	G	G	K	K	Q	Q	Q	U	T	U	U	U	6
7	Z	U	J	J	J	K	K	A	A	A	A	A	B	B	B	Q	T	V	V	V	H	H	A	A	A	7
8	A	A	K	K	K	Q	Q	E	E	V	E	E	C	C	E	H	H	X	X	X	N	N	E	E	N	8
9	E	E	Q	Q	E	V	V	I	X	X	I	I	D	I	I	N	N	Z	Z	N	R	R	I	R	R	9
10	I	I	V	I	I	X	X	Z	Z	Z	O	O	O	O	O	R	R	J	R	R	S	S	S	S	S	10
11	O	O	O	O	O	Z	Z	J	J	J	U	K	U	U	U	S	S	S	S	S	T	V	T	T	T	11
12	U	T	U	U	U	J	G	K	K	K	Q	Q	A	A	A	T	G	T	T	T	X	X	H	H	H	12
13	H	H	A	A	A	B	B	Q	Q	Q	V	V	E	E	X	B	B	H	H	H	Z	Z	N	N	J	13
14	N	N	E	E	N	C	C	V	V	C	X	X	I	Z	Z	C	C	N	N	C	J	J	R	K	K	14
15	R	R	I	R	R	D	D	X	D	D	Z	Z	J	J	J	D	D	R	D	D	K	K	Q	Q	Q	15
16	S	S	S	S	S	F	F	F	F	F	J	J	K	K	K	F	F	F	F	F	Q	Q	V	V	V	16
17	T	G	T	T	T	G	T	G	G	G	K	T	Q	Q	Q	G	U	G	G	G	V	G	X	X	X	17
18	B	B	H	H	H	H	H	B	B	B	H	H	V	V	V	A	A	B	B	B	B	B	Z	Z	Z	18
19	C	C	N	N	C	N	N	C	C	N	N	N	X	X	N	E	E	C	C	E	C	C	J	J	C	19
20	D	D	R	D	D	R	R	D	R	R	R	R	Z	R	R	I	I	D	I	I	D	D	K	D	D	20
21	F	F	F	F	F	S	S	S	S	S	S	S	S	S	S	O	O	O	O	O	F	F	F	F	F	21
22	G	Y	G	G	G	T	Y	T	T	T	T	Y	T	T	T	U	Y	U	U	U	G	Y	G	G	G	22
23	L	L	B	B	B	L	L	H	H	H	L	L	H	H	H	L	L	A	A	A	L	L	B	B	B	23
24	M	M	C	C	M	M	M	N	N	M	M	M	N	N	M	M	M	E	E	M	M	M	C	C	M	24
25	P	P	D	P	P	P	P	R	P	P	P	P	R	P	P	P	P	I	P	P	P	P	D	P	P	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

SYNOPTIC TABLE OF THE LETTER
X

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	0
1	Z	U	Z	Z	Z	Z	Z	F	Z	Z	Z	Z	Z	R	Z	Z	Z	Z	Z	N	Z	Z	Z	Z	Z	1
2	A	A	J	J	J	J	G	G	J	J	J	J	S	S	J	J	J	J	R	R	J	J	J	J	C	2
3	E	E	K	K	K	B	B	B	K	K	K	T	T	T	K	K	K	S	S	S	K	K	K	D	D	3
4	I	I	Q	Q	E	C	C	C	Q	Q	H	H	H	H	Q	Q	T	T	T	T	Q	Q	F	F	F	4
5	O	O	V	I	I	D	D	D	V	C	N	N	N	N	V	H	H	H	H	H	V	G	G	G	G	5
6	U	T	O	O	O	F	F	S	D	D	R	R	R	P	N	N	N	N	N	C	B	B	B	B	B	6
7	H	H	U	U	U	G	T	T	F	F	S	S	W	W	R	R	R	R	D	D	C	C	C	C	M	7
8	N	N	A	A	A	H	H	H	G	G	T	Y	Y	Y	S	S	S	F	F	F	D	D	D	P	P	8
9	R	R	E	E	N	N	N	N	B	B	L	L	L	L	T	T	G	G	G	G	F	F	W	W	W	9
10	S	S	I	R	R	R	R	R	C	N	M	M	M	M	H	B	B	B	B	B	G	Y	Y	Y	Y	10
11	T	G	S	S	S	S	S	W	R	R	P	P	P	D	M	C	C	C	C	E	L	L	L	L	L	11
12	B	B	T	T	T	T	Y	Y	S	S	W	W	F	F	P	D	D	D	I	I	M	M	M	M	E	12
13	C	C	H	H	H	L	L	L	T	T	Y	G	G	G	W	F	F	O	O	O	P	P	P	I	I	13
14	D	D	N	N	C	M	M	M	H	H	B	B	B	B	Y	G	U	U	U	U	W	W	O	O	O	14
15	F	F	R	D	D	P	P	P	N	M	C	C	C	C	L	A	A	A	A	A	Y	U	U	U	U	15
16	G	Y	F	F	F	W	W	O	P	P	D	D	D	I	C	E	E	E	E	M	A	A	A	A	A	16
17	L	L	G	G	G	Y	U	U	W	W	F	F	O	O	D	I	I	I	P	P	E	E	E	E	N	17
18	M	M	B	B	B	A	A	A	Y	Y	G	U	U	U	F	O	O	W	W	W	I	I	I	R	R	18
19	P	P	C	C	M	E	E	E	L	L	A	A	A	A	G	U	Y	Y	Y	Y	O	O	S	S	S	19
20	W	W	D	P	P	I	I	I	M	E	E	E	E	E	B	L	L	L	L	L	U	T	T	T	T	20
21	Y	Z	W	W	W	O	O	Z	I	I	I	I	I	Z	E	M	M	M	M	Z	H	H	H	H	H	21
22	J	J	Y	Y	Y	U	J	J	O	O	O	O	J	J	I	P	P	P	J	J	N	N	N	N	J	22
23	K	K	L	L	L	K	K	K	U	U	U	K	K	K	O	W	W	K	K	K	R	R	R	K	K	23
24	Q	Q	M	M	Q	Q	Q	Q	A	A	Q	Q	Q	Q	U	Y	Q	Q	Q	Q	S	S	Q	Q	Q	24
25	V	V	P	V	V	V	V	V	E	V	V	V	V	V	A	V	V	V	V	V	T	V	V	V	V	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

SYNOPTIC TABLE OF THE LETTER
Y

ALPHABET

GENERATRIX	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	GENERATRIX
0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	0
1	J	L	L	L	L	A	L	L	L	L	B	L	L	L	L	V	L	L	L	L	A	L	L	L	L	1
2	K	M	M	M	Q	E	M	M	M	E	C	M	M	M	C	X	M	M	M	Z	E	M	M	M	E	2
3	Q	P	P	V	V	I	P	P	I	I	D	P	P	D	D	Z	P	P	J	J	I	P	P	I	I	3
4	V	W	X	X	X	O	W	O	O	O	F	W	F	F	F	J	W	K	K	K	O	W	O	O	O	4
5	X	Z	Z	Z	Z	U	U	U	U	U	G	G	G	G	G	K	Q	Q	Q	Q	U	U	U	U	U	5
6	Z	J	J	J	J	K	A	A	A	A	A	B	B	B	V	Q	V	V	V	V	H	A	A	A	A	6
7	A	K	K	K	K	Q	E	E	E	V	E	C	C	C	E	H	X	X	X	X	N	E	E	E	N	7
8	E	Q	Q	Q	E	V	I	I	X	X	I	D	D	I	I	N	Z	Z	Z	N	R	I	I	R	R	8
9	I	V	V	I	I	X	O	Z	Z	Z	O	F	O	O	O	R	J	J	R	R	S	O	S	S	S	9
10	O	X	O	O	O	Z	J	J	J	J	U	U	U	U	U	S	K	S	S	S	T	T	T	T	T	10
11	U	U	U	U	U	J	K	K	K	K	Q	A	A	A	A	T	T	T	T	T	X	H	H	H	H	11
12	H	A	A	A	A	B	Q	Q	Q	Q	V	E	E	E	X	B	H	H	H	H	Z	N	N	N	J	12
13	N	E	E	E	N	C	V	V	V	C	X	I	I	Z	Z	C	N	N	N	C	J	R	R	K	K	13
14	R	I	I	R	R	D	X	X	D	D	Z	O	J	J	J	D	R	R	D	D	K	S	Q	Q	Q	14
15	S	O	S	S	S	F	Z	F	F	F	J	K	K	K	K	F	S	F	F	F	Q	V	V	V	V	15
16	T	T	T	T	T	G	G	G	G	G	K	Q	Q	Q	Q	G	G	G	G	G	V	X	X	X	X	16
17	B	H	H	H	H	H	B	B	B	B	H	V	V	V	V	A	B	B	B	B	B	Z	Z	Z	Z	17
18	C	N	N	N	C	N	C	C	C	N	N	X	X	X	N	E	C	C	C	E	C	J	J	J	C	18
19	D	R	R	D	D	R	D	D	R	R	R	Z	Z	R	R	I	D	D	I	I	D	K	K	D	D	19
20	F	S	F	F	F	S	F	S	S	S	S	J	S	S	S	O	F	O	O	O	F	Q	F	F	F	20
21	G	G	G	G	G	T	T	T	T	T	T	T	T	T	T	U	U	U	U	U	G	G	G	G	G	21
22	L	B	B	B	B	L	H	H	H	H	L	H	H	H	H	L	A	A	A	A	L	B	B	B	B	22
23	M	C	C	C	M	M	N	N	N	M	M	N	N	N	M	M	E	E	E	M	M	C	C	C	M	23
24	P	D	D	P	P	P	R	R	P	P	P	R	R	P	P	P	I	I	P	P	P	D	D	P	P	24
25	W	F	W	W	W	W	S	W	W	W	W	S	W	W	W	W	O	W	W	W	W	F	W	W	W	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

ALPHABET

SYNOPTIC TABLE OF THE LETTER
Z

ALPHABET

GENERATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	0
1	A	J	J	J	J	J	G	J	J	J	J	J	S	J	J	J	J	J	R	J	J	J	J	J	C	1
2	E	K	K	K	K	B	B	K	K	K	K	T	T	K	K	K	K	S	S	K	K	K	K	D	D	2
3	I	Q	Q	Q	E	C	C	Q	Q	Q	H	H	H	Q	Q	Q	T	T	T	Q	Q	Q	F	F	F	3
4	O	V	V	I	I	D	D	V	V	C	N	N	N	V	V	H	H	H	H	V	V	G	G	G	G	4
5	U	X	O	O	O	F	F	X	D	D	R	R	R	X	N	N	N	N	N	X	B	B	B	B	B	5
6	H	U	U	U	U	G	T	F	F	F	S	S	W	R	R	R	R	R	D	N	C	C	C	C	M	6
7	N	A	A	A	A	H	H	G	G	G	T	Y	Y	S	S	S	S	F	F	R	D	D	D	P	P	7
8	R	E	E	E	N	N	N	B	B	B	L	L	L	T	T	T	G	G	G	S	F	F	W	W	W	8
9	S	I	I	R	R	R	R	C	C	N	M	M	M	H	H	B	B	B	B	T	G	Y	Y	Y	Y	9
10	T	O	S	S	S	S	S	D	R	R	P	P	P	N	M	C	C	C	C	H	L	L	L	L	L	10
11	B	T	T	T	T	T	Y	S	S	S	W	W	F	P	P	D	D	D	I	C	M	M	M	M	E	11
12	C	H	H	H	H	L	L	T	T	T	Y	G	G	W	W	F	F	O	O	D	P	P	P	I	I	12
13	D	N	N	N	C	M	M	H	H	H	B	B	B	Y	Y	G	U	U	U	F	W	W	O	O	O	13
14	F	R	R	D	D	P	P	N	N	M	C	C	C	L	L	A	A	A	A	G	Y	U	U	U	U	14
15	G	S	F	F	F	W	W	R	P	P	D	D	D	M	C	E	E	E	E	B	A	A	A	A	A	15
16	L	G	G	G	G	Y	U	W	W	W	F	F	O	D	D	I	I	I	P	E	E	E	E	E	N	16
17	M	B	B	B	B	A	A	Y	Y	Y	G	U	U	F	F	O	O	W	W	I	I	I	I	R	R	17
18	P	C	C	C	M	E	E	L	L	L	A	A	A	G	G	U	Y	Y	Y	O	O	O	S	S	S	18
19	W	D	D	P	P	I	I	M	M	E	E	E	E	B	B	L	L	L	L	U	U	T	T	T	T	19
20	Y	F	W	W	W	O	O	P	I	I	I	I	I	C	E	M	M	M	M	A	H	H	H	H	H	20
21	J	Y	Y	Y	Y	U	J	O	O	O	O	O	J	I	I	P	P	P	J	M	N	N	N	N	J	21
22	K	L	L	L	L	K	K	U	U	U	U	K	K	O	O	W	W	K	K	P	R	R	R	K	K	22
23	Q	M	M	M	Q	Q	Q	A	A	A	Q	Q	Q	U	U	Y	Q	Q	Q	W	S	S	Q	Q	Q	23
24	V	P	P	V	V	V	V	E	E	V	V	V	V	A	A	V	V	V	V	Y	T	V	V	V	V	24
25	X	W	X	X	X	X	X	I	X	X	X	X	X	E	X	X	X	X	X	L	X	X	X	X	X	25
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

GENERATRIX

ALPHABET

Methods for the Reconstruction

of

Primary Alphabets

Publication No. 21

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Two Hundred copies of this publication were printed of which this is

No. 64

RIVERBANK
LABORATORIES
GENEVA
ILLINOIS

INTRODUCTORY NOTE

It is not our intention in this brochure to describe any newly-discovered methods of cipher solution, or indeed, to make a detailed analysis of even any one system. We do not claim any remarkable achievement in putting forth the few principles herein described. They are meant rather as a stimulant to the more advanced student of deciphering. Therefore no attempt has been made to make any exhaustive analysis of different systems, or of varying methods of using the same system. The methods here given are issued primarily as an outline or suggestion to the cipher student who is more or less familiar with complicated systems, and who therefore will be quick to see the application of the present principles to any variations of known methods. For him who wishes to go farther into the subject, these suggestions will be found to yield a wealth of possibilities for research, which would need volumes to describe.

KEY-WORD ALPHABETS

In Riverbank Publication No. 15 a method was shown for reconstructing a Primary Alphabet from any one of the Secondary Alphabets. In that monograph only Key-Word Alphabets were considered. It is our purpose in this pamphlet to deal not only with Key-Word Alphabets, but with Arbitrarily—and Random-mixed Alphabets as well.

Let us consider the first of the examples at the end of Publication 15. We are given the deciphering alphabet:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Q M T A Z S C U X L I W P Y N E B D R F V G H J K O

You will note that X Y of the upper alphabet represents J K of the lower. Each being a group of two infrequent consonants, we shall assume as a starting point that the letters constituting the two pairs are sequent in the Primary Alphabet. Then, taking the values by twos as they result from the preceding groups, we should have, with X Y equalling J K, J K equalling L I and so on:

X Y
J K
L I
W X
H J
U L
V W
G H
C U
T V
F G
S C
R T
D F
A S
Q R
B D
M A
P Q
E B
Z M
O P
N E
Y Z
K O
I N
X Y

Having reached the starting point, we conclude this part of the operation and begin to build the alphabet proper from the pairs thus obtained. Beginning with the first pair, X Y, which has Y for its second letter, we follow it with that pair which has Y for its first letter, which is Y Z; then Y Z is followed by that group which has Z for its first letter, which is Z M. This process is continued until all the pairs have been used. Thus:

X Y Z M A S C U L I N E B D F G H J K O P Q R T V W X

The reconstruction of the Primary Alphabet from a single secondary alphabet, as in the foregoing example, is possible only where the system from which the deciphering or secondary alphabet came is a Primary Alphabet System in which the two components are identical. (See Riverbank Publication No. 18, Table V, 4a.) It is possible, of course, to have a Primary Alphabet System in which the components are not identical, in which case it is impossible to recover the Primary Alphabets from a single one of the secondaries.

1)	V W	S T	(1
	P H	E Y	
	D F	B C	
	N O	L M	
3)	X Y	U V	(3
	B E	W O	
	G I	F G	
	Q R	N P	
5)	Z A	X Z	(5
	T S	R D	
	J K	H I	
	U V	Q S	
	L P	K E	
	C D	A B	
	M N	J L	
2)	W X	T U	(2
	H B	Y W	
	F G	C F	
	O Q	M N	
4)	Y Z	V X	(4
	E T	O R	
	I J	G H	
	R U	P Q	
6)	A L	Z K	(6
	S C	D A	
	K M	I J	
	V W		

However, with the preceding method in mind, let us consider a case in which we shall deal with two deciphering or secondary alphabets.

```
  I  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 II  Z W A B O C F Y G H I K J L M E N P D R Q S T U V X
III  P U K E V Y W T O R D Q A B C S F G Z X H I J L M N
```

In the preceding example twenty-six pairs resulted. In this example it will be found that fifty-two pairs will result.

Choosing a pair of sequent letters in Alphabet I, follow it by its equivalent pair in Alphabet II; then finding the second pair in Alphabet III, which letters are not recorded, take their equivalents in Alphabet I. Repeat this cycle until the starting point is reached.

Here the alternate groups have been placed to the right, forming two columns of pairs. It will be found that the pairs in the left column comprise the letters of one Primary Alphabet, those on the right the other Primary Alphabet. As when dealing with a single alphabet, take as a starting point any group and follow it by the pair which has for its second letter that which was the first in the former pair. The column on the left, then, will unite in this manner:

```
1 2 3 4 5 6, etc.
VWXYZALPHBETSCDFGIJKMNOQRU
```

The right column forms the remaining Primary Alphabet, taking its pairs in the same order and positions.

```
1 2 3 4 5 6, etc.
STUVXZKEYWORDABCFGHIJLMNPQ
```

Having recovered the Primary Alphabets, whose key words are KEYWORDALPH(A)BETS, it is ascertained that the secondary alphabets used in their reconstruction were the second and ninth deciphering alphabets—that is, of the twenty-six possible deciphering alphabets to be used, one even-numbered and one odd-numbered alphabet brought the results shown. If two even-numbered or two odd-numbered alphabets had been taken, the cycle would have been concluded with twenty-six pairs instead of fifty-two. Let us note the results when two odd-numbered alphabets are used. The following are the first and seventeenth deciphering alphabets:

```
  I  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 II  K O B C R F G W H I J E L M N Y P Q A D S T U V X Z
III  F J P Q L S T I U V X G Z K E H Y W N M O R D A B C
```

```
V W
      T U
G I
      G H
L P
      E Y
O Q
      N P
S C
      A B
X Y
      V X
J K
      I J
H B
      W O
R U
      Q S
D F
      C F
Z A
      Z K
M N
      L M
E T
      R D
V W
```

Here the cycle is completed after twenty-six pairs. Hence it is not possible, as in the preceding example, to follow pair by pair with the last and first letters of the succeeding groups comprising the indicators. But nevertheless, when dealing with Key-word Alphabets, it is a fairly simple matter to build the Primary Alphabet. In this case, for instance, starting with V W in the left column, one would naturally look for a pair to follow it, the letters of which would most likely be found at the end of the alphabet, such as X Y, X Z, or Y Z. Following down the left column, the fifth pair from V W is seen to be X Y. Searching then for a Z, which would very probably follow Y, it is seen to be the first letter of the fifth group from X Y. This gives a clue, and it is found that by taking every fifth pair the Primary Alphabet is completed. Exactly as before, the other Primary Alphabet will result from the column on the right, by taking pairs in the same order—namely every fifth group.

Now it is rarely, if ever, possible to tell with which of the deciphering alphabets one is dealing, until the Primary Alphabets are known. Hence, the secondary alphabets being derived from messages deciphered, it may happen that the first two tried would not at once yield results. Another trial should be made, in such a case, with a different pair of alphabets. Any two alphabets whose interval is 13, such as alphabets 9 and 22, 2 and 15, and the like, will be found incapable of yielding to the foregoing method of reconstruction. However, this contingent need hardly be considered, for it would be a rare case indeed where not more than two alphabets could be found whose interval was other than 13.

ARBITRARILY-MIXED ALPHABETS

We shall first discuss the reconstruction of a single arbitrarily-mixed alphabet, i. e., a Primary Alphabet System where the components are identical. By an arbitrarily-mixed alphabet, is meant one which is made up according to some pre-arranged plan, and yet which presents the appearance of being mixed at random*.

*See Riverbank Publication No. 17, pages 22 and 23; also Gioppi, *La Crittografia*, page 54, and De Viaris, *L'Art de Dechiffrer*, page 126.

Such an alphabet would be, for example, using the key word DEMOCRA(C)Y :

```
3 4 5 6 2 7 1 8
D E M O C R A Y
B F G H I J K L
N P Q S T U V W
X Z
```

AKVCITDBNXEFPZMGQOHSRJUYLW

Or taking the columns after the manner of an alternate vertical transposition cipher:

DBNXZPFEMGQSHOCITUJRAKVWLY.

Once aware of any such system of forming an alphabet, it is comparatively easy to rebuild the generating rectangle. Take, for instance, the first of the two alphabets above. It is advisable here, as with key-word alphabets, to make the attack upon the XYZ part of the alphabet. Note here that X and Z are found four intervals apart, and that the third letters preceding are D and E respectively, themselves four intervals apart. This would lead one to place them in a possible rectangle thus:

```
D E
B F
N P
X Z
```

If this is correct, it at once shows that DE is a part of the key word, and that C, O, and Y are also in the key word. Returning to the alphabet, we look for Q, R, or S to follow P, as this seems to be the simplest method of procedure. The three letters after Z in the alphabet are MGQ, which, if they are made the adjoining column on the right, will bring G and Q in their correct alphabetical sequence. Following MGQ one finds OHS which will place H after G, and S after Q, signifying that R is in the key word. Now we have

```
D E M O
B F G H
N P Q S
X Z
```

At once we guess that the key word is DEMOCRACY or DEMOCRATIC, and a trial quickly proves the former.

In the second alphabet derived from this rectangle, or any alphabet of the same nature, the juxtaposition of such letters as X Z, Q S, T U, and V W, should reveal at once the alternate vertical method of transposition.

To proceed, then, let us take the following deciphering alphabet, derived from a Primary Alphabet System in which the two components are identical.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
N S U F A B H C P E D O G R J W T Y X K I M L Z Q V

In the case of an Arbitrarily-Mixed Alphabet, the method of formation precludes the possibility of dealing directly with pairs of letters. But let us begin with any letter in the direct alphabet, and form a sequence, such as A – N – R – Y, etc. By writing this sequence of equivalents on two strips of cross-section paper, it is made a simple matter to shift the strips until the correct pairs are found. With the sequence started above written on two strips and set in the first possible position, that is, shifted one space from identity of equivalents, they appear thus:

```
A N R Y Q T K D F B S X Z V M G H C U I P W L O J E A
  A N R Y Q T K D F B S X Z V M G H C U I P W L O J E
```

Now if this is the correct position, we should be able to obtain from here a sequence of equivalents which will build into a generating rectangle. Beginning then, we have N A E J O L W P I U C, etc., which from an inspection for symmetry in a possible rectangle, seems very improbable. Hence we try the next position. Here we get R A J L P U H M Z S F, etc., which is likewise unpromising. Of course, it is not always necessary to record the sequence of equivalents resulting from any position. Usually a simple, rapid inspection will reveal the possibilities of construction.

Finally we have the strips in this position:

```
A N R Y Q T K D F B S X Z V M G H C U I P W L O J E A N R Y Q T K D F B S
                      A N R Y Q T K D F B S X Z V M G H C U I P W L O J E
```

Here the resulting sequence is X A G Q I F O Z N H T P B J V R C K W S E M Y U D L X. Immediately it becomes apparent that V, W, Y, and X are four intervals apart. If we assume, then, that these are the final letters in columns of four letters each, we have:

```
P R U S
B C D E
J K L M
V W X Y
```

Searching for Z, we find that the letters preceding it adjoin those above in alphabetical sequence, and also indicate that N is in the key word. Thus:

```
P R U S I
B C D E F
J K L M O
V W X Y Z
```

Now looking for G which may follow F, we find A G Q, which is checked for the succeeding position on the right by having Q follow O, since P has already been placed in the key word. Similarly N H T checks as the remaining column, with H to succeed G, and T following Q, and R and S placed in the first line of the rectangle. The rectangle is now complete, the key word being P R U S(S)I A N .

```
4 5 7 6 2 1 3
P R U S I A N
B C D E F G H
J K L M O Q T
V W X Y Z
```

In a Primary Alphabet System where the components are not identical, not one, but two alphabets are to be reconstructed. As was shown in the case of Key-Word Alphabets, it will be found that the number of letters in the sequence of equivalents resulting from any two deciphering alphabets will vary—when two even-numbered or two odd-numbered alphabets are used, the sequence will end with 26 letters; when one even- and one odd-numbered alphabet are used, the sequence will yield 52 letters. But whereas in the case of Key-Word Alphabets it was comparatively easy to recover the Primary Alphabet with only 26 pairs, it is a much more difficult matter here. Therefore it is always best, if the first two alphabets tried result in only a 26-letter sequence, to discard them and try others until a sequence of 52 letters is procured.

Here are two deciphering alphabets, derived presumably from such a system:

```
  I  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 II  D X E Q W S C U N V B H M A G P F O Y K I R Z J T L
III  Z I T N H B D X F E G A Y Q K C J S V P M U L O W R
```

Beginning with A of Alphabet I, follow it by its equivalent D in Alphabet II, then finding D in Alphabet III take its equivalent in Alphabet I, which is G; follow G by C in Alphabet II, and continue the cycle until the starting point is reached. This process is the same as that with Key-Word Alphabets, except that here one can deal with only single letters and not with pairs. The sequence of equivalents should be written, as for a single alphabet, on strips of cross-section paper, which may be shifted at will.

a	A		
	D		
a	G		
	C		
a	P		
	P		
a	T		
	K		
a	O		
	G		
a	K		
	B		
a	F		
	S		
a	R	A	
	O	D	b
a	X	G	
	J	C	b
a	Q	P	
	F	P	b
a	I	T	
	N	K	b
a	D	O	
	Q	G	b
a	N	K	
	A	B	b
a	L	F	
	H	S	b
a	E	R	
	W	O	b
a	Y	X	
	T	J	b
a	C	Q	
	E	F	b
a	J	I	
	V	N	b
a	S	D	
	Y	Q	b
a	M	N	
	M	A	b
a	U	L	
	I	H	b
a	B	E	
	X	W	b
a	H	Y	
	U	T	b
a	V	C	
	R	E	b
a	Z	J	
	L	V	b
a	W	S	

In the present case, since two alphabets will result from the sequence, we designate the first, third, fifth, etc., letters as *a*, and they will constitute one Primary Alphabet, and the remaining, or *b* letters, will be found to comprise the other Primary Alphabet. In shifting the strips to find the sequence of pairs from which the generating rectangle may be built, *a* letters must be paired with *a* letters, and *b*'s with *b*'s.

Having shifted the strips space by space, making a careful trial each time for the generating rectangle, we soon have the strips in the position here shown. As a result from the *a* letters, we have the sequence RAMNKZJITHYXGULFWSDOVCQPBER. The juxtaposition of such letters as MN, YX, and QP, seem to indicate the alternate vertical form of transposition. But upon trying to place the first few letters in the columns of a rectangle, it is seen that RAM and NKZJ certainly cannot be adjacent columns; letting them rest for the moment, then, we pass on to the letters preceding and following YX. Placing these in columns so as to alphabetize X and Y, we have:

```
U T
G H
X Y
```

Now if we go to Z and take the adjacent letters, the next column on the right will be ZKN or ZJI. The former is very unlikely, for it would signify that both J and I are in the key word, which is not probable; but if ZJI is made the next column of letters, it will bring J in the position following H, and I in the key word. Then we note that by placing W in its natural position before X, we also have F before G, and L in the key. We now have:

```
L U T I
F G H J
W X Y Z
```

From this point on, it is a very simple matter to build the remaining part of the rectangle, by seeking to fit alphabetical sequences together. The key word is found to be REVOLUTI(O)N :

```
R E V O L U T I N
A B C D F G H J K
M P Q S W X Y Z
```

```
   Z Y  b
a  A M
   D M  b
a  G U
   C I  b
a  P B
   P X  b
a  T H
   K U  b
a  O V
   G R  b
a  K Z
   B L  b
a  F W
   S Z  b
a  R A
```

Now without moving the strips, the sequence of *b* letters is O D M A B L V N K U T J C I H S Z Y Q G R E F P X W O . By the same process as before the generating rectangle is quickly recovered, and the key word is found to be A M E R I C(A)N .

Being now in possession of the Primary Alphabets, it is ascertained that the deciphering alphabets used in this instance were the fifth and sixteenth, with AMERICAN the key word for the outer or text alphabet, and REVOLUTION for the inner or cipher alphabet. In other words, to have a sequence of 52 equivalents the interval between the two deciphering alphabets must be odd. If the interval is even, as for instance, if the deciphering alphabets were the fourth and tenth, or the fifth and thirteenth, the sequence would yield 26 letters only, as stated before. It is not impossible to build the generating rectangles and Primary Alphabets from a sequence of 26, but it is a process which takes time and patience.

Let us examine the long sequence on page 10 and above. Note that A M is found 28 places removed from R A, M N 28 places from A M, etc. In other words, there is always a symmetry of position, or definite interval, between pairs; and once the number of places between succeeding pairs is ascertained, the alphabet may then be built mathematically. Therefore, if in any given case it should be found impossible to discover two deciphering alphabets which will result in a sequence of 52 letters, the Primary Alphabets may be obtained from the sequence of 26 letters, if a series of 25 tests is made for each possible position of the strips—that is, with the strips set for the first possible position, the pairs at first one, then two, then three intervals, and on to twenty-five, are tested for the generating rectangle. This necessitates approximately 25 x 25 trials; hence it is advisable to use alphabets which will yield the 52-letter sequence, if possible.

In the foregoing paragraphs we have dealt with only one form of Arbitrarily-Mixed Alphabet, namely, that in which the system of formation was a key word generating rectangle. There are, of course, many methods by which an alphabet may be built up, but whatever the method, its very use will enable it in most cases to be discovered.

RANDOM-MIXED ALPHABETS

a	T	A	
	J	R	b
a	B	O	
	U	P	b
a	M	C	
	G	T	b
a	H	E	
	S	B	b
a	X	N	
	K	M	b
a	V	W	
	Y	H	b
a	Z	I	
	D	X	b
a	J	R	
	L	V	b
a	U	P	
	F	Z	b
a	G	T	
	Q	J	b
a	S	B	
	A	U	b
a	K	M	
	O	G	b
a	Y	H	
	C	S	b
a	D	X	
	E	K	b
a	L	V	
	N	Y	b
a	F	Z	
	W	D	b
a	Q	J	
	I	L	b
a	A	U	
	R	F	b
a	O	G	
	P	Q	b
a	C	S	
	T	A	b
a	E	K	
	B	O	b
a	N	Y	
	M	C	b
a	W	D	
	H	E	b
a	I	L	
	X	N	b
a	R	F	
	V	W	b
a	P	Q	
	Z	I	b

The process of recovering Random-Mixed Alphabets is very much the same as that used for Arbitrarily-Mixed Alphabets. But whereas it is always possible to make certain the recovery of an arbitrarily-mixed Primary Alphabet by reconstructing the generating rectangle, or whatever the system of formation, it is not possible to check a random-mixed alphabet in the same way. Here the proof must be found in the solution of cipher text by means of the Primary Alphabets obtained.

Let us consider the following alphabets:

```
  I  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 II  R U T E B W Q S X L O N G M P Z I V A J F Y H K C D
III  I J P C T N F G H D A E U B R V W X Q Z L K M S O Y
```

From these deciphering alphabets results the sequence of 52 equivalents here shown, beginning with A of Alphabet I and continuing the process as described on page 5. Now if the two strips on which the sequence is recorded are shifted to any position, such as for example the one here shown, it will be noted that the alphabet made up from the *a* letters is exactly the same as that formed by the *b* letters—in other words, the Primary Alphabet System from which the foregoing deciphering alphabets were derived, is one in which the components are identical.

The next problem is to ascertain if the alphabet resulting from this position is the Primary Alphabet. Let us suppose that the following is a portion of the message from which the deciphering alphabets were obtained:

```
   Key:  G E N E R A L
Cipher:  H C J N Z Z P
  Text:  H U N S A R E
```

Now placing the alphabet resulting from the position of the sequence as shown here on two strips, set H of the lower or cipher alphabet to H of the upper, and find the value of the key letter G. It is G. Then resetting the strips so that C of the lower equals U of the upper, it is noted that the key letter, or in this case E, again points to G.

Similarly, when J is set to N, N is below G, when N equals S, E is below G. Since each key letter points always to the same letter G, this signifies that G is the first letter of the original Primary Alphabet.

T A U P Q J R F Z I L V W D X N Y H E K M C S B O G T

Y H E K M $\underline{\text{C}}$ S B O G T A U P Q J R F Z I L V W D X N Y H $\underline{\text{E}}$ K M C S

Now returning to the sequence of equivalents, the strip on the right is shifted until it has its beginning opposite G, keeping in mind that *a* letters must be opposite *a* letters. The alphabet then reads G R D M A Z N S P L H O J W K T F X C U I Y B Q V E . This may or may not be the original Primary Alphabet. But it is an alphabet which will solve any message enciphered by means of that Primary Alphabet, for there must necessarily be a symmetry of position in any alphabet thus derived, which makes it exactly as efficacious as the original itself.

So it is, also, with any system of two components which are random-mixed alphabets, even though not identical. To illustrate, here are the Primary Alphabets of such a system:

A — S Z N G D K W F J E O Y T C U X B V L Q M R A H P I

B — W K A Z H R M P B J Q N T V C X D L I O F E S G U Y

The seventh and twelfth deciphering alphabets derived from these Primaries are as follows:

I A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

II A N J O X U V P T G R Y S K C Z D I B W L F M E Q H

III V H G K O E T Q F P B W R S J A I M Y Z C N X D U L

If there is derived from these deciphering alphabets a sequence of equivalents beginning A A P Z T W L, etc., and the strips upon which the sequence is recorded are shifted, two of the possible resulting alphabets may be as follows:

From *a* letters: N A O Q K I J W L B Y D P U X M G C R S V H E T Z F N

From *b* letters: K A C D R T G M Y N Q O Z L E S V J I B F P X W H U K

Now let us test these alphabets upon some cipher text which was enciphered by means of the original Primary Alphabets.

Key: A M E R I C A N

Text: C O M P A N Y D

Cipher: X D X Z C D V X

Taking the pair of alphabets shown immediately preceding and setting them so that C of the lower equals X cf the upper, it will be found that A, or the key letter for such encipherment, equals S, if the message has been enciphered by the Vigenere method. Resetting them so that O equals D, the encipherment of the second letter, the key letter M in this case, again equals S. Such is found to be the case with each succeeding encipherment. This would indicate that S was the first letter of the Primary Alphabet in which the text letters were found. Therefore in any succeeding cipher text, if the key letter is set to S as in the alphabets used in this portion of text, these alphabets will be found to solve the text exactly as easily as the original Primaries, whose actual recovery then becomes unnecessary.

It may be said in conclusion that these methods for recovering alphabets, although here given as applying to Primary Alphabet Systems alone, may be utilized in many other forms and systems of cipher. The real student of the science will be quick to see their application in manifold ways.

The Index of Coincidence

and

Its Applications in Cryptography

Publication N° 22

PARIS
IMPRIMERIE-LIBRAIRIE MILITAIRE UNIVERSELLE
L. FOURNIER
264, Boulevard Saint-Germain, 264.
(En face du Ministère de la Guerre)

1922

CONTENTS

INTRODUCTORY

Cryptographic frequency tables are not usually considered to partake of the nature of mathematical or statistical curves. The purpose of such tables has commonly been the very simple one of enabling the decipherer to make certain assumptions with respect to the plain text equivalents of the various cipher letters in the tables. These assumptions are usually based upon the relative frequencies of the constituent letters of the tables.

However, the occasions when such tables are regarded and treated as real curves having the definite characteristics of mathematical or statistical frequency distributions, without any analysis being made of the individual frequencies composing the curves, are rather rare ; but when such a treatment is possible, it is one of the most useful and trustworthy methods in cryptography.

In this paper two examples of such a treatment, leading to the solution of somewhat complex ciphers, will be given in detail. In the first one it will be shown how a cipher system involving more than one hundred unknown, random mixed alphabets can be solved without necessitating a single assumption of plain text values. In the second example, it will be shown how a multiple alphabet cipher system, involving both substitution and transposition processes in a somewhat complicated method, can be solved from a single message of no great length. It is believed that the solutions will be of interest to students of cryptography in that they illustrate the principle to which reference has been made above.

INTRODUCTORY

Cryptographic frequency tables are not usually considered to partake of the nature of mathematical or statistical curves. The purpose of such tables has commonly been the very simple one of enabling the decipherer to make certain assumptions with respect to the plain text equivalents of the various cipher letters in the tables. These assumptions are usually based upon the relative frequencies of the constituent letters of the tables.

However, the occasions when such tables are regarded and treated as real curves having the definite characteristics of mathematical or statistical frequency distributions, without any analysis being made of the individual frequencies composing the curves, are rather rare; but when such a treatment is possible, it is one of the most useful and trustworthy methods in cryptography.

In this paper two examples of such a treatment, leading to the solution of somewhat complex ciphers, will be given in detail. In the first one it will be shown how a cipher system involving more than one hundred unknown, random mixed alphabets can be solved without necessitating a single assumption of plain text values. In the second example, it will be shown how a multiple alphabet cipher system, involving both substitution and transposition processes in a somewhat complicated method, can be solved from a single message of no great length. It is believed that the solutions will be of interest to students of cryptography in that they illustrate the principle to which reference has been made above.

I. — THE VOGEL CIPHER

This cipher may be classed under the head of machine ciphers, for it involves the use of an apparatus consisting of five superimposed, concentric disks bearing dissimilar, random mixed alphabets. The disks are mounted upon a base, the outer margin of which is divided into 26 equal segments, one of which is marked *clear*.

The correspondents prepare a *numerical key* consisting of the numbers from 1 to 25 mixed at random, and this key is written in the segments of the base in a clockwise direction, beginning with the segment immediately following the Clear Segment.

If, for example, the key contains but 22 numbers, then not all of the segments can bear numbers and the three segments immediately preceding the Clear Segment will remain blank. In order to explain the system clearly, a set of disks has been prepared and will be used in the subsequent illustrations. It is recommended that the student provide himself with a duplicate set in order that he may the more easily follow the details of the solution. In Fig. 1, the key is seen to consist of 21 numbers, leaving 4 segments blank at the end of the numerical key.

DETAILS OF ENCIPHERMENT

Assuming that we have a series of messages to be enciphered, let us take Message 1 and follow through the encipherment of a few groups. Let the message be :

ENEMY IS INTRENCHING ALONG WESTERN SLOPE OF RIDGE FROM HILL SIX ZERO TWO TO HILL FIVE NINE SEVEN, etc...

The encipherment proceeds in regular groups of five letters, ″ set up ″ in the order 1, 2, 3, 4, 5 from the outer disk inwards, in the Clear Segment.

In Fig. 1, the first five letters of Message 1, viz., ENEMY, are shown in the proper position for encipherment.

This being Message 1, the cipher equivalents for the first group of five letters are taken from Segment 1, in the order 1, 2, 3, 4, 5, i. e.. from the outer disk inwards. These letters are PDKPV.

The next group of five plain text letters, viz., ISINT, is then set up in the Clear Segment and the corresponding cipher group is taken from the segment *immediately following Segment* 1, in a clockwise direction, viz., Segment 13, giving the cipher letters RURVB. The cipher for the third group of five plain text letters, viz., RENCH, is taken from the second segment from Segment 1, viz., Segment 18 ; yielding AMPKD, etc.

The fourth plain text group in this case would fall under the last segment bearing a number, viz., Segment 8. The fifth plain text group would then be taken from the first segment immediately following the Clear Segment, viz., Segment 9. In other words, once the starting point has been determined, the encipherment proceeds, group by group, in a clockwise direction, omitting the blank segments, until the entire message has been enciphered.

Message 2 is now ready for encipherment. Its first group of five plain text letters is set up under the Clear Segment and the equivalent cipher group is taken from Segment 2 ; its second set, from the segment immediately following Segment 2, viz., Segment 1 ; etc. The process is the same as described for Message 1. In like manner. the cipher equivalents for the first set of five plain text letters of Message 3 are taken from Segment 3 ; for the second set of five letters, from the segment immediately following Segment 3, viz., Segment 5, etc.

This is continued for the first 21 messages, i.e., a number of messages corresponding to the length of the numerical key. The cipher equivalent for the first five letters of Messages 22, 43, 64, etc., would be taken from Segment 1 again, repeating the cycle through which Message 1 passed. The first five letters of Messages 23, 44, 65, etc., would be taken from Segment 2, etc. In other words, the starting point for each message is determined by the accession number of the message in the day's activity. Messages whose numbers are multiples of the length of the key, only repeat the cycle.

So much for the details of the encipherment. It is presumed that the secrecy of the system, from a cryptographic standpoint, is to be maintained by a more or less frequent change in alphabets and numerical key, and that the enemy is in possession of the details of the system as a result of the capture of one of the instruments and the consequent solution of a number of messages.

The following 26 messages are presumed to have been intercepted on the same day, and are, therefore assumed to be in the same alphabets and key (1).

THE MESSAGES

N° 1 (140 letters)

```
MLVXK  QNXVD  GIRIE  IMNEE  FEXVP  HPVZR  UKSEK  MVQCI
VXSFW  GVART  YBZKJ  WVUPV  XZCBD  BDOLS  GHINZ  LJCTE
KSLPY  VPBYD  WTRJK  BDDFA  ANJXE  XGHED  ERYVP  YPWDJ
DFTJV  ZHTWB  WXTMF  OZDOJ
```

(1) These are the actual messages submitted by Mr. Vogel.

N° 2 (139 letters)

```
ULJCY   GXAEU   DTEIL   UZBRW   GJZSS   QLUOX   PTFOO   NWSHD
BPTJO   HQRYY   YAXRZ   KTEMP   UAKMK   ISRDZ   VUVKW   HXAYD
YAGSM   CURBZ   LBXOV   EBBPI   BMLCB   UMAXF   ZSLXV   QFUXE
MPZMK   MQZZT   KMURW   EJVB
```

N° 3 (161 letters)

```
YLMKW   CBGSF   VGABP   HOZFV   QQNSQ   NQLQL   DIGXM   XCWAI   QFJOQ
TYDEL   MBMJB   SEPSO   DHREM   ELKIP   KXNMW   QYBIH   BHFDC   GLYWC
YGMMP   EEXZH   UBBSB   SBONG   URQKW   YRAYU   NYUCS   LNEMV   VNSXN
WGVME   MXPDF   WGTZE   KRLGU   ZJFZJ   W
```

N° 4 (142 letters)

```
UFHUJ   LTMKJ   PONFG   RIUGG   OZGWS   UBNMW   WGILB   JNXTD   BPREX
MMWHB   OBFVO   TFGSJ   SLXEH   RTZMI   LLUUX   FIFWC   PGSBA   KRCAS
XWKQV   SLDKS   NTESD   QVQBN   RZDMB   JQLYH   LTMXB   BSVWL   ILKYU
NMFEB   HB
```

N° 5 (156 letters)

```
VJZCQ   KZJJK   DCVQD   KSSXY   TSUXE   GRROH   PXKZF   ZKFMS   VGDWU
XLTBW   EXHEF   AWQWF   ZBSMK   GWCEM   JPNVB   GRJGB   IBWOH   YMOAP
IZYNX   GXMSB   OZZGK   EVURN   NJFGQ   DTPLV   STOID   DWVLR   TXTBH
WNWIE   YJXXW   BKOJQ   FOUHO   T
```

N° 6 (159 letters)

```
XGORF   GCHAX   DUEIQ   XAOWK   BKBUH   SKWWW   XNEYZ   JAKUK   BEQMG
IWTVU   NPCLU   KQDIG   YLMNC   KYJJF   SDSTU   DCBUK   OQUVA   WHSXE
VGQSW   OGHPI   XCYIO   SUAEU   BQAPY   RMDMW   FWGSQ   HMYRQ   LPUVN
LNGQT   IPJRI   HUMAD   DZUTW   BFMO
```

N° 7 (143 letters)

```
UFUCL   HJYDY   ZTHHA   NWJWJ   IFMZI   VZIJE   QODUT   MZPRX   SWNFC
DKKXR   TOSVL   MNHNO   RZRTX   Q1PFN   HOUNL   FGUVO   TPWOI   VHNCQ
RTDCO   LNTTM   MXMXR   TUIIG   ZOJCU   BTXJK   XGUEJ   MSJBS   ESVWJ
IKGSL   APA
```

N° 8 (174 letters)

NWWVY UMHVB RPQHF XOHQN IPATI CFMZT DIMQI 1RUJI NSBWR
VTEGJ IAFEO BMUUT VPSKO HUYNA VPRXS SCUZB JHCDE WUHJV
GXHRP OIHWF LBTKF QESIO YXVNK AWDAA EQLVJ MYYTH GSEYA
KLXHR NCVNY XSQMC XVXJC TJVSC UJEGZ TFONC HNPM

N° 9 (145 letters)

NYMPE YZYRZ AWLPP IMPBB VWAXZ QSVFG ITZMT KZNFC DHSUA
NNCMP SOJKI GDPQZ IIPMV ZOCBO UCKXR SEPEM OTZNM AMHWX
NDEUH YUEIP RFOHI QLQHG IJFRT UTNQC JEGAF SQRWO DAJMT
YKXXQ VRQUW

N° 10 (116 letters)

TEPDA XXHHC FYMFK QRBJV YVJID JBNXF JBLXU KSOXR KNHJK
UFRXL WELQJ QJKFW RLSSF BQJWR BZKYN EAUWP AYSKO UWJDX
CQRVW ZVXXH NZHCW SVEYH NEANW G

N° 11 (124 letters)

SEYBZ MGSOZ CMPSQ BASFH VFSCG CHKSB ZOPRZ CZEVH OCADC
LGRXO XXCKK MVQGJ XYUOC FFFVJ OZCJE AQSJY WZCMO TOXVM
KEXYA VWONX GTCWT TGLOI IWORT JJVQE HYNK

N° 12 (121 letters)

OMTXX WUXZE YEHOJ ALJCO EPLPJ RBCVX VVARW DYBDQ FTZDA
XEUJG ROHUP OFSGQ PONLW RAIBP KACIB GMYSB VKHEU XSPFG
WKZTE KZYIZ ZXFJO HZIVG ESGOX YYCEO B

N° 13 (111 letters)

QNKIT FZHNC GJBSA JIQBX PFTAO RJLUD IKPKI TNUWU EVGHU
LJUFZ UBSMD VNMNZ UWVYQ DJPFY KETMN CLEQS DQXNA GEYHC
JBCPG RNNNH BSYZR STGBV E

N° 14 (141 letters)

```
ZJRKK  CLYZK  RINOK  NBTAK  NOBBI  WRZRX  DQTAR  AEKMY  MOXLT
YVWFL  DXZSK  ZPWNI  JUULI  TPUJR  TPQGH  RJZCQ  XCNHU  NOKMI
KKGEF  FJWWR  ZXROX  PZUGG  HMYNB  DUHQZ  BJDFA  FJAYU  RKHKB
ZMKMI  D
```

N° 15 (163 letters)

```
OSULC  VZAFW  SQAUC  WPRBI  WCFUO  JKQHY  OIWVX  KSMSX  MBXOZ
QQDCX  CBIMT  DGIAS  BAQRK  RUHHF  JYUJG  DYNMA  CWULT  PKWEE
UUHTF  FOQOK  KNRPI  PLLXQ  DRDEM  JMCFB  WLHVX  FIFZR  STVJV
XDCAS  BEHQV  OPWEY  UTISE  NZFCU  BXI
```

N° 16 (120 letters)

```
VHXVD  RSRYI  PVNWQ  QEDMJ  LTKFN  RMDGT  DNVBM  JDGVP  KJMND
RRQDM  STTAL  GKPPO  PZTCU  BNCEE  HAWMB  KRGNU  ZXCWQ  VEZTC
DIPSG  ZUFVH  OZIGB  TQXND  HMHEW  VHTLT
```

Nº 17 (135 letters)

```
UMMOL  HVVEQ  GWTJI  PQTNS  AEFZH  TOFQH  COXNQ  NPDDT  QVSJR
RAABK  ZCVWR  UUJEG  NMJHQ  CHZUM  TTSIU  GHELW  HUMFH  LZHNH
CJEDW  AKHZA  SDZIE  HIHWG  LBUFZ  DVPUB  DCMXO  NAYEY  GQHID
```

N° 18 (127 letters)

```
LALNH  QUDUA  ZBZUD  VSJFE  MEHXW  EUWZT  OKWNO  OOSIL  TASEG
OVQVX  PMKKW  BQBBI  VGDGJ  JDAHW  RZDIA  WQJXB  FBRLA  AHJEP
PUMEU  HJQJR  ZSPPQ  VAWDL  HECDA  LPJJS  ZOJYB  MO
```

N° 19 (204 letters)

```
YTVUL  TWEVD  MBHKV  IHTPI  GNXBQ  XAUAQ  OUFVO  GSMKB  BAKIG
YRNAF  BKIJC  ZJSRN  WBQHM  UYJPT  CHCCB  RLNVH  OLDQA  ZZDCV
UWMNZ  OPRFC  RDONY  RCZAM  ZYNVQ  WFONZ  CTTES  IRWER  GKETA
YUSUK  TFECD  BMQVB  VBWVV  VWCZP  TWCTJ  FHFEH  VNDCO  MZVLK
YUJPZ  BHLDY  VVPMD  KFHPB  VCYU
```

N° 20 (138 letters)

```
OBHOK  UWRON  AJDFH  FRQMI  ULOTG  XXIEV  HMAKV  PVMAV  OITKD
LDQIW  UYVWI  JEJRQ  MCUZP  KGUDN  QSPBF  TQVZP  IZJTU  RBUFZ
JUSIZ  DCIGX  QESJD  LIZVM  AOPME  YNEXI  HOXJK  KUYHK  AORUY
LVD
```

N° 21 (154 letters)

```
OMXOW  LTWEW  KFJHN  ZMSKK  GXFDL  YLGPT  YYYNQ  CYYMA  ZWRAD
HGWBI  HHCGM  FDGMN  XIQDN  NPLYQ  NPJNZ  OWFVV  KMGVH  KHCUC
STNVZ  CGXHV  LZZXX  SVTKG  POEAC  OJYQU  MEULH  KHYDD  ETPDN
QYZVU  HIMGG  RBHEW  CUSO
```

N° 22 (167 letters)

```
SFDFM  AQMQW  FFONY  GVFZH  JTPSY  IAONR  TWSZJ  OJUGA  HOGXW
YJOUN  AEGQG  HTZPB  YRNEI  BWIVZ  JNPXG  SXXSZ  HVRUC  QEHQR
CXEUF  UKCTB  BETEX  ZSLRK  QFXUV  CLRIL  LHIGG  FVDSQ  RJCSH
JJMIV  JFCEU  QFPMO  TFSOQ  XKESC  CJCFI  BN
```

N° 23 (141 letters)

```
LHKGP  KUKNY  WJROV  XZHPK  JJIHU  LUVBU  ZRUDA  XXHRF  MOAFT
XUWVE  YZAJE  NFDEX  GDZGA  JBZET  XYHAL  DGECA  CDPYM  BTMYK
LCSMI  YVSWW  DQNAP  KFPAO  FIQTR  KQQIE  HHYCA  GHEBF  PFTYF
DZAUO  W
```

N° 24 (127 letters)

```
OMOOK  OKWHR  MPXQI  PIQMN  ALWNK  HZIKQ  XQNUY  GQZNG  DFTFO
YJODO  XIRIX  KDCBX  UEQTU  VPIWA  NFWOH  GWXXY  EKBMG  MGETD
WFKKZ  PXXZL  XFRWL  FHTEG  INNJI  ETVUP  QHTJY  OP
```

N° 25 (161 letters)

```
FPETJ  CDVNY  LMKQU  CDALX  FIYGR  HQMIP  FAONR  QCAVJ  MFIAC
YXDKR  GWMQL  FQMEJ  KOBMS  ZURAN  ULZFE  YDLOT  UZMJM  SETNP
GWILM  FGCVS  NCZGB  HU1RT  XUWAI  DGAML  QBTFK  VYIGT  FLUVK
FJYAZ  YQNVO  WSMSS  CCMFY  KVKRA  Y
```

N° 26 (549 letters)

```
XFYKU   NDBFZ   KNDMF   GBVIJ   TKNDA   LGPKS   CWPSK   BSNWH   LTTXN
VDCYO   GYZLI   TRURC   GBIWL   VEKYG   YOOHV   IAUNO   LPSJJ   UTNIE
ZAECE   XQDYB   FDBPB   SEBMA   SRUEU   RUWKE   RIYIT   BDWVG   MZNGB
TRJTG   PZJCM   LSFXW   ANHJO   UZHRQ   ULXFU   XS1NC   MVKNT   ZWXXQ
VWRIH   MPMHG   DURHG   IJKIR   UFRNA   APKQP   KAXUF   CACVC   LNICD
ESOWP   MJQEC   GGJBF   SGMFC   TQRGT   JODEE   XHRXE   KIOZG   DLRZV
DLZCS   EMVZL   GAMFQ   ULGXC   WIZWK   IIZYY   HTAVV   OTTTO   RFTHL
HQWVZ   XZUAB   GLHMH   ZFTIQ   OTJEP   VZXCL   YFYOE   LS1JU   SYBMC
YQXGD   SECCE   CIJTI   BUILZ   ZUAPV   QRYXB   VMHWL   LPXGC   RLETI
DJBCW   IHSAM   RHCMJ   RAQBJ   IWORY   OISIE   RESKE   PAUJD   SMQVB
VEASF   TZCWL   AUHKA   MSTZZ   DDQYB   RCMUS   UXWQX   WDPDB   BYGMQ
XRLCH   IOKZO   EPLQU   XKZKI   JNSSI   HCHXX   ZMZKW   PVUGD   QCVQ
```

PRINCIPLES OF SOLUTION

When the details of the method of encipherment have been thoroughly grasped, the principles upon which a solution may be achieved become rather easy to comprehend. Let us consider the two-fold result of the method of encipherment.

1. — The encipherment proceeds in regular groups of five plain text letters each, and the equivalent cipher groups are taken from *the successive and unbroken sequence of segments, in a clockwise direction from any given initial segment.* In a single long message this sequence of cipher segments must repeat itself, resulting, therefore, in the production of what we have termed an *internal cycle* within messages. The length of this cycle is equal to that of the numerical key, i. e., it contains as many numbers as does the numerical key. Thus, in the illustrative example the numerical key consists of 21 numbers, and the length of the Internal Cycle, therefore, is 21 groups. In a message of 105 groups, for example, the cycle would be repeated five times, the 1st, 22nd, 43rd, 64th, and 85th groups marking the initial segments of the five repetitions of the cycle. These groups would be enciphered in the same cipher segment. The 2nd, 23rd, 44th, 65th, and 86th groups would be enciphered in the next segment to the right of the preceding segment, etc.

Since the letters within each group of five are enciphered in regular order by means of the five primary alphabets, the length of this cycle in terms of letters is five times its length in terms of groups. Thus, the length of a cycle of 21 groups is 105 letters, that of a cycle of 22 groups is 110 letters, etc. The length of the Internal Cycle in terms of letters we have called the *Internal period.*

Now, each cipher segment is a different distance from the Clear Segment, so that the result of this method of encipherment is the same as though five sliding primary alphabets were employed. For example, suppose we had the alphabets of the illustrative disks mounted upon sliding strips. and shifted these sliding alphabets eight letters apart. Thus :

Alphabet 1

```
                                              +
Y G W J O I D M N C T X S B L P K V A U F Q Z E R H Y
A U F Q Z E R H Y G W J O I D M N C T X S B L P K V A
          |                                   +
```

Alphabet 2

```
                                              +
Q A O X G F Z M Y L P U K E T D J V S W I R B N H C Q
S W I R B N C H Q A O X G F Z M Y L P U K E T D J V S
          |                                   +
```

Alphabet 3

```
                                              +
Z X C M L R Y A W J B Q I H V K P U F O G T N E D S Z
F O G T N E D S Z X C M L R Y A W J B Q I H V K P U F
          |                                   +
```

Alphabet 4

```
                                              +
N U I O S E H J R D L G K Q B P Y A C V X Z W M T F N
C V X Z W M T F N U I O S E H J R D L G K Q B P Y A C
          |                                   +
```

Alphabet 5

```
                                              +
R L Q B P C I S A E T J U D M V Z N W H X O G Y K F R
W H X O G Y K F R L Q B P C 1 S A E T J U D M V Z N W
          |                                   +
```

Note that the cipher equivalents of the plain text letters ENEMY are PDKPV, the same as we found in the encipherment by the means of the concentric disks. In the latter, the cipher segment was the eighth segment after the Clear Segment ; in the sliding alphabets we shifted the two alphabets eight letters apart and obtained the same result. The method of the encipherment by means of the disks is therefore equivalent to the use of five sliding primary alphabets with the exceptions to be noted below.

The sliding of a 26 character primary alphabet against itself through all possible positions, results in the production of a series of 26 secondary alphabets, and the sliding of five such primary alphabets results in the production of a total of 130 secondary alphabets. But, since in the Vogel Cipher the Clear Segment is never used as a cipher segment, there can be involved in this cipher not more than 125 secondary alphabets, for the omission of this segment from the sequence of cipher segments is the same as having the primary alphabets slide through only

25 possible positions. Further more, if the numerical key consists of less than 25 numbers then the number of secondary alphabets employed will be less than 125 and will be a function of the length of the numerical key. Thus, if the key consists of 21 numbers there will be involved 21 × 5, or 105 secondary alphabets ; if of 22 numbers, 22 × 5, or 110 secondary alphabets, etc. In other words, the exact number of secondary alphabets involved coincides with the length of the Internal Period.

If the numerical key consists of 21 numbers, and a message of 105 letters is enciphered, each letter of this message will belong to a different secondary alphabet. If the message consists of 210 letters, there will be two letters in each of the 105 secondary alphabets ; if of 315 letters there will be three letters in each secondary alphabet, etc. If, now the message of 315 letters is written out in lines of 105 letters, the length of the Internal Period, the successive columns in the set up will contain the letters of the successive 105 secondary alphabets.

2. — The Internal Cycle is the same for all messages ; it is only the initial segment in the cycle which changes with each message, and the number of different initial segments is obviously determined by the length of the numerical key. The initial segment for each message is indicated by the accession number of the message in the day's activity. Thus, in a key consisting of 21 numbers there are only 21 different starting points, or initial segments, and messages whose numbers are greater than the length of the numerical key merely repeat the sequence of initial segments, so that Messages 1, 22, 43, 64... begin with the same initial segment. Since the numbers applying to the segments are in a random mixed sequence determined by the numerical key, *these initial segments constitute a cycle which when reconstructed will give us the sequence of numbers in the numerical key*. This latter cycle we have termed the *External Cycle*, since it does not involve the internal relations within the messages themselves but is concerned with the relations existing outside the messages, viz., those relations existing between the initial and successive segments of the series of messages in the day's activity.

It is by taking advantage of the existence of the *Internal Period* that we are able to gain our first information concerning the numerical key, viz., its *length*. Then, by taking advantage of the existence of the *External Cycle*, we shall be able to reconstruct the *sequence* in the numerical key. After these two steps have been successfully accomplished, we shall then be able to attack the more difficult problem of reconstructing the alphabets.

The solution resolves itself therefore into three distinct steps as follows :

1. — The determination of the length of the Internal Period.

2. — The reconstruction of the External Cycle.

3. — The reconstruction of the alphabets.

1° THE DETERMINATION OF THE LENGTH OF THE INTERNAL PERIOD

It was stated that within a single long message, the cycle of cipher segments repeats itself. Thus, if the key consists of 21 numbers, the 22nd group will be enciphered in the same segment as the 1st ; the 23rd, in the same segment as the 2nd, etc.

Now it is clear that identical plain text letters whose cipher equivalents fall within the same primary alphabet and within the same cipher segment, will be represented by identical cipher letters, *thus giving rise to recurrences at definite intervals dependent upon the length of the Internal Period.* Thus, if the key consists of 21 numbers, the length of the Internal Period is 105 letters. If there are repetitions in the plain text at intervals of 105 letters, there will be corresponding repetitions in the cipher text. The interval between such repetitions will be indicative of the length of the Internal Period, and hence of the length of the numerical key. There would be involved here only a special case of the ordinary process of factoring as known in the typical multiple alphabet cipher of the periodic or cyclic type. Thus, in this case, if it happens that, the 1st, 2nd, and 3rd, and the 106th, 107th, and 108th letters of the message are THE, then there will be a repetition of the initial trigraph in the cipher text representing THE at a distance of 105 letters, which would indicate a key of 21 numbers. But such recurrences of trigraphs or polygraphs would naturally be very infrequent, except in a large amount of text, on account of the relatively long Internal Period of the system.

However, we need not depend upon the finding of recurrences of bigraphs, trigraphs, or polygraphs. The recurrences of individual letters may be used, with considerable accuracy, as a basis for determination of the length of the Internal Period, through the preparation of what we have termed *Tables of coincidence.* In explaining the preparation and use of such tables we may as well use the series of test messages with which we are concerned.

Let us start with the assumption that the length of the Internal Period is 100 letters, in which case the numerical key would consist of 100/5 = 20 numbers. Taking the longest message of the series, Message 26, it is transcribed in lines containing 100 letters each. These lines are then exactly superimposed, letter for letter, and a count is made of the total number of repetitions *within columns.* Thus, if in the 1st column the letter K occurs twice, this fact is indicated in our table by placing one check mark opposite the line labelled " 20 numbers ", indicating that there is a coincidence of two letters within the column. If there are three identical letters, then three check marks are recorded, for we have here a coincidence between the 1st and 2nd repetitions, the 2nd and 3rd, and the 1st and 3rd. If there are four identical letters, then six check marks are recorded. The total number of such coincidences is found and indicated in the proper line of the table.

Then an assumption of an Internal Period 105 letters in length is made. The message is now transcribed into lines of 105 letters each, and the number of coincidences within columns again determined. When the correct assumption with respect to the length of the Internal Period is made, the greatest total of coincidences will be obtained, for this will correspond to the greatest number of repetitions of identical letters within the same alphabets and within the same segments.

For accurate comparison, the various totals of coincidence obtained for the different assumed lengths of the Internal Period should be corrected in some manner in order to make a proper allowance for the differences which are due solely to the various numbers of alphabets assumed. For example, suppose that a total of 39 coincidences were obtained for the assumption of an Internal Period of 100 letters and also for one of 105 letters. From a cryptographic point of view, it stands to reason that a total of 39 coincidences indicates a slightly higher amount of repetition within 105 columns than the same number of coincidences within only 100 columns from the mere fact that in the former arrangement the number of letters in each column is slightly less than it is in the latter arrangement, and hence the chances for repetitions are less in the former. If, therefore, we wish to make an accurate comparison we should reduce all totals to a common basis. If we select as our basis of comparison an assumed length of 100 letters, then the total of coincidence for a length of 105 letters should be multiplied by the factor $\frac{105}{100} = 1{,}05$; that for a length of 110 letters, by the factor $\frac{110}{100} = 1{,}10$, etc.

Note the Table of Coincidence for Message 26 (Table 1). It is not thought necessary to assume a period of less than 100 letters, and we know it could not be more than 125, since the numerical key cannot contain more than 25 numbers.

Since the greatest number of coincidences is obtained on an assumption of an Internal Period 115 letters in length, it follows that the numerical key consists of 23 numbers, and that there must be two blank segments on the base disk. Note the repetitions within columns when Message 26 is transcribed upon this basis (Fig. 2).

2° THE RECONSTRUCTION OF THE EXTERNAL CYCLE

Having found the length of the Internal Period, and thus of the length of the numerical key, the next step is to reconstruct the sequence of numbers of which the latter is composed. This, as stated before, is accomplished by taking advantage of the fact that the initial points of the various messages of the day's activity go through the External Cycle determined by the numerical key. The External Cycle will give the *relative* positions of the numbers in the numerical key, and later, their absolute positions on the base disk, i. e., the numerical key itself, will be found.

We will first proceed, therefore, to reconstruct the External Cycle. This is done by regarding the cycle as partaking of the nature of a continuous, unbroken chain, which in fact it is, since there is nothing in the messages themselves to indicate the positions of the initial segments in the External Cycle.

Since the key is 23 numbers in length, it follows that Messages 24, 25, and 26 start with the same initial segment as Messages 1, 2, and 3, respectively.

We proceed at once, therefore, to combine Messages 1 and 24, 2 and 25, 3 and 26, into 3 sets as shown in Figs. 3, 4, and 5.

Now Messages 1 & 24, 2 & 25, 3 & 26 belong in such relative positions as are determined by the relative positions of the numbers 1, 2, and 3 in the numerical key. For example, if the sequence were... 3.... 1.. 2..., then if we superimpose Messages 1 & 24 and 3 & 26 in various relative positions and make a Table of Coincidence for the various positions, we should get the greatest total of coincidences when Messages 1 & 24 have been moved five segments to the right (corresponding to a clockwise encipherment) of Messages 3 & 26, *because the successive groups of cipher letters would then represent enciphwerments in exactly the same sequence of cipher segments.* Likewise, we should get the greatest total of coincidences when Messages 2 & 25 are moved eight segments to the right of Messages 3 & 26, or three segments to the right of Messages 1 & 24. In other words, when one message is superimposed in the correct position with respect to another message the greatest number of coincidences will result. Conversely, by making a Table of Coincidence for all possible relative positions of two superimposed messages, that superimposition which gives the greatest total of coincidences will indicate their correct relative positions.

Taking Messages 1 & 24, written in superimposed lines of 23 groups of five letters each, and placing them one group, or interval [1], to the right of the corresponding groups of Messages 3 & 26, we make a count of all the coincidences as before. Then Messages 1 & 24 are moved 2, 3, 4... intervals to the right until all the 22 possible positions have been tried. The greatest total, as shown in Table 2, is found when Messages 1 & 24 are placed three intervals to the right of Messages 3 & 26. This means that Number 1 occupies Position 4 in a cycle in which Number 3 occupies Position 1.

Our External Cycle, therefore, begins as follows :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
3	.	.	1																			

As soon as the position of each number is found, it is omitted from the succeeding trials, since there can be no repetitions in the numerical key.

Messages 2 & 25 are then taken for experiment and a similar table is made for the various superimpositions with Messages 3 & 26. In this table the 3 interval or 4th position test is omitted, since we have found that Number 1 belongs in the 4th position in the cycle. The data for Messages 2 & 25 when superimposed with Messages 3 & 26 are given Table 3.

When we reach Position 9 the total of coincidences is so much higher for that position than for the previously tested positions that there can be no doubt about the correctness of Position 9 for Number 2. We may, therefore, omit all further tests for positions after 9 for Number 2. In the subsequent tests, when a trial for a certain position gives a much larger number of coincidences than the average for the preceding tests, the succeeding trials are omitted.

On the other hand, in certain cases, no trial stands out prominently enough from among the others to enable a definite placement to be made. In such cases a secondary test must be applied. For example, in attempting to find the position of Number 4, the table 4 of coincidences results when Messages 3 & 26 are used as the base.

It is doubtful whether a preponderance of five coincidences in the trial for Position 21 over that for Position 5, is significant. We must look for confirmation in another test. Having found the position of Numbers 1 and 2, in the cycle we may use them as bases just as well as Number 3.

Our cycle so far is as follows :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
3	.	.	1	.	.	.	.	2														

If Number 4 belongs in Position 21, and not in Position 5, then a greater number of coincidences should obtain when Message 4 is superimposed with the combined Messages [1 & 24] + [2 & 25] in the former position, which is 12 intervals to the right of Message 2, than in the latter position, which is 4 intervals to the left of Message 2. These trials give 55 coincidences for Position 21 as against only 32 for Position 5. The data for this complete secondary test are given Table 5.

This calculation shows conclusively that Number 4 belongs in Position 21. In the subse-

[1] An interval in this case is equal to a group of five letters.

quent trials a similar procedure is followed when the first set of tests gives inconclusive results. The data for the placement of the remaining numbers in the External Cycle are given in Table 6, with the result that the following External Cycle is established :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
3	18	17	1	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10

This reconstructed cycle represents, as stated above, the relative, not the absolute, positions of the numbers of the numerical key, because there is as yet no way of determining which of these numbers occupies any given segment after the Clear Segment ; not can it be determined as yet where the break of two intervals, representing the two blank segments, falls.

The next step is to attempt a reconstruction of the primary alphabets.

3° RECONSTRUCTION OF THE PRIMARY ALPHABETS

Upon the basis of the cycle as determined above, all the messages are superimposed in their correct relative positions so that all groups which have been enciphered in the same segment are beneath one another.

The External Cycle is first transcribed with the Number 1 as the initial number in the cycle, making it read as follows :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17

There is no special purpose in thus rewriting the cycle ; it is merely to permit of the superimposition of the series of messages in regular order from 1 to 26. They are shown in Fig. 6.

The letters in each of the 115 columns of Fig. 6 belong to individual, single mixed alphabets, all secondary alphabets, resultants of the five primary alphabets.

Inasmuch as these secondary, single mixed alphabets will be used as the basis for further work, individual frequency tables applying to them have been made and are given Table 7. The individual tables are given in groups of five, labelled A, B, C, D, and E, corresponding to the five primary alphabets of the system. The groups themselves are given in the External Cycle sequence, so that each set of five alphabets is accompanied by the number which identifies its position in the sequence of segments. Thus we may refer to any of these alphabets by number and letter, as for example 8A, meaning the first single alphabet under Segment 8. The A alphabets all apply to the outermost primary alphabet, or alphabet 1 ; the B alphabet, to alphabet 2, etc. (Table 7.)

Now it is clear that we could attempt a decipherment and a tentative partial reconstruction of each of the 115 secondary alphabets, on the basis of the repetitions in each alphabet. For example, we might assume the most frequently occurring letter in each alphabet to be the cipher equivalent of E, the next T, and so on, attempting to build up words from such assumptions. But each of these alphabets contains only approximately 36 letters, so that no assumptions could be made with any degree of certainty. This is especially the case in English where the letter E does not *always* stand out as the most frequently used letter. Should such an attempt be necessary, and were there available a large volume of text, such a reconstruction might seem practicable and feasible.

But as a matter of fact this is not necessary and such labor is not entailed, for we can, by another method, effect a direct reconstruction of the five primary alphabets, which will not only enable us to find the plain text for every message but will also give us every one of the possible 125 secondary alphabets of the entire system.

Furthermore, in order to effect such a reconstruction it is only necessary that there be available a sufficient volume of texte so that the cipher equivalent of *solely the letter* E can be selected with certainty in every column in each group. For English, certainly no less than 50 letters per column would be necessary ; for German, or French, probably 35 to 40 letters would do.

The method is based upon the fact that the segments from which the cipher groups are taken follow one another in an almost uninterrupted succession and in a clockwise direction from a given initial segment. The only interruption in the succession occurs where the blank segments, representing the break in the numerical key, fall. To explain the principle in detail, we will first call attention to the fact that, as a result of this method of encipherment, *the series of successive cipher equivalents for any given plain text letter in any one of the five primary alphabets constitutes the sequence of letters in that alphabet* (1). For example, turn to Fig. 1 and note that in Alphabet 1 the sequence of letters beginning with A, is as follows :

A U F Q Z E R H Y G W J O I D M N C...

Now it is patent that if we place letter A *in the Clear Segment, its series of successive cipher equivalents coincides with the sequence of letters succeeding* A *in the same alphabet*, viz., UFQZERHYGWJOIDMNC.... If we place another letter, for example, Z, in the Clear Segment, its series of successive cipher equivalents constitutes exactly the same sequence, except with a different initial point, viz., ERHYGWJOIDMNC... In other words the successive cipher equivalents for these two plain text letters form one and the same cycle or sequence. Now, the same is true with respect to every other letter of Alphabet 1, and also of the other primary alphabets. Of course, the sequence is different for each primary alphabet.

Since this cycle or sequence of letters is the same for all the letters of each primary alphabet, only the series of successive cipher equivalents for one letter of each primary alphabet is necessary in order to effect a complete reconstruction of that alphabet. In other words, if we can select with accuracy the cipher equivalent for *one and only one* plain text letter in each of the successive 115 secondary alphabets, we can then arrange them into five sequences of letters which will coincide with the five primary alphabets, thus resulting in their reconstruction. The reconstructed sequences will be complete except for the omission of two or more letters representing the blank segments. If the numerical key consists of 23 numbers, three letters will be missing from each sequence. These letters will be known, of course, but their relative positions in the omitted section will have to be found later.

[1] This sequence will be complete except for the omission of two or more letters. The reason for this omission is given on page 7.

Obviously, the letter which will lend itself best to such a procedure is E, for it is usually the most frequently occurring letter in English plain text. If, therefore, by a careful study of the individual frequency tables applying to the columns of the superimposed messages, we can select the cipher equivalents of E with certainty in the successive *secondary* alphabets, we shall at once have the sequences of letters in the five primary alphabets and the solution of the problem will be at hand. For example, if in a hypothetical sequence of these alphabets we select the letters W, K, R, and Z, respectively, as the four successive cipher equivalents of E, then this will mean that in primary Alphabet 1 there is a sequence... WKRZ..., (providing a break in the numerical key does not exist between the members of the sequence of key numbers applying to the segments concerned). Continuing this process, ultimately the five primary alphabets can be completely reconstructed. But we must remember always that this process is dependent upon the correct assumptions for the cipher equivalent of E in each of the 115 secondary alphabets, or columns of cipher text.

Let us attempt such a reconstruction. Turning to the series of secondary alphabets given in Table 7, wo try to find in each A Alphabet the letter which undoubtedly represents plain text letter E. At the very start we encounter difficulties. In Alphabet IA, the letters M and Y are of equal frequency. There is no way of telling which letter might represent E, so that we shall have to consider both M and Y as possibilities. In Alphabet 8A again we have difficulties, for both J and Q have the same frequency. It begins to look like a very doubtful procedure. As we go further along, the difficulties in selecting the representative of E increase rather than decrease and the decipherer becomes lost in a multiplicity of possibilities. Evidently the method, while theoretically correct, is practically out of the question because of the limited size of each frequency table. In fact, it is doubtful whether we can select the representative of E with certainty in any one of the A alphabets (1), and certainly, if we cannot do this with the letter which theoretically occurs the most frequently we cannot do it with any other letter. We may, however, console ourselves with the knowledge that there is, theoretically, absolutely no doubt but that the method outlined above, based upon the selection of the most frequently occurring letter in each secondary alphabet, is correct and practicable for a large volume of text.

This method failing, however, because the representative of E could not be selected with certainty in even 50 % of the columns, we shall proceed to apply another method, and shall hope for more success.

First, let us make a consolidated frequency table for all of the A secondary alphabets. This is done by collecting the data contained in the individual frequency tables shown in Table 7 into one large table, taking only the data applying to the letters of primary Alphabet 1, i. e., the A Alphabets only are taken. This larger table is shown Table 8.

This consolidated frequency table is of a rather peculiar nature. Each column gives the frequency of the cipher letters in a particular segment. There are 23 such columns, corresponding to the 23 segments of the numerical key. The columns are in the sequence determined by the External Cycle, as given on page 19, viz., 1 8 12 16, etc. Each row gives the frequency of a particular cipher letter and since the columns succeed one another in one and the same sequence,

(1) It was found later that the cipher equivalent of E has the greatest frequency in only three out of the twenty-three alphabets. In one alphabet E did not occur at all, and in six cases it occured only two times. It will be of interest to the student to study these tables for the information they contain with regard to the extreme degrees of variation from the normal that small frequency tab'es can exhibit.

it follows that the frequencies in the successive segments on a line with any given cipher letter form a definite *sequence of frequencies*. There being 26 cipher letters, there are 26 such rows, or sequences of frequencies. Some rather important conclusions can be drawn from the data in this table, as will presently be explained.

The total frequency for each cipher letter is given in the column labelled as such and the average frequency for all cipher letters is then found to be 841/26 = 32,4 occurrences. The number of different segments in which the cipher letter applying to the given line occurs is indicated in the next column ; and the average frequency per segment for each cipher letter is given in the last column.

Before we can proceed it will be advisable to establish certain principles which will enable us to follow the subsequent reasoning more easily. We shall make use of Alphabet 1 shown in Fig. 6, calling attention to the fact that the same principles apply to the other four primary alphabets. In order to make the illustration comparable in all its details with the real situation in the test problem, let us make the numerical key 23 numbers in length by adding Numbers 22 and 23 at the end of the key shown in Fig. 1. (Fig. 7.)

Let us see what plain text letters the cipher letters A, B, and C represent in the sequence of segments. (Fig. 8.)

It will be noted that the successive plain text letters which cipher letters A, B, and C represent, constitute almost exactly the same sequence in the three lines. This follows from the nature of the cipher system itself, and the cause of it has already been pointed out. In the B line there is a section not present in the A line, consisting of the letters FUA ; in the A line, the section not present in the C line consists of the letters XTC ; and in the C line, the section not present in the B line consists of the letters PLB. This is due to the fact that the numerical key requires only 23 segments to be employed, leaving two segments unoccupied, plus one more segment representing the Clear Segment, since no plain text letter can be enciphered by itself. This missing section of three letters will be different for every cipher letter ; but it will always consist of a sequence of *three successive* letters of the primary alphabet.

Let us now accompany the sequence of plain text letters opposite each of the letters A, B, and C, with a sequence of frequencies corresponding to the theoretical frequency of each plain text letter (1). (Fig. 9.)

Now, since the sequences of plain text letters represented by these sequences of frequencies are the same, it follows that we can so arrange the latter as to make the successive individual frequencies coincide ; and if we make due allowance for the break in the sequences caused by the omitted sections of three letters, the three sequences should coincide exactly. (Fig. 10.)

In order to make the sequences coincide, we displaced the B sequence five intervals to the right of the A sequence, and the C sequence four intervals to the right of the B sequence. Let us reverse the order of these letters, A, B, and C, and space them in accordance with the number of intervals which each sequence of frequencies has been shifted relative to the others. Thus :

...C... B... A...

[1] These theoretical frequencies are given by Hitt on the basis of 200 letters of plain text. See Hitt, Parker. *A Manual for the Solution of Military Ciphers*, 1918, p. 6.

Refer now to the illustrative cipher alphabet in Fig. 7, and note that this corresponds to the order of these letters A, B, and C in this primary alphabet. We have determined the order of these letters in our alphabet merely by correctly superimposing or shifting the three sequences of frequencies relative to one another so as to make the individual frequencies coincide.

Now had we not known what letters these individual frequencies represented, but had merely been given the sequences of frequencies themselves it would still have been just as easy to find the correct relative positions of the three sequences, from a comparison of the positions of high and low points in each sequence of frequencies. In other words, *we do not need to know what letters the individual frequencies in each sequence represent ;* it is still possible to determine, (*by a study of the positions of the high and low points in each sequence of frequencies,*) the relative positions (in the primary alphabet) of the letters applying to each sequence in the cipher alphabet. No analysis whatever of the individual frequencies is necessary, the entire frequency table being treated as an ordinary statistical curve. This, in its final analysis, is the meaning of the proposition stated in the opening paragraph of this paper [1]. It thus follows that the five primary alphabets may be reconstructed, without a knowledge of what letter any individual frequency represents, by an analysis of the frequency tables considered as true statistical curves.

Let us return now to the test messages. Table 8 represents a set of 26 sequences of frequencies similar in origin to those for A, B, and C in the illustrative alphabet above. We could superimpose these sequences in the same manner and as easily as we did in the case above were it not for two circumstances : first, we do not know where the break in the sequences falls, because we have only the relative position of each number in the numerical key and not its absolute position ; and secondly, the individual frequencies in each sequence of frequencies in our problem, do not exactly correspond to the theoretical frequencies of the plain text letters to which they apply, but only correspond approximately to the theoretical. In some cases this approximation is far from close because of the paucity of text, and this will make the determination of the correct relative positions of two sequences a much more difficult process than was the case with the illustrative sequences above.

We are, therefore, confronted with the problem of superimposing the sequences of frequencies correctly without a knowledge of these two factors, and this we shall accomplish by a slight modification of method and a recourse to some simple mathematics.

First, as to the modification of method due to our ignorance of the exact location of the break in the numerical key, this consists in superimposing sequences, not to find the relative displacements, or positions, of *any pair of sequences* that may be chosen for experiment, but to find such

[1] The ordinary frequency table applying to a plain text, or a cipher alphabet does not correspond to the ordinary frequency distribution of statistical work. In the latter, the positions of the points along one of the axes of the graph and their extension along the other axis are either causally related, or the curve treats of data which, being subject to the operation of the laws of probability, form the normal, or Quetelet Curve of error. In the former, the positions and extensions of the coordinates are not related in any way unless one considers the arbitrary order of the letters of the alphabet as constituting a cause. The positions of the coordinates in a cryptographic curve were determined many centuries ago when the English language was first evolved.

But the sequences of frequencies in Table 8 are not similar in origin to the ordinary plain text or cipher alphabet frequency tables of cryptographic work. They are, in fact, closely related to certain frequency distributions of statistical data because the positions and extensions of the coordinates are absolutely determined by a cause other than the arbitrary order of the letters of the English alphabet. These two characteristics of the curves of a series of secondary alphabets may be varied at will by changing the sequence of letters in the primary alphabet. Any set of frequency distributions applying to a series of secondary alphabets derived from a variable primary alphabet may be treated in the same mathematical manner as these will be treated in the subsequent pages.

sequences as are *one and only one interval apart*,i. e., sequences which represent a relative displacement of only one interval.

Let us consider the sequences of frequencies corresponding to the cipher letter A and the letter which immediately follows it in the illustrative alphabet, viz., U, arranging the sequences as though we had only reconstructed the External Cycle and had not as yet reconstructed the numerical key, i. e., beginning the sequences with Segment 1. (Fig. 11.)

It is evident that we may superimpose these sequences correctly by shifting the A sequence one space to the right of the U sequence, and repeating the letter G at the end of the U sequence. (Fig. 12.)

Note now that complete and perfect coincidence between successive pairs of superimposed segments is obtained except in two cases, viz., those involving the letters A and Q in the U and A lines respectively. This is due to the fact that the break in the sequence comes between segments 23 and 9. The frequency of letter A of the U sequence should be matched with the frequency of A in the sequence, but the latter does not occur because of the break in the numerical key. The same is the case with the letter Q of the A sequence.

Now suppose that we did not know where the break in the numerical key falls, and let us superimpose the sequences again (Fig. 13).

It is seen that perfect coincidence is still maintained throughout except in the case of the one pair of segments containing the letters A and Q of the U and A lines, respectively. By omitting the three blank segments representing the place where the break occurs, we have brought the letters A and Q into an incorrect superimposition. But the amount of the error due to the superimposition of one pair of incorrect letters as against the correct superimposition of 22 other pairs is of so little consequence that it may be neglected altogether. *In other words, when we superimpose sequences which are only one interval apart, we may neglect the discrepancy that would be due to our ignorance of where the break in the numerical key comes.*

Now suppose that we did not know that the letter U immediately follows A in this illustrative primary alphabet, and had only a table containing sequences of frequencies applying to the cipher letters (similar to those shown in Table 8). It is evident that by placing the A sequence one interval to the right of all other sequences successively, and choosing that sequence which most closely coincides with the A sequence in the positions of the high and low points, we shall thus have determined what letter immediately follows A in the primary alphabet. In this case, for example, the U sequence would be chosen and we would conclude that the sequence in the primary alphabet is ...AU... Taking the U sequence the same operation is performed with the other sequences as before, and we thus find the letter that follows U in the primary alphabet. Theoretically, therefore, we should be able to reconstruct the complete primary alphabet by this method, and thus overcome the difficulty with regard to the location of the break in the numerical key.

In this process of matching sequences of frequencies to decide which one most closely coincides with a given sequence, we cannot depend upon a mere ocular examination and comparison. We must reduce the operation to a mathematical method. This, we shall proceed to consider.

Let us return now to Table 8, and select that line for experiment which gives the best indications of representing the closest approximation to a theoretical frequency table containing as few elements as are contained in the average line in the table. In a theoretical frequency table of small size such as the one shown in Fig. 14, only the high frequency letters are represented ;

the low frequency letters are absent. The average frequency per letter that does occur is evidently the total frequency, viz., 32, divided by the number of different letters that go to make up this total, viz., 12. This quotient is 32/12 = 2,67.

Note now that the Y line of frequencies in Table 8 averages 3.00 occurrences par segment ; this is, the average frequency par plain text letter which Y represents is 3.00. This is even a little better than the average theoretical frequency per letter as determined above. Let us consider the Y sequence of frequencies, therefore, as representing the closest approximation to a theoretical frequency table of similar total frequency as the Y sequence.

Following the method discussed above, let us see if we can find the letter in Alphabet 1 which follows Y.

Taking our Y sequence of frequencies, let us apply it to all the other sequences, placing the Y sequence one interval to the right of the other sequences. Thus, with A, the Y sequence is placed as shown. Fig. 15.

We shall now proceed to find an abstract number such as will indicate the degree to which these two sequences of frequencies agree, or fit, when placed with reference to each other as in Fig. 15. It is evident that when we strike the letter which really follows Y in the Alphabet 1, the sequence of frequencies concerned should give the best fit with the Y sequence and thus produce the greatest coincidence.

Let us now compare the two superimposed sequences above, segment by segment. In the upper one of the first pair of superimposed segments there are 2 occurrences of A ; in the lower one, 5 occurrences of Y. The first pair of segments agree, therefore, in 2 occurrences ; i. e. there are 2 coincidences. In the next pair of segments, an occurrence of 1 in the Y sequence is matched by an occurrence of 1 in the A sequence ; i. e., there is 1 coincidence. Let us go through the rest of the segments in the same manner. The results are given in Table 9 :

We have a total of 12 coincidences. But we must also take into consideration the number of non-coincidences between the two sequences ; for these, as can easily be demonstrated, are of equal importance with the coincidences. In the two hypothetical sequences given Fig. 16, both with the same total frequency, the number of coincidences is very high, viz., 28, yet the two sequences do not agree at all closely.

Let us find the total of non-coincidences, therefore, between the Y and the A sequences. In the first pair of segments there are 3 non-coincidences ; in the second pair, none ; in the third pair 1, etc. Let us now add these to our table, and include also the number of occurrences in the segments, for we shall have need of this information very soon (Table 10).

We find that the total of coincidences is 12, that of non-coincidences, 34. The difference is 12 — 34 = — 22. Were the sequences in closer agreement, this difference would be a positive quantity ; but as a rule, we shall find it to be a negative quantity in our work because of the fact that the frequencies throughout are relatively low. In this case, then, the number of non-coincidences is 22 greater than the number of coincidences. This difference between the totals of coincidences and non-coincidences will be used as the basis for the determination of the degree to which two sequences coincide, and inasmuch as we shall have a great many such differences to compute, a short cut to their determination will be of use. If we subtract the total of occurrences from three times the total of coincidences, we can find this difference directly without having to count up the number of non-coincidences. Thus, in this case, (3 × 12) — 58 = — 22. In all subsequent determinations we shall use this method.

Now it is obvious that the number of coincidences as well as the number of non-coincidences is not only a function of the distribution of the occurrences in each sequence of frequencies, but also of the total number of occurrences. It is patent that in one pair of sequences with a greater total number of occurrences than in another pair, the totals of coincidences and non-coincidences might be greater in the former than in the latter from the mere preponderance of chances for coincidences and non-coincidences in the former. We should therefore take into consideration the total number of occurrences in the two superimposed sequences, and the most logical correction would be to divide the difference between the totals of coincidences and non-coincidences by the total number of occurrences of all the segments. For example, it is only reasonable to place more reliance upon a case in which out of 30 occurrences the difference between the totals of coincidences and non-coincidences is + 10, than upon a case in which out of 60 occurrences the difference between these same totals is also + 10. In the former case, the quotient obtained by dividing the difference, + 10, by the total occurrences, 30, is + .33 ; in the latter case, the quotient obtained by dividing + 10 by 60 is only + .17.

This quotient, which indicates in a general way the " goodness of fit " of the two superimposed sequences, and which is obtained by dividing the difference between the totals of coincidences and non-coincidences by the total occurrences, we have termed the INDEX OF COINCIDENCE. It is evident that the greater the index of coincidence, the better is the agreement between the superimposed sequences, and thus, the closer is the fit. Where the two sequences are relatively low in frequency, the total of non-coincidences will, as a rule, be greater than the total of coincidences, so that the difference will usually be a negative quantity and the index will also be negative. As these negative indices approach 0, they become closer to positive indices, so that when we are dealing with negative indices, the lowest absolute index will indicate the greatest coincidence. Thus, an index of — .03 will indicate a much better fit than an index of — .35 (1).

Returning now to case in hand, we found the difference between the totals of coincidences and non-coincidences to be —22. Since a total of 58 occurrences enters into the formation of these two tables, then the index of coincidence for the assumption that A follows Y in Alphabet 1 is — 22/58 = — .38.

Let us perform the same calculations for the rest of the letters in Table 8, omitting of course, Y. The data are given in Table 11. As stated above, the best fit is obtained when the index of coincidence is the greatest positive quantity. In none of these cases above, is the index of coincidence positive, but the value for P, viz., — .12, approaches the nearest to a positive quantity, and therefore represents the greatest degree of coincidence. The next greatest index is given by

[1] It is easy to demonstrate that according to the method adopted, all indices must must lie within the limits — 1.00 and + 0,50. Given two sequences with equal numbers of occurences and in one case, perfect coincidence, in the other case, perfect non-coincidence.

Let x = Occurences for one sequence
Then 2 x = Total » » both sequences

Case 1

Perfect coincidence

No. of coincidences = x

Differences = 3 x — 2 x = x

Index of coincidence $= \frac{x}{2x} = \frac{1}{2} = + .50$

Case 2

Perfect non-coincidence

No. of coincidences = 0

Differences 0 — 2 x — = 2 x

Index of coincidence $= \frac{-2x}{2x} = - 1.00$

the letter Q : but inasmuch as the index for P is almost twice as great as that for Q, we may conclude that it is the letter P, and not the letter Q, which immediately succeeds Y in the Alphabet 1.

To demonstrate the superiority of this mathematical method of comparison over a graphic method in which a close study of curves would be necessary, three sets of superimposed curves have been prepared and are shown in Fig. 17. In the upper set, the Y and the P frequencies are superimposed in their correct relative positions. We found that the Index of Coincidence for this superimposition, which is the correct one, is — .12. In the middle set of curves, the frequencies for Y and Q are superimposed. The index for this superimposition is the closest to that for Y and P, viz., — .23. In the bottom set of ourves, the frequencies for Y and W are superimposed. The index for this superimposition is the furthest removed from that for Y and P, viz., —.67. In a large series of such sets it would be a rather difficult matter to select the correct superimposition from a study of the closeness of fit. The eye and the memory would be overtaxed with a multiplicity of such curves and no conclusive selection could be made. The mathematical method, however, reduces all the data to a common basis of comparison, so that little difficulty is encountered in finding the correct sequence of letters.

We may now proceed to find the letter that follows P. The same operations are performed with the letter P as were with the letter Y, this time using the frequency of P as the base and trying it one interval removed from the frequencies of all letters except Y and P ; for as the position of each letter is determined, it can be automatically omitted from the succeeding calculations.

The data are as given Table 12.

It is seen that the index for letter C, viz., —.20 represents the greatest degree of coincidence. But the index for A is —.25 and that for R is —.30. In other words, the index for C is only .05 greater than that for A, and .10 greater than that for R. The question then arises : Is a difference of .05, or .10, in favor of C over A and R, respectively, a significant difference ? In other words, might not the letter A or R follow P, instead of C ? The answer may be found by modifying the method in one particular. We have been superimposing sequences with a relative displacement of but one interval. If now we superimpose sequences with a relative displacement of two intervals, the error due to the failure to take into account the break in the numerical key will be greater than it is with a relative displacement of one interval, for now there will be two incorrect pairs of superimposed letters, but still the results should be significant. Let us, therefore, test out all the letters which are less than twice the index of C, with the Y sequence removed two *intervals*. Thus with A, the sequences are in this position :

The data for the letters which may possibly follow P, when tested with the Y sequence at two intervals removed are as given Table 12 a.

These calculations show conclusively that C follows P in Alphabet 1. In the tables showing the calculations for the reconstruction of Alphabet 1, whenever the first calculation, using one-interval data, fails to show a letter whose index of coincidence is at least twice as great as its nearest rival, a secondary calculation will be made using two-interval data. In two cases, viz., for the letters following K and Z, it will be noted that three-interval data were employed to determine the correct letter subsequent to an inconclusive secondary calculation.

The tables containing the rest of the data for the reconstruction of Alphabet 1 are given Table 13. In these tables the columns have been labelled 1 to 4. Column 1 gives the total of occurrences ; Column 2, the number of coincidences ; Column 3, the differences ; Column 4, the index of coincidence.

The now completely reconstructed Alphabet 1 is as follows :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Y	P	C	O	U	G	A	K	D	V	X	R	S	H	W	B	I	N	Q	M	F	Z	E	J	L	T

This reconstruction is, so far, purely the result of hypothesis. Moreover, we do not as yet know where the break in the numerical key comes, and this we shall proceed now to find.

Consider the External Cycle as we have given it on page 00.

1 8 12 16 20 2 22 15 6 11 5 19 13 23 9 21 7 4 14 10 3 18 17

Let us begin by assumeng that the break occurs between the first two numbers in our External Cycle.

If the break occurrs between Segments 1 and 8, the numerical key would be, beginning with the first segment to the right of the plain text segment. (Fig. 19.)

Returning now to the Y sequence of frequencies in Table 8, still retaining the assumption of a break between Segments 1 and 8 in the numerical key, the Y sequence should be broken and rearranged in order to conform to the assumed break in numerical key as shown. Fig. 20.

Below these frequencies let us place the plain text letters which they represent upon the assumption of a break between the numbers 1 and 8 in the key. (Fig. 21.)

This looks like a fairly good assortment of high frequency letters, with the single exception of T. It may be that we have struck the correct place for the break at the first trial. Let us corroborate it by another method.

Assuming the break to be as shown in Fig. 19, let us make a list of the cipher letters which should represent E in the successive segments (Fig. 22).

Let us turn now to the respective frequencies of these cipher letters as given in Table 7, taking the frequencies of the letters, J, L, T,... in the A columns. They are as shown. Fig. 23.

On the whole, this is as good as can be expected for the small number of occurrences in each table. Let us do the same for the letters T, O, and A. If the results are as good as those for E we may conclude that we have really found the absolute positions of the numbers in the numerical key. (Fig. 24.)

These distributions and frequencies are certainly excellent and we may regard our numerical key as established. The initial segment after the Clear is Number 8.

We could proceed to reconstruct Alphabets 2, 3, 4, and 5 by exactly the same principles as were used in the reconstruction of Alphabet 1. To do so would be of theoretical interest, because it would represent a case where the reconstruction of five primary alphabets, from the frequencies of 115 unknown secondary alphabets, is accomplished without a preliminary tentative decipherment of even so much as a single word. In short, it would represent a case where the decipherer, without attempting the decipherment of any part of the text, comes at once to be in the same position as the correspondents, and can decipher any message as rapidly as the legitimate recipients.

Where a staff of clerks and experts is available, this method would indeed be followed, for the personnel could be divided into five groups, each group being assigned an alphabet to reconstruct. Each group could be subdivided into two sections, one working forward from a given letter, the other working backward from the same letter. After not more than three to six hours all five alphabets will have been reconstructed in their entirety. Or perhaps it would be more practicable to reconstruct only three of the primary alphabets, say the 1st, 3rd, and 5th, filling in the other two from the resulting decipherment.

In the present instance, however, after Alphabet 1 had been reconstructed, the reconstruction of Alphabet 3 was successfully accomplished by the application of the same principles as were used for Alphabet 1.

Then a partial decipherment, in which the repetitions of digraphs and trigraphs within adjacent columns played an important part, led to the reconstruction of the other three primary alphabets.

The data for the reconstruction of Alphabet 3 are given in Table 15. Since the location of the break in the numerical key was determined after the reconstruction of Alphabet 1, the columns in Table 14, upon which the reconstruction of Alphabet 3 is based, are given in the correct numerical key order so that any two sequences of frequencies could be superimposed at any intervals. However, one interval and two-interval data were used almost exclusively except in one or two doubtful instances where greater intervals were employed. (Tables 14 et 15.)

The completely reconstructed Alphabet 3 is as follows :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
H	Y	M	U	B	I	N	C	T	W	R	X	L	A	D	Z	G	F	S	V	K	O	E	J	P	Q

With Alphabets 1 and 3 et hand, the partial decipherment of the initial groups of a few messages soon lead to the complete reconstruction of the other three alphabets. For example, note what these two alphabets give for the beginning of Message 11 :

Segments	11	5	19
Alphabets	12345	12345	12345
Cipher...........	SEYBZ	MGSOZ	CMPSQ
Plain text........	O.S..	V.T..	N....

```
                 12345  12345  1
The word OBSER  VATIO  N comes to mind almost at once.
```

This means that we have determined the following values :

Alphabet 2	Alphabet 4	Alphabet 5
Segment 11, $B_p = E_c$	Segment 11, $E_p = B_c$	Segment 11, $R_p = Z_c$
» 5, $A_p = G_c$	» 5, $I_p = O_c$	» 5, $O_p = Z_c$

New values thus determined are inserted in their correct positions, with the result that after a short time Alphabets 2, 4, and 5 are completely reconstructed. The five alphabets are found to be as follows :

1. — YPCOUGAKDVXRSHWBINQMFZEJLT
2. — EQMSLPYVCJTAKHUZFBRXIGNWDO
3. — RXLADZGFSVKOEJPQHYMUBINCTW
4. — ATEVXZYNFGSBIHQRPCMDKWOJUL
5. — AEFBNKLTIXMVORYWHQJUGCZPDS

Proof of their correctness may be at once established by deciphering the first few groups of Message 1. They are as follows :

```
MLVXK  QNXVD  GIRIE  IMNEE  FEXVP  HPVZR  UKSEK  MVQCI  etc.
EVENI  NGREP  ORTSS  HOULD  INCLU  DEDAI  LYLOS  SESSE  etc.
```

" EVENING REPORTS SHOULD INCLUDE DAILY LOSSES ...... "

This cipher is of interest also in view of its striking similarity to the Bazeries disk cipher, or the " Star Cipher ", described in a previous publication [1].

In the latter cipher, instead of only five primary alphabets, there are 20 to 25, and instead of having a numerical key to determine where the cipher equivalents are to be taken, no key of that nature is used, or needed, since the correct line, or generatrix, is easily found because it is the only one that gives intelligible text throughout its length. The segments in the Vogel Cipher correspond to the generatrices in the Star Cipher. In the former, the cipher letters are taken from a definite cycle of generatrices, and not all generatrices are used ; in the latter, no such cycle obtains, for it is unnecessary, and all 25 generatrices may be used at random.

The fatal defect in this cipher, from the point of view of its practical indecipherability, is that the segments, or generatrices, are used in a definite sequence or cycle, giving rise to the internal and external cycles. It was through them that the recovery of the numerical key and the primary alphabets was possible.

[1] Riverbank Publication N° 20. *Several Machine Ciphers and Methods for their Solution,* 1918.

FIGURES

Fig. 1

Vogel Cipher

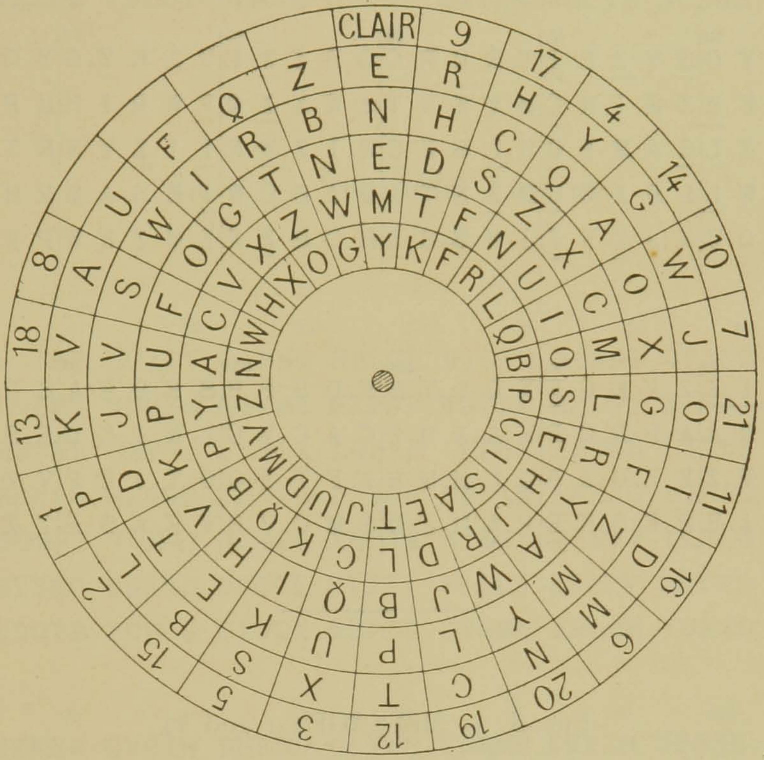

CLAIR 9 17 4 14 10 7 21 11 16 6 20 19 12 3 5 15 2 1 13 18 8
E R H Y G W J O I D M N C T X S B L P K V A U F Q Z
N H C Q A O X G F Z M Y L P U K E T D J V S W I R B
E D S Z X C M L R Y A W J B Q̆ I H V K P U F O G T N
M T F N U I O S E H J R D L C K Q̆ B P Y A C V X Z W
Y K F R L Q B P C I S A E T J U D M V Z N W H X O G

FIG. 2. — MESSAGE 26 transcribed according an internal period of 115 letters

```
1       5        10        15        20        25        30        35        40
X F Y K U|N D B F Z|K N D M F|G B V I J|T K N D A|G G P K S|C W P S K|B S N W H
R U W K E|R I Y I T|B D W V G|M Z N G B|T R J T G|P Z J C M|L S F X W|A N H J O
M J Q E C|G G J B F|S G M F C|T Q R G T|J O D E E|X H R X E|K I O Z G|D L R Z V
Y F Y O E|L S I J U|S Y B M C|Y Q X G D|S E C C E|C I J T I|B U I L Z|Z U A P V
A U H K A|M S T Z Z|D D Q Y B|R C M U S|U X W Q X|W D P D B|B Y G M Q|X R L C H

41     45        50        55        60        65        70        75        80
L T T X N|V D C Y O|G Y Z L I|T R U R C|G B I W L|V E K Y G|Y O O H V|L A U N O
U Z H R Q|U L X F U|X S I N C|M V K N T|Z W X X Q|V W R I H|M P M H G|D U R H G
D L Z C S|E M V Z L|G A M F Q|U L G X C|W I Z W K|I I Z Y Y|H T A V V|O T T T O
Q R Y X B|V H M W L|L P X G C|R L E T I|D J B C W|I H S A M|R H C M J|R A Q B J
I O K Z O|E P L Q U|X J Z K I|J N S S I|H C H X X|Z M Z K W|P V U G D|Q C V Q

81     85        90        95       100       105       110       115
L P S J J|U T N I E|Z A E C E|X Q D Y B|F D B P B|S E B M A|S R U E U
I J K I R|U F R N A|A P D Q P|K A X U F|C A C V C|L N I C D|E S O W P
R F T H L|H Q W V Z|X Z U A B|G L H M H|Z F T I Q|O T J E P|V Z X C L
I W O R Y|O I S I E|R E S K E|P A U J D|S M Q V B|V E A S F|T Z C W L
```

FIG. 3. — MESSAGES 1 and 24

```
         5    10    15    20    25    30    35    40    45    50    55    60
1.   MLVXK QNXVD GIRIE IMNEE FEXVP HPVZR UKSEK MVQCI VKSFW GVART YBZKJ WVUPV
     YPWDJ DFTJV ZHTWB WXTMF OZDOJ
24.  OMOOK OKWHR MPXQI PIQMN ALWNK HZIKQ XQNUY GQZNG DFTFO YJODO XIRIX KDCBX
     ETVUP QHTJY OP

        65    70    75    80    85    90    95   100   105   110   115
1.   XZCBD BDOIS GHINZ LJCTE KSLPY VPBYD WTRJK BDDFA ANJXE XGHED ERYVP
21.  UEQTU VPIWA NFWOH GWXXY EKBMG MGETD WFKKZ PXXZL XFRWL FHTEG INNJI
```

Fig. 4. — MESSAGES 2 and 25

```
        5    10    15    20    25    30    35    40    45    50    55    60
    ULJCY GXAEU DTEIL UZBRW GJZSS QLUOX PTFOO NWSHD BPTJO HQRYY YAXRZ QTEMO
    QFXUE MPZMK MQZZT KMURW EJVB
25. FPETJ CDVNY IMKQU CDAOX FIYGR HQMIP FAONR QCAVJ MFIAC YXDKR GWMQL FQMEJ
    DGAML QBTFK VYIGT FLUVK FJYAZ YQNVO SWMSS CCMFY KVKRA Y

       65    70    75    80    85    90    95   100   105   110   115
2   UAYMK ISRDZ VUVKW HXAYD YAGSM CURBZ LBXOV EBBPI BMLCB UMAXF ZSLXV
25  KOBMS ZURAN ULZFE YDLOT UZMJM SETNP GWILM FGCVS NCZGB HUIRT XUWAI
```

Fig. 5. — MESSAGES 3 and 26

```
        5    10    15    20    25    30    35    40    45    50    55    60
    YLMKW CBGSF VGABP HOZFV QQNSQ NQLQL DIGXM XCWAI QFJOQ TYDEL MBMJB SEPSO
    YRAYU NYUCS LNEMV VNSXN QGVME MXPDF WGTZE KRLGU ZJFZJ W
26. XFYKU NDBFZ KNDMF GBVIJ TKNDA LGPKS CWPSK BSNWH LTTXN VDCYO GYZLI TRURC
    RUWKE RIYIT BDWVG MZNGB TRJTG PZJCM LSFXW ANHJO UZHRQ ULXFU XSINC MVKNT
    MJQEC GGJBF SGMFC TQRGT JODEE XHRXE KIOZG DLRZV DLZCS EMVZL GAMFQ ULGXC
    YFYOE LSIJU SYBMC YQXGD SECCE CIJTI BUILZ ZUAPV QRYXB VHMWL LPXGC RLETI
    AUHKA MSTZZ DDQYB RCMUS UXWQX WDPDB BYGMQ XRLCH IOKZO EPLQU XJZKI JNSSI

       65    70    75    80    85    90    95   100   105   110   115
3   DHREM ELKIP KXNMW QYBIH BHFDC GLYWC YGMMP EEXZH UBBSB SBONG URQKW
26  GBIWL VEKYG YOOHV IAUNO LPSJJ UTNIE ZAECE XQDYB FDBPB SEBMA SRUEU
    ZWXXQ VWRIH MPMHG DURHG IJKIR UFRNA APKQP KAXUF CACVC LNICD ESOWP
    WIZWK IIZYY HTAVV OTTTO RFTHL HQWVZ XZUAB GLHMH ZFTIQ OTJEP VZXCL
    DJBCW IKSAM RHCMJ RAQBJ IWORY OISIE RESKE PAUJD SMQVB VEASF TZCWL
    HCHXX ZMZKW PVUGD QCVQ
```

FIG.

```
    1      8      12     16     20     2      22     15     6      11     5
1.  MLVXK  QNXVD  GIRIE  IMNEE  FEXVP  HPVZR  UKSEK  MVQZI  VXSFW  GVART  YBZKJ
    YPWDJ  DFTHV  ZHTWB  WXTMF  OZDOJ
                                   2.  ULJCY  GXAEU  DTEIL  UZBRW  GJZSS  QLUOX
    LBXOV  EBBPI  BMLCB  UMAXF  ZSLXV  QFXUE  MPZMK  MQZZT  KMURW  EJVB
    HOZFV  QQNSQ  NQLQL  DIGXM  XCWAI  QFJOQ  TYDEL  MBMJB  SEPSO  DHREM  ELKIP
    VNSXN  WGVME  MXPDF  WGTZE  KRLGU  ZJFZJ  W
    WGILB  JNXTD  BPREX  MMWHB  OBFVO  TFGSJ  SLXEH  RTZMI  LLUUX  FIFWC  PGSBA
                                                                      5.  VJZCQ
    GWCEM  JPNVB  GRJGB  IBWOH  YMOAP  IZYNX  GXMSB  OZZGK  FVURN  NJFGQ  DTPLV
                                                     6.  XGORF  GCHAX  DUEIQ
    DCBUK  OQUVA  WHSXE  VGQSW  OGHPI  XCYIO  SUAEU  BQAPY  RMDMW  FWGSQ  HYMRQ

    MZPRX  SWNFC  DKXXR  TOSVL  MNHNO  RZRTX  QIPFN  HOUNL  FGUVO  TPOWI  VHNCQ
       8.  NWWVY  UMHVB  RPQHF  XOHQN  IPATI  CFMZT  DIMQI  IRUJI  NSBWR  VTEGJ
    YXVNK  AWDAA  EQLVJ  MYYTH  GSEYA  KLXHR  NCVNY  XSQMC  XVXJC  TJVSC  UJEGZ
    NNCMP  SOJKI  GDPQZ  IIPMV  ZOCBO  UCKXR  SEPEM  OTZNM  AMHWX  NDEUH  YUEIP

    YVJID  JBNXF  JBLXU  KXOSR  KNHJK  UFRXL  WELQJ  QJKFW  RLSSF  BQJWR  BZKYN
                                                           11.  SEYBZ  NGSOZ
    OZCJE  AQSJY  WZCMO  TOXVM  KEXYA  VWONX  GTCWT  TGLOI  IWORT  JJVQE  HYNK
             12.  OMTXS  WUXZE  YEHOJ  ALJCO  EPLPJ  RBCVX  VVARW  DYBDQ  FTZDA
    HZIVG  ESGOX  YYCEO  B
    VNMNZ  UWVYQ  DJPFY  KETMN  CLEQS  DQXNA  GEYHC  JBCPG  RNNNH  BSYZR  STGBV
    WRZRX  DQTAR  AEKMY  MOXLT  YVWFL  DXZSK  ZPWNI  JUULI  TPUJR  TPQGH  RJZCQ
                                                15.  OSULC  WZAFW  SQAUC  WPRBI
    CWULT  PKWEE  UUHTF  FOQOK  KNRPI  PLLXQ  DRDEM  JMCFB  WLHVX  FIFZR  STVJV
                    16.  VHXVD  RSRYI  PVNWQ  QEDMJ  LTKFN  RMDGT  DNMBM  JDGVP
    OZIGB  TQXND  HMHEW  VHTLT
    HVVEQ  GWTJI  PQTNS  AEFZH  TOFQH  OOXNQ  NPDDT  QVSJR  RAABX  ZCVWR  UUJEG
    DCMXO  NAYEY  GQHID
    ZBZUD  VSJFE  MEHXW  EUWZT  OKWNO  OOSIL  TASEG  OVQVX  PMKKW  BQRBI  VGDGJ
                                                                          19.
    MO
    WBQHM  UYJPT  CHCCB  RLNVH  OLDQA  ZZDCV  UWMNZ  OPRFC  RDONY  RCZAM  ZYNVQ
    MZVLK  YUJPZ  BHLDY  VVPMD  KFHPB  VCYU
                           20.  OBHOK  UWRON  AJDFH  FRQMI  ULOTG  XXIEV  HMAKV
    DCIGX  QESJD  LIZVM  AOPME  YNEXI  HOXJK  KUYHK  AORUY  LVD
    ZWRAD  HGWBI  HHCGM  FDGMN  XIQDN  NPLYQ  NPJNZ  OWFVV  KMGVH  KHCUC  STNVZ
                                         22.  SFDFM  AQMQW  FFONY  GVFZH  JTPSY
    QEHQR  CXEUF  UKCTB  BETEX  ZSLRK  QFXUV  CLRIL  LHIGG  FVDSQ  RJCSH  JJMIV

    YZAJE  NFDEX  GDZGA  JBZET  XYHAL  DGECA  CDPYM  BTMYK  LCSMI  YVSWW  DQNAP
24. OMOOK  OKWHR  MPXQI  PIQMN  ALWNK  HZIKQ  XQNUY  GQZNG  DFTFO  YJODO  XIRIX
    ETVUP  QHTJY  OP                  25.  FPETJ  CDVNY  LMKQU  CDALX  FIYGR  HQMIP
    GWILM  FGCVS  NCZGB  HUIRT  XUAWI  DGAML  QBTFK  VYIGT  FLUVK  FJYAZ  YQNVO
    GBVIJ  TKNDA  LGPKS  CWPSK  BSNWH  LTTXN  VDCYO  GYZLI  TRURC  GBIWL  VEKYG
    MZNGB  TRJTG  PZJCM  LSFSW  ANHJO  UZHRQ  ULXFU  XSINC  MVKNT  ZWXXQ  VWRIH
    TQRGT  JODEE  XHRXE  KIOZG  DLRZV  DLZCS  EMVZL  GAMFQ  ULGXC  WIZWK  IIZYY
    YQXGD  SECCE  CIJTI  BUILZ  ZUAPV  QRYXB  VHMWL  LPXGC  RLETI  DJBCW  IHSAM
    RCMUS  UXWQX  WDPDB  BYGMQ  XRLCH  IOKZO  EPLQU  XJZKI  JNSSI  HCHXX  ZMZKW
```

6

```
  19     13     23      9     21      7      4     14     10      3     18     17
WVUPV  XZCBD  BDOLS  GHINZ  LJCTE  KSLPY  VPBYD  WTRJK  BDDFA  ANJXE  XGHED  ERYVP

PTFOO  NWSHD  BPTJO  HQRYY  YAXRZ  KTEMP  UAYMK  ISRDZ  VUVKW  HXAYD  YAGSM  CURBZ
                                                           3.  YIMKW  CBGSF  VGABP
KXNMW  QYBIH  BHFDC  GLYWC  YGMMP  EEXZH  UBBSB  SBONG  URQKW  YRAYU  NYUCS  LNEMV
                                      4.  UFHUJ  LTMKJ  PONFG  RIUGG  OZGWS  UBNMW
KRCAS  XWKQV  SLDKS  NTESD  QVQBN  RZDMB  JQLYH  LTMXB  BSVWL  ILKYU  NMFEB  HB
KZJJK  DCVQD  KSSXY  TSUXE  GRROH  PXKZF  ZKFMS  VGDWU  XLTBW  EXHEF  AWQWF  ZESMX
STOID  DWVLR  TXTBH  WNWIE  YJXXW  BKOJQ  FOUHO  T
XAOWK  BKBUH  SKWWW  XNEYZ  JAKUK  BEQMG  IWTVU  NPCLU  KQDIG  YLMNC  KYJJF  SDSTU
LPUVN  LNGQT  IPJRI  HUMAD  DZUTW  BFMO
                               7.  UFUCL  HJYDY  ZTHHA  NWJWJ  IFMZI  VZIJE  QODUT
RTDCO  LNTTM  MXMXR  TUIIG  ZOJCU  BTXJK  KGUEJ  MSJBS  ESVWJ  IKGSL  APA
IAFEO  BMUUT  VPSKO  HUYNA  VPRXS  SCUZB  JHCDE  WUHJV  GXHRP  OIHWF  LBTKF  QESIO
TFONC  HNPM      9.  NYMPE  YZYRZ  AWLPP  IMPBB  VWAXZ  QSVFG  ITZMT  KZNFC  DHSUA
RFOHI  QLQHG  IJFRT  UTNQC  JEGAF  SQRWO  DAJMT  YKXXQ  VRQUW
                                                  10.  TEPDA  XXHHC  FYMFK  QRBJV
EAUWP  AYSKO  UWJDX  CQRVW  ZVXXH  NZHCW  SVEYH  NEANW  G
CMPSQ  BASFH  VFSCG  CHKSB  ZOPRZ  CZEVH  OCADC  LGRXO  XXCKK  MVQGJ  XYUOC  FFFVJ

XEUJG  ROHUP  OFSGQ  PONLW  RAIBP  KACIB  GMYSB  VKHEU  XSPFG  WKZTE  KZYIZ  ZXFJO
  13.  QNKIT  FZHNC  GJBSA  JIQBX  PFTAO  RJLUD  IKPKI  TNUWU  EVGHU  LJUFZ  UBSMD
E                                          14.  ZJRKK  CLYZK  RINOK  NBTAK  NOBBI
KCNHU  NOKMI  KKGEF  FJWWR  ZXROX  PZUGG  HMYNB  DUHQZ  BJDFA  FJAYU  RKHKB  SMKMI
WCFUO  JKQHY  OIWVX  KSMSX  MBXOZ  QQDCX  CBIMT  DGIAS  BAQRK  RUHHF  JYUJG  DYNMA
XDCAS  BEHQV  OPWEY  UTISE  NZFCU  BXI
KJMND  RRQDM  STTAL  GKPPO  PZTCU  BNCEE  HAWMB  HRGNU  ZXCWQ  VEZTC  DIPSG  ZUFVH
                                                                         17.  UMMOL
NMJHQ  CHZUM  TTSRU  GHELW  HUMFH  LZHNH  CJEDW  AKHZA  SDZIE  HIHWG  LBUFZ  DVPUB
                                                                  18.  LALNH  QUDUA
JDAHW  RZDIA  WQJXB  FBRLA  AHJEP  PUMEU  HJQJP  ZSPPQ  VZWDL  HECDA  LPJJS  ZOJYB
YTVUL  TWEVD  MBHKV  IHTPI  GNXBQ  XAUAQ  OUFVO  GSMKB  BAKIG  YRNAF  BKIJC  ZJSRN
WFONZ  CTTES  IRWER  GKETA  YUSUK  TFECD  BMQVB  VBWVV  VWCZP  TWCTJ  FHFEH  VNDCO

PVMVA  OITKD  LDQIW  UYVWI  JEJRQ  MCUZP  KGUDN  QSPBF  TQVZP  IZJTU  RBUFZ  JUSIZ
                        21.  OMXOW  LTWEW  KFJHN  ZMSKK  GXFDL  YLGPT  YYYNQ  CYYMA
CGXHV  LZZXX  SVTKG  POEAC  OJYQU  MEULH  KHYDD  ETPDN  QYZVU  HIMGG  RBHEW  CUSO
IAONR  TWSZJ  OJUGA  HOGXW  YJOUN  AEGQG  HTZPB  YRNEI  BWIVZ  JNPXG  SXXSZ  HVRUC
JFCEU  QFPMO  TFSOQ  XKESC  CJCFI  BN
         23.  LHKGP  KUKNY  WJROY  XZHPK  JJIHU  LUVBU  ZRUDA  XXHRF  MOAFT  XUWVE
KFPAO  FIQTR  KQQIE  HHYCA  GHEBF  PFTYF  DZAUO  W
KDCBX  UEQTU  VPIWA  NFWOH  GWXXY  EKBMG  MGETD  WFKKZ  PXXZL  XFRWL  FHTEG  INNJI
FAONR  QCAVJ  MFIAC  YXDKR  GWMQL  FQMEJ  KOBMS  ZURAN  ULZFE  YDLOT  UZMJM  SETNP
WSMSS  CCMFY  KVKRY  Y                                    26.  XFYKU  NDBFZ  KNDMF
YOOHV  IAUNO  LPSJJ  UTNIE  ZAECE  XQDYB  FDBPB  SEBMA  SRUEU  RUWKE  RIYIT  BDWWG
MPMHG  DURHG  IJKIR  UFRNA  APKQP  KAXUF  CACVC  LNIVD  ESOWP  MJQEC  GGJBF  SGMFC
HTAVV  OTTTO  RFTHL  HQWVZ  XZUAB  GLHMH  ZFTIQ  OTJEP  VZXCL  YFYOE  LSIJU  SYBMC
RHCMJ  RAQBJ  IWORY  IOSIE  RESKE  PAUJD  SMQVB  VEASF  TZCWL  AUHKA  MSTZZ  DDQYB
PVUGD  QCVQ
```

Fig. 7

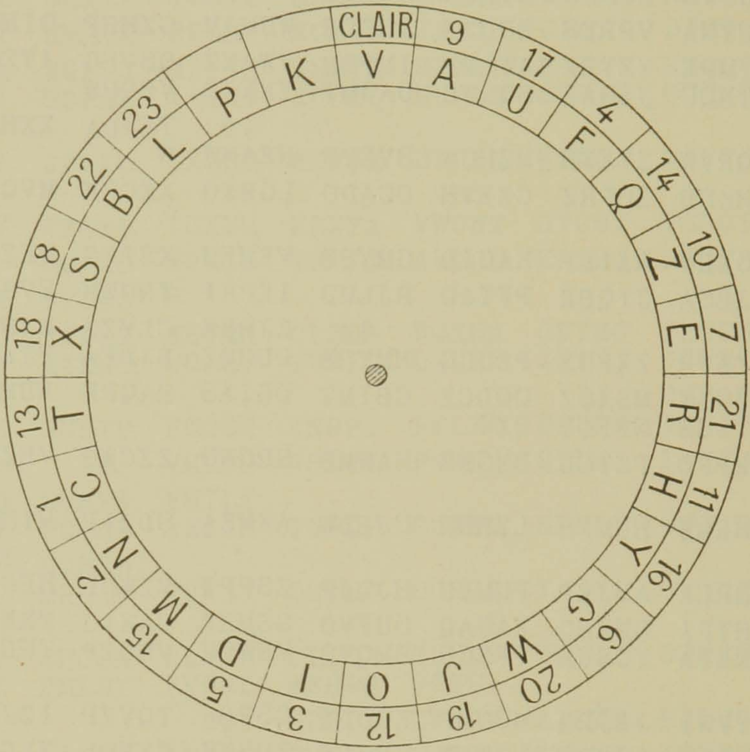

CLAIR
9
17
4
14
10
7
21
11
16
6
20
19
12
3
5
15
2
1
13
18
8
22
23
V
A
U
F
Q
Z
E
R
H
Y
G
W
J
O
I
D
M
N
C
T
X
S
B
L
P
K

Fig. 8

	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2	1	13	18	8	22	23
A	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G	Y	H	R	E	Z	Q
B	S	X	T	C	N	M	D	I	O	J	W	G	Y	H	R	E	Z	Q	F	U	A	V	K
C	N	M	D	I	O	J	W	G	Y	H	R	E	Z	Q	F	U	A	V	K	P	L	B	S

Fig. 9

	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2	1	13	18	8	22	23
A	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G	Y	H	R	E	Z	Q
	2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3	3	4	12	13	26	»	»
B	S	X	T	C	N	M	D	I	O	J	W	G	Y	H	R	E	Z	Q	F	U	A	V	K
	12	»	17	6	14	6	8	13	16	1	3	3	4	12	13	26	»	»	4	6	16	2	2
C	N	M	D	I	O	J	W	G	Y	H	R	E	Z	Q	F	U	A	V	K	P	L	B	S
	14	6	8	14	16	1	3	3	4	12	13	26	»	»	4	6	16	2	2	4	7	3	12

Fig. 10

A——VKPLBSXTCNMDIOJWGYHREZQ | Break | VK PL BSXTCNMDI

B——————SXTCNMDIOJWGYHREZQ FUA VK | Break | SXTCNMDI

C——————————NMDIOJWGYHREZQ FUA VK PL BS | Break | NMDI

Fig. 11

	1	13	18	8	22	23	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2
U	G	Y	H	R	E	Z	A	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W
	3	4	12	13	26	»	16	2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3
A	Y	H	R	E	Z	A	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G
	4	12	13	26	»	16	2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3	3

Fig. 12

	1	13	18	8	22	23	Break	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2	1
U	G	Y	H	R	E	Z		A	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G
	3	4	12	13	26	»		16	2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3	3

	1	13	18	8	22	23	Break	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2
A	Y	H	R	E	Z	Q		V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G
	4	12	13	26	»	»		2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3	3

Fig. 13

	1	13	18	8	22	23	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2	1
U	G	Y	H	R	E	Z	A	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G
	3	4	12	13	26	»	16	2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3	3

	1	13	18	8	22	23	9	17	4	14	10	7	21	11	16	6	20	19	12	3	5	15	2
A	Y	H	R	E	Z	Q	V	K	P	L	B	S	X	T	C	N	M	D	I	O	J	W	G
	4	12	13	26	»	»	2	2	4	7	3	12	»	17	6	14	6	8	13	16	1	3	3

FIG. 14

(Total frequency 32, number of different letters 12, Average frequency 2,67)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3		1	1	6			2	3			1		3	3			2	2	5						

FIG. 15

A	1	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17	1
		2	1	2	2	1	1	2	1				1			2	2		1		2	2		

Y	5	1	1		4					2	2	2			2	6			2		7	2	
	1	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17

FIG. 16

5		2		6		4		5	1	2	6		2		4		5		4		5
5			5			4		5		2	6		2	6		4		2	4	5	

FIG. 17

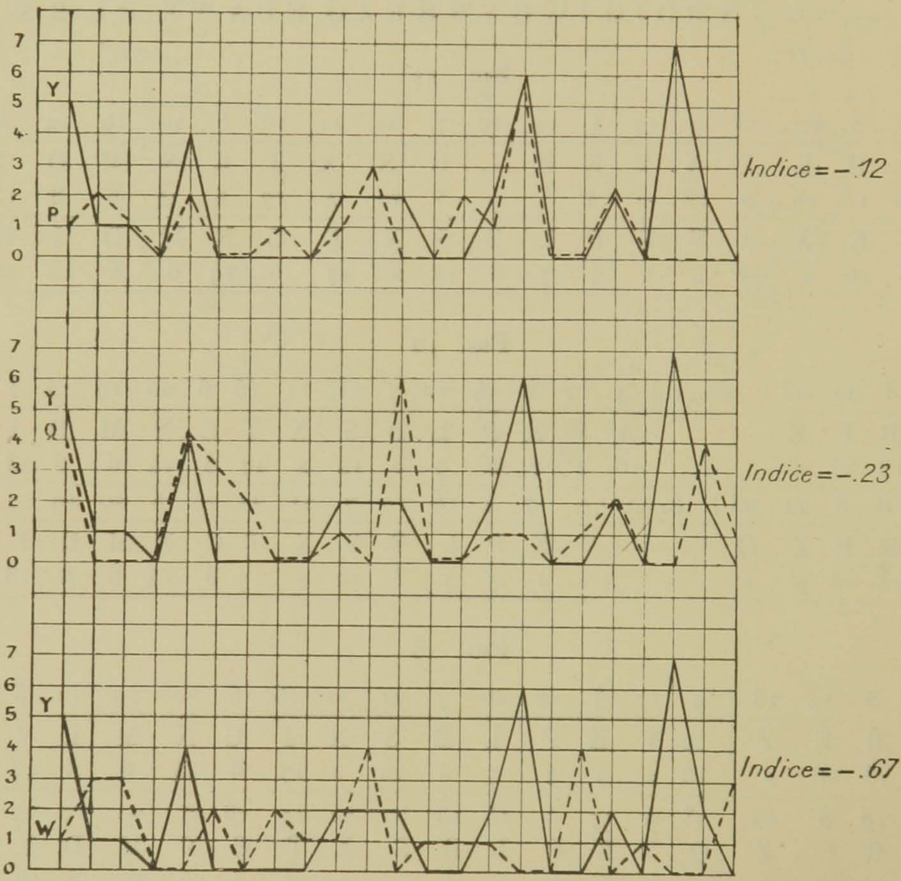


Fig. 18

A	$\frac{1}{}$	$\frac{8}{2}$	$\frac{12}{1}$	$\frac{16}{2}$	$\frac{20}{2}$	$\frac{2}{1}$	$\frac{22}{1}$	$\frac{15}{2}$	$\frac{6}{1}$	$\frac{11}{}$	$\frac{5}{}$	$\frac{19}{}$	$\frac{13}{1}$	$\frac{23}{}$	$\frac{9}{}$	$\frac{21}{2}$	$\frac{7}{2}$	$\frac{4}{}$	$\frac{14}{1}$	$\frac{10}{}$	$\frac{3}{2}$	$\frac{18}{2}$	$\frac{17}{}$	$\frac{1}{}$	$\frac{8}{2}$
Y			$\frac{5}{1}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{}{16}$	$\frac{4}{20}$	$\frac{}{2}$	$\frac{}{22}$	$\frac{}{15}$	$\frac{}{6}$	$\frac{2}{11}$	$\frac{2}{5}$	$\frac{2}{19}$	$\frac{}{13}$	$\frac{}{23}$	$\frac{2}{9}$	$\frac{6}{21}$	$\frac{}{7}$	$\frac{}{4}$	$\frac{2}{14}$	$\frac{}{10}$	$\frac{7}{3}$	$\frac{2}{18}$	$\frac{}{17}$

Fig. 19

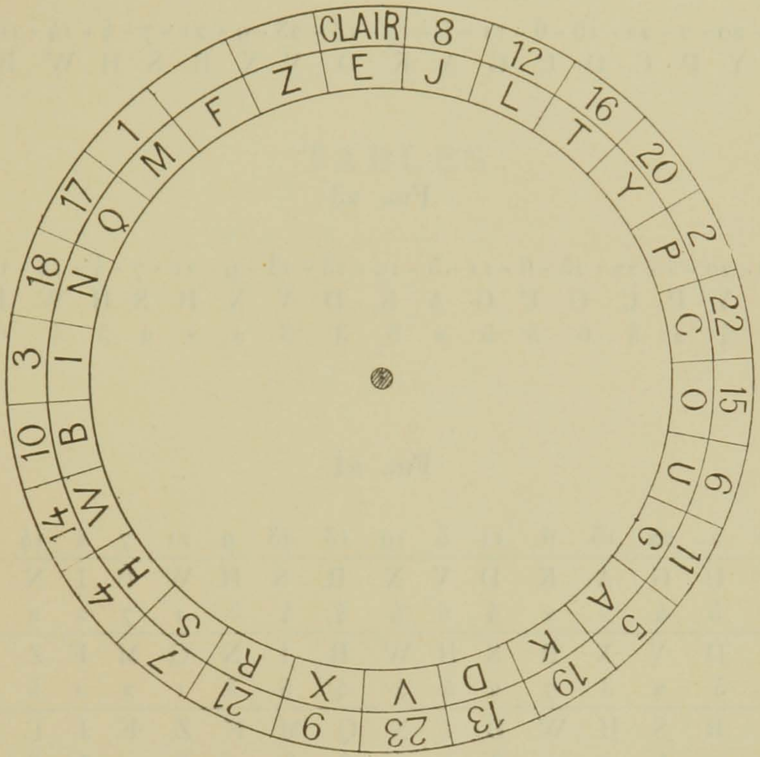


Fig. 20

	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17	1	[Break]
Y	1	1		4					2	2	2			2	6			2		7	2		5	

Fig. 21

	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17	1	[Break]
Y	1	1		4					2	2	2			2	6			2		7	2		5	
	T	L	J	E	Z	F	M	Q	N	I	B	W	H	S	R	X	V	D	K	A	G	U	O	

Fig. 22

$E_p =$	8 -	12 -	16 -	20 -	2 -	22 -	15 -	6 -	11 -	5 -	19 -	13 -	23 -	9 -	21 -	7 -	4 -	14 -	10 -	3 -	18 -	17 -	1
	J	L	T	Y	P	C	O	U	G	A	K	D	V	X	R	S	H	W	B	I	N	Q	M

Fig. 23

$E_p =$	8 -	12 -	16 -	20 -	2 -	22 -	15 -	6 -	11 -	5 -	19 -	13 -	23 -	9 -	21 -	7 -	4 -	14 -	10 -	3 -	18 -	17 -	1
	J	L	T	Y	P	C	O	U	G	A	K	D	V	X	R	S	H	W	B	I	N	Q	M
Frequencies	4	2	2	4	2	4	6	3	5	»	6	3	3	2	2	2	5	4	6	5	4	4	5

Fig. 24

	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17	1
T_p	Y	P	C	O	U	G	A	K	D	V	X	R	S	H	W	B	I	N	Q	M	F	Z	E
	1	2	1	6	5	4	2	2	4	6	4	4	4	5	1	7	2	2	2	2	3	6	1
O_p	U	G	A	K	D	V	X	R	S	H	W	B	I	N	Q	M	F	Z	E	J	L	T	Y
	3	6	2	5	5	2	3	7	2	4	4	4	5	3	1	2	2	5	2	1	6	»	5
A_p	K	D	V	X	R	S	H	W	B	I	N	Q	M	F	Z	E	J	L	T	Y	P	C	O
	»	2	4	6	2	4	1	2	3	2	1	6	3	2	5	2	3	5	4	7	»	3	3

TABLES

Table 1

Table of coincidence for the message 26

Lenght of Internal Period (letters)	Lenght of Internal Cycle (groups)	Coincidences	Correction Factor	Corrected Totals
100	20	39	0	39,0
105	21	45	1,05	47,3
110	22	47	1,10	51,7
115	23	60	1,15	69,0
120	24	36	1,20	43,2
125	25	33	1,25	41,3

Table 2

Coincidences when messages 1 and 24 are tested at various intervals with messages 3 and 26

Position in cycle	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Coincidences	59	49	86	40	53	39	55	60	59	47	55	45	61	64	53	54	46	58	50	48	52	40

Table 3

Coincidences when messages 2 and 25 are tested at various intervals with messages 3 and 26

Position in cycle	2	3	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Coincidences	45	49	58	57	62	61	99														

Table 4

Coincidences when message 4 is tested at various intervals with messages 3 and 26

Position in cycle	2	3	5	6	7	8	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Coincidences	34	35	38	36	16	33	27	23	19	24	28	24	24	21	19	25	20	42	35	32

Table 5

Secondary test for determining position of number 4 using messages 1-24 and 2-25 as the base

Position in cycle	2 -	3 -	5 -	6 -	8 -	21 -	22 -	23
Coincidences	32	18	24	12	16	55	16	28

TABLE 6

Data for determining the position of numbers in the External Cycle, Base messages 3 and 26

	1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	59	45	34	44	25	23	36	27	18	16	18	20	29	38	24	15	48	28	55	26	48	50
3	49	49	35	31	33	33	27	32	18	28	27	19	17	32	23	44	31	37	14	33	22	
4	86	58	38	33	37	26	53	26	15	10	56	15	32	37	47	30	26	66		47		
5	40	57	36	31	25	27		17	13	15		18	30	27								
6	53	62	16	33	40	25		21	23	14		18	18	24								
7	39	61	33	29	31	20		21	19	16		19	20	59								
8	55	99	27	26	20	24		30	14	15		16	23									
9	60		23	22	11	31		17	18	26		38	33									
10	59		19	16	66	31		13	13	17			24									
11	47		24	23		16		21	20	28			42									
12	55		28	49		19		27	10	20												
13	45		24			28		58	15	31												
14	61		24			28			18	19												
15	64		21			28			52													
16	53		19			46																
17	54		25																			
18	46		20																			
19	58		42																			
20	50		35																			
21	48		32																			
22	52																					
23	40																					

Secondary Tests, Base Messages 1-24, 2-25

Message 4		Message 5		Message 11	
2	32	2	22	3	21
3	18	14	58	13	30
5	24			16	22
6	12			19	16
8	16				
21	55				
22	16				
23	28				

			1		
	A	B	C	D	E
A			1	1	
B		4	1		3
C	1	4	3		
D	4				4
E	1	1		2	2
F				1	
G	3	1		5	1
H	3		1	1	
I			5	2	
J			1	2	2
K					5
L	1	1		4	
M	5	1	3	2	3
N	1	3	1	1	1
O	3	2	1	2	1
P		1	1		2
Q	1	2	1	1	1
R	1	1	2	2	1
S			1		1
T	1	1			2
U			1	4	
V	2	2	6	1	2
W	3	4	1		
X		1	2	2	3
Y	5			1	
Z	2	7	3		1

			8		
	A	B	C	D	E
A	2	1		2	3
B		2	1	1	1
C	1		2	1	1
D	2		3	1	4
E	2	2	1	4	5
F	1	2		2	2
G	1	3	1		1
H	1	1		1	
I					4
J	4		5	5	
K		3		1	
L					
M				1	
N	3	2	5	1	
O	2	2		1	
P	1	1		3	
Q	4	5		1	2
R		1			2
S	3	2	2	1	1
T	3		4	2	1
U	3	1	1	1	
V	1		2	5	1
W	1	5	5		
X		2	3	1	3
Y	1	1	1	1	4
Z					1

			12		
	A	B	C	D	E
A	1				1
B	3	1			8
C	2	1	5	3	
D	2	3		3	1
E	1	2		3	3
F				1	2
G	5	1		4	
H	2	6	5		
I		3		2	2
J	1	1	3		1
K		2	2	1	
L	2		5		1
M	3	4		2	3
N	1			1	
O	2				2
P	2	3	5		
Q		4		3	
R		1	3		1
S			1		2
T			3	3	
U	3	1			1
V				3	
W	3			1	2
X	1	1	1	6	2
Y	1	1			3
Z	1	2	3		1

Table 7^1. — Groups 1, 8, 12

			16		
	A	B	C	D	E
A	2		1		
B	4	2			1
C	1				
D	1	1			2
E	1	3		3	4
F	2		2		3
G		2	3		1
H	1	2		2	4
I	3	4	2		
J	I				
K	3				2
L	1	1		3	1
M	3	3		8	2
N			2		3
O		5	2	2	
P	1	1	4		
Q			4		1
R				1	1
S		2	1	2	
T	2		5	1	5
U	1	4			
V	4	1		4	1
W	3	1	3		2
X		1	4	4	1
Y		2	1		
Z			1	5	4

			20		
	A	B	C	D	E
A	2		1	4	3
B	1	2		1	1
C	1	1	1	1	
D	1		2	1	
E		3	3		
F	1	1	2	1	
G	1	1		1	1
H			9		3
I		1			6
J				2	1
K	5	1			4
L		4	4		2
M	1	1			
N		5	1	3	2
O	6	3	1	3	5
P				4	2
Q			1	4	
R	1	2	3	1	
S		5			1
T	1	1			
U		2			1
V		1		2	3
W			5	1	
X	6		2	2	
Y	4			3	
Z	4	1		1	

			2		
	A	B	C	D	E
A	1		2		2
B					1
C		3		5	
D	5		1		
E			2		1
F	1	5	1		
G		2	1		
H	3		1	1	
I	3		1	2	1
J		1	3	1	3
K	1		2	1	2
L	1	5	2		3
M				1	
N	1		1	4	2
O	2	4	1	2	3
P	2	4			
Q	4	1			7
R	2	1	3	1	3
S			1	2	1
T	1	1	1	4	
U	5			3	
V	2	1	1		2
W		2		1	
X	1	1	6	5	3
Y			4		1
Z	2	5	2	3	

TABLE 7². — Groups 16, 20, 2

	22					15					6				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
A	1	1	2			2	1	1			1	1	4		
B		2			1	2	3			2			1	1	
C	4	1	2		1			3	1	5	1	1			3
D	1	2	6	1		2					1	2	4		
E	3	4		8				1				1	1		
F		2		5		1		1	5		5	2		3	2
G	4				1	3	1		4	3		2	2	1	1
H		1		2	2	1	1						2		2
I		1		1	1		1	3	1	8	2				4
J		1	1		3	3	2		2		1			3	
K	1	1			4			3	1	2	2		2	1	1
L		3	3		4	4		1	3	2	3	7		1	
M	1	1	4	2	4	3	2	5	3	1	1	7		2	
N	3		1	5	1				4	1		1	1	4	1
O					1	6	2		1				5		3
P		6	3	1			2		2		1	1	1		
Q	3	1		2		2	4	4	3	1					1
R		1	1			2	.1	2		1	7	2		7	1
S	4		2	1			3	1			1		4	4	
T	2	1	1		3	1	5			2	2		1	2	3
U	3	2		1	4		1	3	1	1	3		8	1	
V	2		3			1	3		3	1	2	6		4	
W	2	1	1	2			1			2	2	1		1	7
X	1	2	2			3		1		2	2	1	1	1	5
Y		1	2	2	3		2		1	2					2
Z	1		1	2	2		1	7	1			2			

TABLE 7^3. — Groups 22, 15, 6

11

	A	B	C	D	E
A			2	3	
B	3	1	3	4	
C		4	2	1	4
D	4	1		2	
E	1	1	1	2	1
F	5		4		
G	5		1	3	
H	1	2	2		4
I		4	2		2
J	1	9	1		
K	1				1
L					2
M		1			3
N	3				
O			2		1
P		2			
Q		3	1	1	4
R	2		2	1	6
S	2	2	1	4	1
T	3				1
U				3	
V	1	3	5		1
W	1	2		8	1
X	1	1	1	2	2
Y	2	1	4		
Z	2		3	3	2

5

	A	B	C	D	E
A			1	2	2
B	1	1		3	
C				3	
D	3	1	1	1	
E	1	1	4	1	
F	1				
G		3	2	3	2
H	4	2			1
I	2	2		7	1
J	3	4	1	1	3
K			3	4	
L		2		1	
M	1	2	3		1
N			6		1
O				2	1
P	1	1	2		5
Q	1	3			6
R	1		3	1	
S	3		3	1	
T		7			
U	2	3	1		
V	6		1	4	5
W	1	1			1
X	1				2
Y	2	3		3	2
Z	2	1	6		3

19

	A	B	C	D	E
A		5	2	4	
B				1	
C	2	2	5	1	1
D		3	1		3
E	2	1		2	
F	1	5	3		
G		1		1	2
H	1	1		7	
I	2			1	1
J	2	1	2	2	1
K	6				2
L	1				1
M	1	2	4	2	
N	1		2	5	1
O		1	8	1	5
P	3	2	2	1	1
Q					2
R	3	1			2
S	1	1		2	3
T	1	5			
U			5	2	2
V		3	1	2	5
W	4			2	2
X	4	2	1		1
Y	2				
Z					1

Table 7^4. — Groups 11, 5, 19

	13				
	A	B	C	D	E
A	1	3	1		1
B	4		2	2	
C	2	4	1		
D	3		1	1	5
E		2	1	1	
F	1	1		2	
G			1		2
H	1	1	2	4	3
I	1	2		3	1
J	1				3
K		2	3	2	
L	3	1		1	
M		1	1	3	3
N	2	4		1	
O	2	2			4
P			2		1
Q	6		6	5	
R	4	1	1		2
S	1		4		1
T	2	2	4	4	3
U	1	1	2	4	1
V			3	2	2
W		5			
X	2			1	1
Y		2			2
Z		3	2	1	

	23				
	A	B	C	D	E
A				2	3
B	3	1		1	1
C				1	3
D		2	1	2	
E				3	
F	1	5	2		1
G			1	3	2
H		2	2	1	1
I	5	1	2	4	1
J		3	3	2	1
K	4	2	3	4	
L	3	1		1	2
M	3		1		
N				1	
O	4		2	1	2
P		6			1
Q		2	2		3
R	1	1		4	2
S	4	1	7		2
T	3	2	5		1
U	1		1		1
V	3	3		1	1
W	1	1	4	2	2
X		2		3	2
Y					3
Z		1			

	9				
	A	B	C	D	E
A				2	6
B		1	1		1
C	2			1	4
D			1		2
E			6		6
F	2	2			
G	6		1		1
H	5	5			1
I	1	1	3	4	2
J		2			
K	2	3	2	1	
L		1		3	
M			3		
N	3	2	3	4	
O	1	3		1	1
P	2		1	3	
Q		3		1	
R			4		2
S		2	1	6	
T	2	4	1	1	
U	5	4	1		
V			1	2	
W	1		4	3	4
X	2	1		2	1
Y	2	2	3	2	2
Z					3

TABLE 7^5. — Groups 13, 23, 9

21

	A	B	C	D	E
A	2	4		2	
B		1		5	1
C	1		2	4	
D	1				
E		3	2	1	3
F			1	2	2
G	5	1	1		
H	1	2			3
I		1	1		1
J	4	6	3		
K			2	1	2
L	1				1
M	1	1	3	1	
N	1	1			2
O	2	2	1	5	
P	1	2	1		4
Q	1		2	3	2
R	2	1	4	4	
S			2		1
T			1	2	
U		2	2	3	4
V	1	2			
W	1	2			3
X	1	1	7	4	2
Y	6		1		2
Z	5	5			4

7

	A	B	C	D	F
A	2	4		2	
B	7		1		5
C	1	2	2	4	
D			3		2
E	2	4	3	4	1
F	1	5			3
G	1		1	1	4
H			4		5
I			1	1	
J				3	1
K	4	2	1		2
L	2	1	2	1	1
M	2		3	5	
N	1	2		1	
O			1	1	2
P	6			3	3
Q	1	4	1	1	2
R	1		1		
S	2	1			
T	1	3	2		
U	1	1	7	1	1
V				1	
W		1	1	1	2
X	3	2	3		1
Z				2	1
Y		6		4	

4

	A	B	C	D	E
A		4	2		
B	1	2	4	1	9
C	3	1	2		2
D	2	1		6	4
E			3	1	1
F	2	3	2		
G	1	3			
H	5	2	1	3	2
I	2		2	1	
J	3	5	2	1	2
K	5	1			1
L			2		
M	1	5		6	
N				1	2
O	2	2			3
P		1	1	2	1
Q		1	3		1
R	1				
S	2			2	2
T		1	2	1	2
U	3	1	3	3	2
V	1	1		5	
W		1	1		1
X					
Y			5	3	1
Z	2	1	1		

Table 7^6. — Groups 21, 7, 4

14	A	B	C	D	E
A	1		3	2	3
B		2	1	3	3
C			1	1	
D	2		1	1	1
E	1	3		3	
F		1			2
G	1	3	1	1	1
H			5	1	
I	2		2		2
J		1	2	2	1
K	1	4	1	6	3
L	5			1	
M	1	1	3	1	
N	2	1	1	3	2
O	1		1		1
P		1	4	1	
Q	1			1	2
R		2	5		
S	2	5	1	1	2
T	1	6			
U		4			5
W	5		1	1	2
V	4	1	1	1	1
X			1	4	
Y	2				
Z	5			1	4

10	A	B	C	D	E
A		2			4
B	6			1	
C	1		4	1	
D		2	3	4	
E	2	1		1	2
F			1	6	
G	3				5
H			1		
I			1	3	
J		1	1		2
K	1		1	3	3
L		3			6
M					
N	1	1	1		
O		1	1		
P	2		2		4
Q	2	2	3		1
R		4		2	
S	2	5			
T	4		1		
U	2	1	3	1	3
V	5		5	2	
W		3	1	7	4
X	3	5	2		
Y		1	1		
Z	2	3	3	4	1

3	A	B	C	D	E
A	2		3	1	2
B					
C			2		4
D		1		1	1
E	2	2		2	4
F	1	4			5
G			3	3	4
H	4		7	3	
I	5	5			1
J	1	2	2		2
K		2	1	4	1
L		4	1		2
M	2		4	1	
N		2	2	1	
O	1			3	
P			1	1	
Q			2		
R	4	2	1	1	
S				1	
T	1	1		4	3
U		3	1		6
V	1	2			
W	1	1	1	3	1
X	4	4		2	
Y	7		2	4	
Z		1	3	1	

TABLE 7^7. — Groups 14, 10, 3

	18				
	A	B	C	D	E
A	2	2	2	1	
B	1	6	1	1	2
C	1			1	3
D	1	1			1
E				5	1
F	3		2	7	5
G	1	1	3		3
H		2	3		2
I		2	3	2	
J	1	3	3	6	
K	3	2		3	2
L	6		1		
M	2	1	2		2
N	4		1	2	
O	1	1		1	
P		2	1		
Q			1		1
R	4				
S	1	2		4	3
T			4		2
U	1		6		1
V	1				
W		1		2	1
X	2	1			
Y	2	6	4		
Z		5		1	7

	17				
	A	B	C	D	E
A			1		4
B	1	3	3	3	3
C	3			1	3
D	4	3	4		1
E	1	3	1		1
F	1	1	3	1	1
G		2			1
H	2	1			1
I	1			2	3
J	1	1	1	3	1
K	1		1		
L	1				1
M		2	2	9	
N	1	4	3	1	1
O		3		2	3
P			1		3
Q	4		1	1	
R		2	2		
S	4		8		
T			1	1	1
U	3	6		5	1
V	2	2		5	2
W			2		1
X	1	1			1
Y		3	2	2	
Z	6				2

TABLE 7^8. — Groups 18, 17

Table 8

Consolidated frequency Table of 1st position letters or A Alphabet

	1	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17	Total Frequency	Number of segments occupied	Average Frequency per segment
A		2	1	2	2	1	1	2	1				1			2	2		1		2	2		22	14	1.58
B			3	4	1			2		3	1		4	3			7	1		6		1	1	37	13	2.85
C	1	1	2	1	1		4		1			2	2		2	1	1	3		1		1	3	27	16	1.69
D	4	2	2	1	1	5	1	2	1	4	3	3	3			1		2	2			1	4	39	17	2.30
E	1	2	1	1			3			1	1	2					2		1	2	2		1	20	13	1.54
F		1		2	1	1		1	5	5	1	1	1	1	2		1	2			1	3	1	30	17	1.76
G	3	1	5		1		4	3		5					6	5	1	1	1	3		1		40	14	2.86
H	3	1	2	1		3		1		1	4	1	1		5	1		5			4		2	35	15	2.34
I				3		3			2		2	2	1	5	1			2	2		5		1	29	12	2.42
J		4	1	1				3	1	1	3	2	1			4		3			1	1	1	27	14	1.93
K				3	5	1	1		2	1		6		4	2		4	5	1	1		3	1	40	15	2.67
L	1		2	1		1		4	3			1	3	3		1	2		5			6	1	34	14	2.43
M	5		3	3	1		1	3	1		1	1		3		1	2	1	1		2	2		31	16	1.94
N	1	3	1			1	3			3		1	2		3	1	1		2	1		4	1	28	15	1.86
O	3	2	2		6	2		6					2	4	1	2		2	1		1	1		35	14	2.50
P		1	2	1		2			1		1	3			2	1	6			2				22	11	2.00
Q	1	4				4	3	2			1		6			1	1		1	2			4	30	12	2.50
R	1			2	1	2		2	7	2	1	3	4	1		2	1	1			4	4		38	16	2.37
S		3					4		1	2	3	1	1	4			2	2	2	2		1	4	32	14	2.28
T	1	3		2	1	1	2	1	2	3		1	2	3	2		1		1	4	1			31	17	1.82
U		3	3	1		5	3		3		2		1	1	5		1	3		2		1	3	37	15	2.47
V	2	1		4		2	2	1	2		6			3		1		1	5	5	1	1	2	39	16	2.45
W	3	1	3	3			2		2	1	1	4		1	1	1			4		1			28	14	2.00
X			1		6	1	1	3	2	1	1	4	2		2	1	3			3	4	2	1	38	17	2.24
Y	5	1	1		4					2	2	2			2	6			2		7	2		36	12	3.00
Z	2		1		4	2	1			2	2					5		2	5	2			6	34	12	2.83

Total number of letters 841

Table 9

A	2	1	2	2	1	1	2	1				1			2	2		1		2	2	
Y	5	1	1		4					2	2	2			2	6			2		7	2
Coincidences -	2	1	1	0	1	0	0	0	0	0	0	1	0	0	2	2	0	0	0	0	2	0	= 12

Table 10

																						Totals
A	2	1	2	2	1	1	2	1				1			2	2		1		2	2	
Y	5	1	1		4					2	2	2			2	6			2		7	2
Coincidences -	2	1	1	0	1	0	0	0	0	0	0	1	0	0	2	2	0	0	0	0	2	0	= 12
Non-coincidences -	3	0	1	2	3	1	2	1	0	2	2	1	0	0	0	4	0	1	2	2	5	2	= 34
Number of letters -	7	2	3	2	5	1	2	1	0	2	2	3	0	0	4	8	0	1	2	2	9	2	= 58

Table 11

	Frequencies	Coincidences	Differences	Indices of coincidence
A	58	12	-22	-.38
B	73	16	-27	-.37
C	63	13	-24	-.38
D	75	16	-27	-.36
E	56	12	-20	-.36
F	66	11	-33	-.50
G	76	8	-52	-.69
H	71	13	-32	-.45
I	65	10	-35	-.54
J	63	15	-18	-.29
K	76	13	-37	-.49
L	70	16	-22	-.28
M	67	9	-40	-.60
N	64	16	-16	-.24
O	71	10	-41	-.58
P	58	17	- 7	-.12
Q	66	17	-15	-.23
R	74	15	-29	-.34
S	68	14	-26	-.38
T	67	11	-34	-.51
U	74	18	-20	-.27
V	75	12	-39	-.52
W	64	7	-43	-.67
X	74	16	-26	-.35
Z	70	11	-37	-.53

Table 12

	Frequencies	Coincidences	Differences	Indices of coincidence
A	44	11	-11	-.25
B	59	10	-29	-.49
C	49	13	-10	-.20
D	61	11	-28	-.46
E	42	9	-15	-.36
F	52	10	-22	-.42
G	62	9	-35	-.57
H	57	13	-18	-.32
I	51	8	-27	-.53
J	49	11	-16	-.36
K	62	12	-26	-.42
L	56	8	-32	-.57
M	53	11	-20	-.38
N	50	9	-23	-.46
O	57	9	-30	-.53
Q	52	7	-31	-.60
R	60	14	-18	-.30
S	54	8	-30	-.56
T	53	11	-20	-.38
U	60	9	-33	-.55
V	61	7	-40	-.65
W	50	8	-26	-.52
X	60	11	-27	-.45
Z	56	8	-32	-.57

Table 12a

	Frequencies	Coincidences	Differences	Indices of coincidence
A	58	9	-31	-.55
C	63	20	- 3	-.05
E	56	13	-17	-.30
H	71	16	-23	-.32
J	63	10	-33	-.52
M	67	14	-25	-.37
R	74	11	-41	-.55
T	67	13	-28	-.42

Table 13

C

	1	2	3	4
A	49	14	-7	-.14
B	64	14	-22	-.34
D	66	18	-12	-.18
E	47	9	-20	-.43
F	57	13	-18	-.32
G	67	15	-22	-.33
H	62	14	-20	-.32
I	56	11	-23	-.41
J	54	13	-15	-.28
K	67	11	-34	-.51
L	61	18	- 7	-.11
M	58	17	- 7	-.12
N	55	12	-19	-.35
O	62	20	+ 2	+.03
Q	57	11	-24	-.42
R	65	16	-17	-.26
S	59	10	-29	-.49
T	58	15	-13	-.22
U	65	9	-38	-.58
V	66	16	-18	-.27
W	55	14	-13	-.24
X	65	13	-26	-.40
Z	61	13	-22	-.36

O

	1	2	3	4
A	58	13	-19	-.33
B	72	11	-39	-.54
D	74	17	-23	-.31
E	55	11	-22	-.40
F	65	15	-20	-.31
G	75	13	-36	-.48
H	70	13	-31	-.44
I	64	13	-25	-.39
J	62	9	-35	-.57
K	75	16	-27	-.36
L	69	16	-21	-.30
M	66	12	-30	-.46
N	63	17	-12	-.19
Q	65	14	-23	-.35
R	73	14	-31	-.43
S	67	15	-22	-.33
T	66	17	-15	-.23
U	73	25	+ 2	+.03
V	74	17	-23	-.31
W	64	14	-22	-.34
X	73	13	-34	-.47
Z	69	9	-42	-.61

U

	1	2	3	4
A	59	12	-23	-.39
B	74	15	-29	-.39
D	76	15	-31	-.41
E	57	13	-18	-.32
F	67	13	-28	-.42
G	78	25	- 3	-.03
H	72	15	-27	-.38
I	66	13	-27	-.41
J	64	15	-19	-.30
K	77	13	-38	-.49
L	71	14	-29	-.41
M	68	19	-11	-.16
N	65	14	-23	-.35
Q	67	9	-40	-.60
R	75	16	-27	-.36
S	69	12	-33	-.48
T	68	15	-23	-.34
V	76	16	-28	-.37
W	65	21	- 2	-.03
X	75	14	-33	-.44
Z	71	17	-20	-.28
O at 2 intervals.				
G	75	26	+ 3	+.04
W	63	12	-27	-.43

G

	1	2	3	4
A	62	16	-14	-.23
B	77	16	-29	-.38
D	79	15	-34	-.43
E	60	12	-24	-.40
F	70	13	-31	-.44
H	75	15	-30	-.40
I	69	14	-27	-.39
J	67	19	-10	-.15
K	80	14	-38	-.48
L	74	15	-29	-.39
M	71	16	-23	-.32
N	68	10	-38	-.56
Q	70	12	-34	-.49
R	78	16	-30	-.39
S	72	13	-33	-.46
T	71	13	-32	-.45
V	79	20	-19	-.24
W	68	11	-35	-.52
X	78	17	-27	-.35
Z	74	8	-50	-.68
U at 2 intervals.				
A	59	17	- 8	-.14
J	64	14	-22	-.34
V	76	18	-22	-.29

A

	1	2	3	4
B	59	13	-20	-.34
D	61	15	-16	-.26
E	42	8	-18	-.43
F	52	14	-10	-.19
H	57	11	-24	-.42
I	51	9	-24	-.47
J	49	9	-22	-.45
K	62	17	-11	-.18
L	56	13	-17	-.30
M	53	12	-17	-.32
N	50	9	-23	-.46
Q	52	8	-28	-.54
R	60	13	-21	-.35
S	54	12	-18	-.33
T	53	11	-20	-.38
V	61	13	-22	-.36
W	50	8	-26	-.52
X	60	15	-15	-.25
Z	56	12	-20	-.36
G at 2 intervals.				
D	79	14	-37	-.47
F	70	17	-19	-.27
K	80	29	+ 7	+.09
X	78	21	— 15	— .19

K

	1	2	3	4
B	77	11	-44	-.57
D	79	23	-10	-.13
E	60	8	-36	-.60
F	70	13	-31	-.44
H	75	20	-15	-.20
I	69	12	-33	-.48
J	67	11	-34	-.51
L	74	13	-35	-.47
M	71	9	-53	-.75
N	68	15	-23	-.34
Q	70	20	-10	-.14
R	78	16	-38	-.49
S	72	13	-33	-.46
T	71	14	-29	-.41
V	79	17	-28	-.35
W	68	11	-35	-.51
X	78	16	-30	-.39
Z	74	23	- 5	-.07
A at 2 intervals.				
D	61	15	-16	-.26
H	74	11	-41	-.55
Q	69	8	-45	-.65
Z	73	12	-37	-.50
G à 3 intervals				
D	79	28	+ 5	+.06
Z	74	18	-20	-.27

Table 13

D

	1	2	3	4
B	76	15	-31	-.41
E	59	17	- 8	-.14
F	69	13	-30	-.44
H	74	16	-26	-.38
I	68	15	-23	-.34
J	66	15	-21	-.32
L	73	16	-25	-.34
M	70	19	-13	-.19
N	67	16	-19	-.28
Q	69	16	-21	-.30
R	77	17	-26	-.34
S	71	22	- 5	-.07
T	70	22	- 4	-.06
V	78	24	- 6	-.08
W	67	20	- 7	-.10
X	77	16	-29	-.38
Z	73	14	-31	-.43

K at 2 intervals.

E	60	13	-21	-.35
S	72	20	-12	-.17
T	71	18	-17	-.24
V	79	28	+ 5	-.06
W	68	16	-20	-.30

R

	1	2	3	4
B	75	16	-27	-.36
E	58	10	-28	-.48
F	68	21	- 3	-.04
H	73	11	-40	-.55
I	67	15	-22	-.33
J	65	10	-25	-.39
L	72	18	-18	-.25
M	69	14	-27	-.39
N	66	18	-12	-.18
Q	68	14	-26	-.38
S	70	23	- 1	-.01
T	69	19	-12	-.17
W	66	10	-36	-.55
Z	72	14	-30	-.42

V

	1	2	3	4
B	76	14	-34	-.45
E	59	16	-11	-.19
F	69	13	-30	-.44
H	74	15	-29	-.39
I	68	11	-35	-.52
J	66	12	-30	-.45
L	73	10	-43	-.59
M	70	13	-31	-.44
N	67	17	-16	-.24
Q	69	12	-33	-.48
R	77	16	-29	-.38
S	71	14	-29	-.41
T	70	20	-10	-.14
W	67	15	-12	-.19
X	77	26	+ 1	+ .01
Z	73	13	-34	-.47

S

	1	2	3	4
B	69	13	-30	-.44
E	52	12	-16	-.31
F	62	12	-26	-.42
H	67	20	- 7	-.10
I	61	14	-19	-.31
J	59	14	-17	-.29
L	66	13	-27	-.41
M	63	17	-12	-.19
N	60	12	-24	-.40
Q	62	99	-35	-.57
T	63	12	-27	-.43
W	60	16	-12	-.20
Z	66	13	-27	-.41

R at 2 intervals.

H	73	23	- 4	-.06
M	69	16	-21	-.30
W	66	13	-27	-.41

W

	1	2	3	4
B	65	20	- 5	-.08
E	48	10	-18	-.38
F	58	13	-19	-.33
I	57	7	-36	-.63
J	55	13	-16	-.29
L	62	11	-29	-.47
M	59	12	-23	-.39
N	56	14	-14	-.25
Q	58	14	-16	-.28
T	59	18	- 5	-.09
Z	62	10	-32	-.52

H at 2 intervals.

B	72	25	+ 3	+.04
T	66	17	-15	-.23

X

	1	2	3	4
B	75	15	-30	-.40
E	58	11	-25	-.43
F	68	20	- 8	-.12
H	73	19	-16	-.22
I	67	17	-16	-.24
J	65	15	-20	-.31
L	72	20	-12	-.17
M	69	16	-21	-.30
N	66	15	-21	-.32
Q	68	16	-20	-.29
R	76	28	+ 8	+.11
S	70	15	-25	-.36
T	69	16	-21	-.30
W	66	11	-33	-.50
Z	72	13	-33	-.46

V at 2 intervals.

F	69	15	-24	-.35
L	73	19	-16	-.22
R	77	26	+ 1	+.01

H

	1	2	3	4
B	72	9	-45	-.63
E	55	14	-13	-.24
F	65	14	-23	-.35
I	64	10	-34	-.53
J	62	15	·17	-.27
L	69	18	-15	-.22
M	66	15	-21	-.32
N	63	17	-12	-.18
Q	65	12	-29	-.45
T	66	15	-21	-.32
W	63	20	- 3	-.05
Z	69	16	-21	-.30

B

	1	2	3	4
E	57	8	-33	-.58
F	67	15	-22	-.33
I	66	23	+ 3	+.05
J	64	12	-28	-.44
L	71	11	-38	-.54
M	68	15	-23	-.34
N	65	8	-41	-.63
Q	67	5	-52	-.78
T	69	14	-27	-.39
Z	71	11	-38	-.54

Table 13

I

	1	2	3	4
E	49	10	-19	-.39
F	59	11	-26	-.44
J	56	6	-38	-.68
L	63	13	-24	-.38
M	60	9	-33	-.55
N	57	20	+ 3	+.05
Q	59	10	-29	-.49
T	61	15	-16	-.26
Z	63	12	-27	-.43

N

	1	2	3	4
E	48	11	-15	-.31
F	58	10	-28	-.48
J	55	15	-10	-.18
L	62	13	-23	-.37
M	59	16	-11	-.19
Q	58	14	-16	-.28
T	60	13	-21	-.35
Z	62	14	-20	-.32

I at 2 intervals.

J	56	13	-17	-.30
M	60	10	-30	-.50
Q	59	17	- 8	-.14

Q

	1	2	3	4
E	50	11	-17	-.34
F	60	9	-33	-.55
J	57	9	-30	-.53
L	64	13	-25	-.39
M	61	20	- 1	-.02
T	62	14	-20	-.32
Z	64	6	-46	-.72

M

	1	2	3	4
E	51	10	-21	-.41
F	61	20	- 1	-.02
J	60	14	-16	-.27
L	64	13	-26	-.40
T	62	18	- 9	-.14
Z	64	11	-32	-.49

F

	1	2	3	4
E	50	8	-26	-.52
J	60	13	-21	-.35
L	64	12	-28	-.44
T	62	13	-23	-.37
Z	64	18	+ 8	-.13

Z

	1	2	3	4
E	54	16	- 6	-.11
J	64	9	-37	-.58
L	68	9	-41	-.60
T	66	16	- 8	-.12

F at 2 intervals.

E	50	14	- 8	-.16
T	61	15	-16	-.26

M at 3 intervals.

E	51	16	- 3	-.06
T	62	18	- 8	-.13

E

	1	2	3	4
J	47	13	- 8	-.17
L	61	12	-25	-.41
T	59	9	-32	-.54

J

	1	2	3	4
L	61	18	- 7	-.11
T	58	12	-22	-.38

L

	1	2	3	4
T	65	22	+ 1	+.02

Table 14

Consolidated frequency Table of 3rd position letters or C Alphabet.

	8	12	16	20	2	22	15	6	11	5	19	13	23	9	21	7	4	14	10	3	18	17	1	Total Frequency	Number of segments occupied	Average Frequency per segment
A			1	1	2	2	1	4	2	1	2	1					2	3		3	2	1	1	29	16	1.81
B	1							1	3			2		1		1	4	1			1	3	.1	19	11	1.72
C	2	5		1		2	3		2		5	1			2	2	2	1	4	2			3	37	15	2.46
D	3			2	1	6		4		1	1	1	1	1		3		1	3			4		32	14	2.28
E	1			3	2		1	1	1	4		1		6	2	3	3					1		29	13	2.23
F			2	2	1		1		4		3		2		1		2		1		2	3		24	12	2.00
G	1		3		1			2	1	2		1	1	1	1	1		1		3	3			22	14	1.57
H		5		9	1			2	2			2	2	3		4	1	5	1	7	3		1	48	15	3.20
I			2		1		3		2				2		1	1	2	2	1		3		5	25	12	2.08
J	5	3			3	1			1	1	2		3		3		2	2	1	2	3	1	1	34	16	2.12
K		2			2		3	2		3		3	3	2	2	1		1	1	1		1		27	14	1.92
L		5		4	2	3	1									2	2			1	1			21	9	2.33
M						4	5			3	4	1	1	3	3	3		3		4	2	2	3	41	14	2.92
N	5		2	1	1	1		1		6	2			3				1	1	2	1	3	1	31	15	2.07
O			2	1	1			5	2		8		2		1	1		1	1				1	26	12	2.17
P		5	4			3		1		2	2	2		1	1		1	4	2	1	1	1	1	32	16	2.00
Q			4	1			4		1			6	2		2	1	3		3	2	1	1	1	32	14	2.28
R		3		3	3	1	2		2	3		1		4	4	1		5		1		2	2	37	15	2.46
S	2	1	1		1	2	1	4	1	3		4	7	1	2			1				8	1	40	16	2.50
T	4	3	5		1	1		1				4	5	1	1	2	2		1		4	1		36	15	2.40
U	1						3	8		1	5	2	1	1	2	7	3	3	1	6			1	45	15	3.00
V	2				1	3			5	1	1	3		1			1	5					6	29	11	2.64
W	5		3	5		1							4	4		1	1	1	1	1		2	1	30	13	2.31
X	3	1	4	2	6	2	1	1	1		1				7	3		1	2				2	37	15	2.46
Y	1		1		4	2			4					3	1		5		1	2	4	2		30	12	2.50
Z		3	1		2	1	7		3	6		2					1		3	3			3	35	12	2.91
Total number of letters																								828		

Table 15

		H		
	1	2	3	4
A	76	14	-34	-.45
B	65	12	-29	-.45
C	82	13	-43	-.52
D	76	12	-40	-.53
E	75	13	-36	-.48
F	71	16	-23	-.33
G	68	15	-23	-.34
I	72	15	-16	-.22
J	76	20	-16	-.21
K	74	14	-32	-.43
L	68	7	-47	-.69
M	88	15	-43	-.49
N	73	15	-28	-.38
O	73	10	-43	-.59
P	79	16	-31	-.39
Q	79	18	-25	-.32
R	84	17	-33	-.39
S	85	15	-40	-.47
T	79	19	-22	-.28
U	91	18	-37	-.41
V	74	12	-38	-.51
W	72	14	-30	-.42
X	81	18	-27	-.33
Y	76	23	- 7	-.09
Z	82	13	-43	-.53

		U		
	1	2	3	4
A	73	17	-22	-.30
B	63	17	-12	-.19
C	79	13	-40	-.51
D	73	14	-31	-.43
E	72	11	-39	-.54
F	68	14	-26	-.38
G	65	13	-26	-.40
I	69	11	-36	-.52
J	73	14	-31	-.43
K	71	14	-29	-.41
L	65	7	-44	-.68
N	70	10	-40	-.57
O	70	10	-40	-.57
P	76	14	-34	-.45
Q	76	17	-25	-.33
R	81	13	-42	-.52
S	82	20	-22	-.27
T	76	16	-28	-.37
V	71	11	-38	-.54
W	69	9	-42	-.61
X	78	8	-54	-.69
Z	79	10	-49	-.62

M at 2 intervals.

A	65	17	-14	-.22
B	54	16	- 6	-.11
S	74	20	-14	-.19

		Y		
	1	2	3	4
A	59	12	-23	-.39
B	48	7	-27	-.56
C	65	13	-26	-.40
D	59	12	-23	-.39
E	58	10	-28	-.48
F	54	8	-30	-.56
G	51	8	-27	-.53
I	55	10	-25	-.46
J	59	13	-20	-.34
K	57	12	-21	-.37
L	51	9	-24	-.47
M	71	23	- 2	-.03
N	56	13	-17	-.30
O	56	5	-41	-.73
P	62	15	-17	-.28
Q	62	10	-32	-.52
R	67	22	- 1	-.02
S	68	15	-23	-.34
T	62	7	-41	-.66
U	74	10	-44	-.60
V	57	7	-36	-.63
W	55	8	-31	-.56
X	57	12	-21	-.37
Z	65	11	-32	-.49

H at 2 intervals.

M	88	29	- 1	-.01
R	81	20	-21	-.26

		B		
	1	2	3	4
A	47	8	-23	-.49
C	53	9	-26	-.49
D	47	5	-32	-.68
E	46	7	-25	-.54
F	42	7	-21	-.50
G	39	6	-21	-.54
I	43	11	-10	-.23
J	47	12	-11	-.23
K	45	10	-15	-.33
L	39	2	-33	-.85
N	44	7	-23	-.52
O	46	7	-25	-.54
P	50	12	-14	-.28
Q	50	8	-26	-.52
R	55	13	-16	-.29
S	56	11	-23	-.41
T	50	7	-29	-.58
V	45	7	-24	.-53
W	43	7	-22	-.51
X	52	7	-31	-.60
Z	53	10	-23	-.43

U at 2 intervals.

I	69	21	- 6	-.09
J	73	16	-25	-.34
K	71	14	-29	-.41
P	76	16	-28	-.37
R	81	18	-27	-.38

		M		
	1	2	3	4
A	67	14	-25	-.37
B	56	12	-20	-.36
C	73	17	-22	-.30
D	68	16	-20	-.29
E	66	13	-27	-.41
F	62	13	-23	-.37
G	59	10	-29	-.49
I	63	14	-21	-.33
J	67	14	-25	-.37
K	65	15	-20	-.31
L	59	6	-41	-.70
N	64	9	-37	-.58
O	64	13	-25	-.39
P	70	13	-31	-.44
Q	70	21	- 7	-.10
R	75	12	-39	-.52
S	76	16	-28	-.37
T	70	21	- 7	-.10
U	82	31	+11	+.13
V	65	10	-35	-.54
W	62	8	-38	-.61
X	65	13	-26	-.40
Z	73	12	-37	-.51

		I		
	1	2	3	4
A	49	11	-16	-.33
C	55	8	-31	-.56
D	49	15	- 4	-.08
E	48	10	-18	-.38
F	44	7	-23	-.52
G	41	8	-17	-.42
J	49	8	-25	-.51
K	47	11	-14	-.30
L	41	6	-23	-.56
N	46	13	- 7	-.15
O	46	7	-25	-.54
P	52	12	-16	-.31
Q	52	7	-31	-.60
R	57	13	-18	-.32
S	58	11	-25	-.43
T	52	7	-31	-.60
V	47	6	-29	-.62
W	45	12	- 9	-.20
X	54	8	-30	-.56
Z	55	7	-34	-.62

B at 2 intervals.

D	47	8	-23	-.49
K	45	7	-24	-.53
N	44	10	-14	-.32
W	43	8	-19	-.44

U at 3 intervals.

D	73	13	-34	-.47
K	71	13	-32	-.45
N	70	16	-22	-.32
W	69	13	-30	-.44

Table 15

N

	1	2	3	4
A	59	13	-20	-.34
C	65	22	+ 1	+.02
D	59	8	-35	-.59
E	58	9	-31	-.53
F	54	13	-15	-.28
G	51	7	-30	-.59
J	59	16	-11	-.19
K	57	11	-24	-.42
L	51	12	-15	-.30
O	56	12	-20	-.36
P	62	16	-14	-.23
Q	62	12	-26	-.42
R	67	17	-16	-.24
S	68	11	-35	-.52
T	62	12	-26	-.42
V	57	10	-27	-.47
W	55	7	-34	-.62
X	64	14	-22	-.34
Z	65	14	-23	-.35

C

	1	2	3	4
A	63	17	-12	-.19
D	63	11	-30	-.48
E	62	10	-32	-.52
F	58	10	-28	-.49
G	55	17	- 4	-.07
J	68	14	-26	-.38
K	61	17	-10	-.16
L	55	10	-25	-.46
O	60	9	-33	-.55
P	66	17	-15	-.23
Q	66	19	- 9	-.14
R	71	12	-35	-.49
S	72	15	-27	-.38
T	66	21	- 3	-.05
V	61	7	-40	-.66
W	59	9	-32	-.54
X	68	12	-32	-.47
Z	69	15	-24	-.35

T

	1	2	3	4
A	65	11	-32	-.49
D	65	11	-32	-.49
E	64	15	-19	-.30
F	60	14	-18	-.30
G	57	10	-27	-.47
J	65	16	-17	-.26
K	63	13	-24	-.38
L	57	14	-15	-.26
O	62	10	-32	-.52
P	68	16	-20	-.30
Q	68	15	-23	-.34
R	73	21	-10	-.14
S	74	17	-23	-.31
V	63	5	-48	-.76
W	61	24	+11	+.18
X	70	15	-25	-.36
Z	71	10	-41	-.58

W

	1	2	3	4
A	58	9	-31	-.54
D	58	6	-40	-.69
E	57	13	-18	-.32
F	53	8	-29	-.55
G	50	6	-32	-.64
J	58	15	-13	-.22
K	56	12	-20	-.36
L	50	14	- 8	-.16
O	55	6	-37	-.67
P	61	13	-22	-.36
Q	61	9	-34	-.56
R	66	22	- 0	-.00
S	67	8	-43	-.64
V	56	6	-38	-.68
X	63	17	-12	-.19
Z	64	11	-31	-.48

R

	1	2	3	4
A	64	14	-24	-.38
D	64	15	-19	-.30
E	63	12	-27	-.43
F	59	12	-23	-.39
G	56	12	-20	-.36
J	64	15	-19	-.30
K	65	12	-29	-.45
L	56	10	-26	-.47
O	61	13	-22	-.36
P	67	17	-16	-.24
Q	67	13	-28	-.42
S	73	13	-34	-.47
V	62	13	-23	-.37
X	69	22	- 3	-.04
Z	70	12	-34	-.49

X

	1	2	3	4
A	64	17	-13	-.20
D	64	16	-16	-.25
E	63	16	-15	-.24
F	59	9	-26	-.44
G	56	9	-29	-.52
J	64	13	-25	-.39
K	65	12	-29	-.45
L	56	18	- 2	-.04
O	61	7	-40	-.66
P	67	13	-28	-.42
Q	67	13	-28	-.42
S	73	10	-43	-.59
V	62	8	-38	-.62
Z	70	16	-22	-.31

Table 15

L

	1	2	3	4
A	50	13	-11	-.21
D	50	6	-32	-.64
E	49	7	-28	-.57
F	45	8	-21	-.47
G	42	6	-24	-.64
J	50	10	-20	-.40
K	48	8	-24	-.50
O	47	5	-32	-.68
P	53	12	-17	-.32
Q	53	11	-20	-.38
S	59	8	-35	-.59
V	48	4	-36	-.75
Z	56	8	-32	-.57

Z

	1	2	3	4
E	56	6	-28	-.50
F	52	11	-19	-.37
G	49	15	- 4	-.08
J	57	12	-21	-.37
K	55	10	-25	-.46
O	54	17	- 3	-.06
P	60	13	-21	-.35
Q	60	10	-30	-.50
S	66	14	-24	-.36
V	55	5	-40	-.73

D at 2 intervals.

G	53	17	- 2	-.04
O	58	11	-25	-.43

S

	1	2	3	4
E	67	14	-25	-.37
J	68	13	-29	-.43
K	66	14	-24	-.37
O	65	14	-23	-.35
P	71	12	-35	-.49
Q	71	11	-38	-.54
V	66	15	-21	-.32

O

	1	2	3	4
E	54	11	-21	-.39
J	55	7	-34	-.62
P	58	9	-31	-.53
Q	58	12	-22	-.38

F at 5 intervals.

E	46	13	- 7	-.15
Q	49	4	-37	-.75

A

	1	2	3	4
D	57	15	-12	-.21
E	56	9	-29	-.52
F	52	14	-10	-.19
G	49	11	-16	-.33
J	57	14	-15	-.25
K	55	12	-19	-.35
O	54	10	-24	-.45
P	60	15	-15	-.25
Q	60	13	-21	-.35
S	66	14	-24	-.37
V	55	16	- 7	-.13
Z	63	15	-18	-.29

L at 2 intervals.

D	50	13	-11	-.22
F	45	6	-27	-.60
J	47	7	-26	-.55
K	46	7	-25	-.54
P	48	10	-18	-.38
V	48	9	-21	-.44

R at 4 intervals.

D	64	21	- 1	-.02
P	57	16	- 9	-.16

G

	1	2	3	4
E	50	10	-20	-.40
F	46	15	- 1	-.02
J	51	14	- 9	-.18
K	49	8	-25	-.51
O	48	9	-21	-.44
P	54	11	-21	-.39
Q	54	9	-27	-.50
S	60	10	-30	-.50
V	49	7	-28	-.57

V

	1	2	3	4
E	51	7	-30	-.59
J	52	12	-16	-.31
K	50	15	- 5	-.10
O	49	5	-34	-.69
P	55	10	-25	-.46
Q	55	10	-25	-.46

E

	1	2	3	4
J	57	18	- 3	-.05
P	60	13	-21	-.35
Q	60	9	-33	-.55

D

	1	2	3	4
E	56	10	-26	-.47
F	52	12	-16	-.31
G	49	9	-22	-.45
J	57	16	- 9	-.16
K	55	13	-16	-.29
O	54	8	-30	-.56
P	60	11	-27	-.45
Q	60	15	-15	-.25
S	66	10	-36	-.55
V	55	14	-12	-.22
Z	63	24	+ 9	+.14

F

	1	2	3	4
E	52	14	-10	-.19
J	53	9	-26	-.49
K	51	15	- 6	-.12
O	50	6	-32	-.64
P	56	12	-20	-.36
Q	56	8	-32	-.57
S	62	14	-20	-.32
V	51	11	-18	-.35

Z at 3 intervals.

E	50	12	-14	-.28
K	57	17	- 6	-.10
P	62	10	-32	-.52
S	68	23	+ 1	+.05

K

	1	2	3	4
E	55	10	-25	-.46
J	56	14	-14	-.25
O	53	16	- 5	-.09
P	59	14	-17	-.29
Q	59	13	-20	-.34

J

	1	2	3	4
P	55	24	+17	+.31
Q	55	13	-16	-.29

P

	1	2	3	4
Q	63	22	+ 3	+.05

II. THE SCHNEIDER CIPHER

The description of this cipher was published by its inventor, Commandant L. Schneider, of the French Army in 1912, and although it is somewhat complicated, in some quarters it has been thought to contain the elements of practicability and indecipherability. Upon investigation it turns out to be only another demonstration of the fact that in cryptography there is not always a positive correlation between the complexity of the operations involved in encipherment and the difficulty of unauthorized decipherment.

METHOD OF ENCIPHERMENT

This system aims to make the entire operation of encipherment and decipherment dependent upon the knowledge of a single key word agreed upon in advance by the correspondents. Let us suppose the word to be TREBIZOND.

An arbitrarily mixed alphabet is derived from a generating rectangle based upon this key word, with a departure from the usual method. Instead of inscribing the letters in the generating rectangle in the key word sequence, as is usual, the initial letter of the second line may be any letter except one of the key word itself. The remaining letters then follow in the key word sequence. Thus, suppose we choose K as this initial letter for the second line. Our rectangle is constructed as shown (Fig. 1) :

By taking the columns in succession and writing them in two lines of 13 letters each we have the Fig. 2 :

These two lines constitute Alphabet 1, in which T = Q, K = F, X = Z, etc. The values are all reciprocal (Fig. 2).

Alphabet 2 is derived from Alphabet 1 by the simple expedient of carrying the upper half of Alphabet 1, i. e., the first line, to the third line and revolving the sequence *one* letter to the right (Fig. 3).

The juxtaposition of lines 2 and 3 results in the formation of Alphabet 2, in which Q = I, F = T, Z = K, etc., also completely reciprocal.

Alphabet 3 is constructed by moving line 2 to line 4, and revolving the sequence *two* letters to the right (Fig. 4).

The juxtaposition of lines 3 and 4 results in the formation of Alphabet 3, in which I = D, T = W, K = Q, etc.

Continuation of this process can result in the production of a total of 13 different, secondary, reciprocal alphabets. As a rule only a limited number of these secondary alphabets is employed, usually not to exceed the first six or seven.

One of the main features of the method of encipherment is that groups of unequal lengths are enciphered in cyclic fashion by means of several alphabets. That is, the text is broken up into groups containing 1, 2, 3.... letters, enciphered by different alphabets, the groups being repeated in sets or cycles, as explained below.

Let us, as one of the correspondents, determine that the cycle is to consist of six groups. Taking the first six letters of line 1, or the upper half of Alphabet 1, their numerical values on the basis of their relative positions in the normal or straight alphabet, are as follows :

T	K	X	R	L	Y
4	1	5	3	2	6

This sequence of numbers, 4 1 5 3 2 6, constitutes a cycle designated hereafter as the NUMERICAL KEY. It partakes of the nature of an " interruptor " in that it dictates the number of letters in each of the irregular groups in encipherment. Thus, the first group contains 4 letters, the second, 1 letter, the third, 5 letters, etc. The seventh group would begin a repetition of the cycle, and it would contain 4 letters ; the eighth group, 1 letter, etc. This cycle is repeated many times within a message.

Encipherment within each group is regular in the succession of the alphabets employed. Thus, if four alphabets are determined upon, the alphabets would be employed in the sequence shown in Fig. 5.

Note that in groups containing moie letters than the number of alphabets decided upon, the sequence of alphabets is repeated. Thus, in the 5 letter group, we have the sequence of alphabets 1 2 3 4 1 ; in the 6 letter group, 1 2 3 4 1 2. Were the number of alphabets limited to 3, these groups would be as shown. Fig. 6.

Substitution then proceeds by the alphabets derived as above, according to the distribution of numbers within the groups. Let the message be :

ENEMY IS INTRENCHING ALONG WESTERN SLOPE OF... etc.

The encipherment using the three alphabets above is as shown. Fig. 7.

After substitution, the order of the letters within each group is reversed throughout the message, as shown. Fig. 8.

The cipher letters are then transmitted in groups of five, as is usual.

Now it is necessary that the information necessary to decipher the message be conveyed to the recipient, who, of course, is already in possession of the key word. This information is transmitted in the form of an INDICATOR GROUP consisting of three letters, whose location within the cipher message has been previously determined, in a manner to be explained below. The first letter of the Indicator Group gives the initial letter of the second line of the generating rectangle ; the second, the number of alphabets employed ; and the third, the length of the Numerical Key, from which its sequence can be derived, as shown above.

In the illustrative example, the initial letter is K. The number of alphabets being three, the 3rd letter in the upper half of Alphabet 1, viz., X, forms the second letter of the indicator group. The length of the numerical key being six, the 6th letter of the upper half of Alphabet 1, viz., Y, forms the third letter of the indicator group. The knowledge of this letter enables the recipient to construct the numerical key. The indicator group for the message above is, therefore, K X Y.

This indicator group is then inserted in the cipher text in a position determined by a previously agreed upon letter of the key word, usually either the first or last letter. Thus, if the correspondents agree upon the first letter of the key word, this indicator group would be inserted after the 20th letter of the cipher text, because T, the first letter of the key word, occupies the 20th position in the normal or straight alphabet. The cipher message above would read, therefore, as follows :

Message :

HOMUO FADXW BHSED EONYM KXYWU TRARX AZHQV LGLU... etc.

By varying the elements of the indicator group, a great number of conbinations can be obtained from one key word.

Let us try to decipher the following message :

Message :

```
KHNVL   IQKGK   NNHKV   QEEXK   XYXOP   MSIEE   TPDKU   LISYZ
HWBRE   SATHR   KZRGM   NJGKD   QKVVM   FQBKE   NEIHA   EAAME
KHFLW   XRKEO   KMHFM   WAFTW   ESPEB   DDGWP   JPXGD   ZVWUX
LZAYU   ENILH   AIUUA   EABRE   PWKFV   JJKIP   EMENF   SBVYZ
KWDMK   VLODO   OBFMB   BYWOQ   YVKVI   XDGIK   HEONE   EIWKW
PAECL   RNIHN   NMODQ   NIKAO   JKEOZ   TCFWD   JJODW   ZUAES
ZDWKG   KKBDT   XNKJD   IHTKS   NPGDU   RQFMD   ONAZA   ZMWCL
RHEOF   ZWFHV   KZYGE   VPNPK   AQAHM   DCCKK   UGDJW   ILIAB
ECESG   SPFEP   KOPIS   HHODN   DMKFI   SYQMZ   KLGQG   KTWYG
JWNPK   NWBHE   ULJVQ   ZZWIM   LWWNJ   UCDQQ   KKFDG   WPMFS
KIEBC   CDXLF   MDODO   EANKH   MHFZT   CPMPP   WDAVL   MPXKR
OJKFN   MVPRA   OEWJO   JVVWR   MDEWA   FYWHX   ENMEN   APRNP
VCUCL   HYFMN   LKHVP   NOJKF   WWCLR   AOOWZ   VJVVW   RMDEW
AFYWO   XENGZ   FKVWP   XUNUM   AYMGX   VNKOJ   KFSVB   ZRNLE
IONGM   NVFTD   HGBJO   LIPOW   NPPWK   NREPM   DWXYE   XNZON
UEVOP   WUQQQ   JNMPV   FQJWN   KKOLI   POWKO   VBHFY   MEPMD
AFMHF   ABEFD   MKHWU   EODRL   ISYDK   VZKWK   MIQXK   THYNS
VHEQA   AEVIX   PZTQK   IAMFT   TALOV   JKVHD   UETCH   MHVWR
HFUNN   GFCKK   EESYN   JUPWW   BC
```

PRINCIPLES OF SOLUTION

This cipher belongs to the class of combined substitution and transposition. The substitution does not follow the method of the ordinary periodic, multiple alphabet system, and the transposition is neither regular nor geometrical. We shall disregard the transposition involved and come at once to a consideration of the results of the method of substitution.

While at first glance it may be thought that this cipher, by the encipherment of the groups of different lengths, eliminates the regularity or cyclic nature of the ordinary periodic, multiple alphabet cipher, such is not strictly the case. It is true that the groups are irregular in length, but at the same time, since the numerical key repeats itself many times throughout a message, *there will be regular and cyclic repetitions of constant sets of groups.* In other words, there is a cycle in the system composed of a constant number of groups of irregular lengths. We shall first proceed to determine the length of this cycle.

The length of this cycle is dependent upon the length of the numerical key, and is the sum of the constituent numbers of the key. It is obvious that the key can be 2, 3, 4... up to 13 numbers in length. It cannot be more than 13 because of the manner in which the key is derived from the upper half of Alphabet 1.

Now the numbers in these numerical keys do not repeat themselves, and it follows, therefore, as a simple mathematical fact, that the sums of the numbers composing every possible key, in other words, the lengths of the possible cycles are constant and determinate quantities. Thus, if the key, consists of 2 numbers, the cycle will be 1 + 2 = 3 letters in length ; of it consists of 3 numbers, the cycle will be 1 + 2 + 3 = 6 letters in length. The table 1 gives the length of all possible cycles of the entire system.

In order to determine the correct cycle length we proceed, if necessary, to apply the coincidence method described in the first part of the preceding paper. The message is written out in lines of 3, 6, 10, 15... letters in length and a Table of Coincidence is to be made for each arrangement.

We must first take into consideration the fact that somewhere within the body of the message there is a group of 3 letters, composing the indicators of the message, and since these three letters do not form a part of any cycle, they will throw all the cycles succeeding them out of phase with the cycles preceding them. But, from the method given for fixing the location of the indicator group, the latter must occur somewhere within the first 26 letters of the cipher message. By discarding the first 26 letters of our message then, we may be sure that we have eliminated this source of distortion. Starting with the 27th letter of the message, viz., S, we proceed to set up the message according to various hypothetical cycle lengths. We may omit the lengths 3 and 6 at the start as being highly improbable.

In this case no table of coincidence is really necessary because the set-up on the assumption of a cycle of 28 letters gives so many repetitions within the same columns, that further corroboration is unnecessary. Note the repetitions of long polygraphs as given. Fig. 9.

The next step is to compile individual frequency tables for the columns. There will, of course, be 28 of them. They have been consolidated in Table 2, and the average frequency per column is given.

Now, according to Table 1, a cycle length of 28 requires that the numerical key consist of seven numbers, obviously the digits 1 to 7. We do not know how many alphabets are involved, but they probably do not exceed seven. If only three alphabets are involved, then they would be distributed in seven irregular groups as shown. Fig. 10.

Alphabet 1 would be employed twelve times, Alphabet 2, nine times, and Alphabet 3, seven times. The Fig. 11 gives the number of times the various alphabets would be employed on different hypotheses and how they are distributed within the cycle.

Returning to Table 2, and following the reasoning given in the first part of this paper, Columns 10 and 12 give the closest approximations to a theoretical single frequency table, and we shall start fitting frequencies with them as bases.

Taking the frequency table for Column 10 and applying it to that for every other column, we get the coincidence data shown in Table 3.

The index of coincidence for Columns 1 and 18 are so much higher than those for all other columns that we are forced to the conclusion that we have here a set of only three columns, viz., Columns 10, 1, and 18 in the same alphabet, which we shall arbitrarily call the A Alphabet.

The fact that we have a set of only 3 columns in one alphabet automatically rules out the assumption that 3 or 4 alphabets are involved in the system, for on these hypotheses there cannot be a set of less than four columns in the same alphabet (see. Fig. 13).

Taking the frequency table for Column 12 we go through the same steps as before, applying it to the frequency tables for all columns except 10, 1, 18, and 12. The data are as given in Table 4.

We can be sure of Columns 7 and 20 as belonging with Column 12, together making up the B Alphabet. Reference to the diagrams and frequencies of alphabets on various hypotheses as given Fig. 13, shows that in no case can the frequency of any alphabet be duplicated under one and the same hypothesis. For example, on a hypothesis of three alphabets, the frequency of Alphabet 1 is 12 ; of Alphabet 2, is 9 ; of Alphabet 3, is 7. We do not find two frequencies alike under the same hypothesis. This is one of the fundamental conditions or results of the system. It follows, therefore, that in combining frequency tables to find which ones belong to the same basic alphabet, no two consolidated tables can be composed of the same number of individual tables. Now the A Alphabet certainly comprises only three columns ; hence no other consolidated table can comprise the same number of columns. Hence it follows that the B Alphabet cannot also comprise three columns. Therefore, some other column of columns besides 7 and 20 belong with Column 12. The column having the next greatest index is Column 3, and it probably should be included with Columns 7 and 20. But the indices for Columns 24, 16, 6, and several others are fairly close to that for Column 3, and it may be that the B Alphabet consists of more than four individual alphabets. We must, therefore, apply a secondary test.

Let us apply the frequency tables for Columns 7, 12, and 20 to the likely candidates, and find the average index of coincidence. The highest average will indicate the column or columns which should be included with 7, 12, and 20. The data are given in Table 5.

It is very probable that Columns 3 and 24 belong with Columns 7, 12, and 20, and we may tentatively include them, looking for further corroboration later. We have, therefore, as comprising the B Alphabet, Columns 7, 12, 20, 24, and 3.

The column not already distributed and having the next highest average frequency is Column 19. The data for this column in connection with all other columns not already distributed are given in Table 6.

It is conclusive that here we have a set of four columns, viz., 19, 2, 11, and 23 belong to the C Alphabet. This number of alphabets does not conflict with the requirement that no two consolidated tables comprise the same number of individual tables. We have found, so far, that the A Alphabet consists of 3 columns, the B Alphabet of 5, and the C Alphabet of 4.

Taking the frequency table for Column 21 we apply it to the remaining undistributed columns. The data are shown in Table 7.

Columns 13 and 27 clearly belong with Column 21, but since we cannot have two sets of three columns (the A Alphabet was found to consist of three) it is clear that some other column or columns belong with Column 21 besides Columns 4, 13, and 27. Since the C Alphabet consists of four columns and the B Alphabet of five, obviously the number of columns for the D Alphabet must be greater than five. Let us apply a secondary test to Columns 4, 5, 6, 8, 15, 25, and 28, using the frequency tables for Columns 13, 21, and 27. The results are as given in Table 8.

We may select Column 4 as belonging with Columns 13, 27, and 21, but the others are close enough so as to leave us in doubt as to which column or columns in addition to Column 4 belong to this set. We must apply another test. Let us summarize what we have already determined :

A Alphabet	B Alphabet	C Alphabet	D Alphabet		
Columns	Columns	Columns	Columns		
10	12	19			5
1	3	2	4	and at	6
18	7	11	13	least	8
	20	23	21	two of the	15
	24		27	following	25
					28

The number of columns not as yet definitely distributed is twelve. Upon the hypotheses of five, six, and seven alphabets, and according to the distributions given in Fig. 11, these twelve columns may be distributed in one of the following ways :

Basis of 5 Alphabets

5	more in D Alphabet	Alphabet 1
7	in E Alphabet	Alphabet 2

or

3	more in D Alphabet	Alphabet 2
9	in E Alphabet	Alphabet 1

Basis of 6 Alphabets

4	more in D Alphabet	Alphabet 1
6	in E Alphabet	Alphabet 2
2	in F Alphabet	Alphabet 6

or

2	more in D Alphabet	Alphabet 2
8	in E Alphabet	Alphabet 1
2	in F Alphabet	Alphabet 6

3 more	in D Alphabet	Alphabet 1
6	in E Alphabet	Alphabet 2
2	in F Alphabet	Alphabet 6
1	in G Alphabet	Alphabet 7

or

2 more	in D Alphabet	Alphabet 2
7	in E Alphabet	Alphabet 1
2	in F Alphabet	Alphabet 6
1	in G Alphabet	Alphabet 7

Which of these distributions is correct, we may now proceed to determine. Referring again to the distributions given in Fig. 11, it will be noted that regardless of whether a hypothesis of five, six, or seven alphabets is assumed, the A Alphabet corresponds to Alphabet 5, since it comprises three columns ; the B Alphabet corresponds to Alphabet 3, since it comprises five columns ; the C Alphabet corresponds to Alphabet 4, since it comprises four columns ; the D Alphabet can correspond to either Alphabet 1 or Alphabet 2, depending upon the number of additional columns which must be assigned to it, and this we were not able to determine from the data. Let us, however, convert the arbitrary designations, A, B, and C into their corresponding putative numerical equivalents, and indicate beneath the series of columns the distributions determined above. (Fig. 14.)

Let us now compare these partial sequences with the sequences of alphabets within the reversed groups on hypotheses of five, six, and seven alphabets.

When these various reversed sequences are compared with the partial sequences given by the distribution of alphabets above, several things become at once obvious.

First, the D Alphabet must correspond, not to Alphabet 1, but to Alphabet 2, regardless of whether there are five, six, or seven alphabets involved, because Alphabet 2 must follow Alphabet 3 in the descending sequences of Alphabets 5 4 3 . . . Columns 8 and 25, belong to the D Alphabet in addition to Columns 4, 13, 21, and 27, because they are necessary to complete the sequences $\begin{matrix}7 & 8\\ 3 & —\end{matrix}$ and $\begin{matrix}23 & 24 & 25\\ 4 & 3 & —.\end{matrix}$ In the experimental fitting of alphabets we find that the index of coincidence for Columns 8 and 25 are next highest to that for Column 4 in the secondary test, and we may consider it as established that Columns 8 and 25 belong to the D Alphabet, or Alphabet 2.

The third point that is noted is that Alphabet 1 must consist of at least Columns 5, 9, 14, 22, 26 and 28, in order that the following sequences be completed in their descending order :

Columns ..	1	2	3	4	5	7	8	9	10	11	12	13	14	18	19	20	21	22	23	24	25	26	27	28
Alphabets .	5	4	3	2	(1)	3	2	(1)	5	4	3	2	(1)	5	4	3	2	(1)	4	3	2	(1)	2	(1)

Our distribution, therefore, becomes as shown. Fig. 15.

The fourth point noted is that the hypothesis of 5 alphabets must be correct, for the distribution of the columns into Alphabets 5, 4, and 3, of which we are sure, allows no room for any Alphabet 6 or 7. This conclusion is reached by the following analysis. Take the only two places where an Alphabet 6 could fall :

3	4	5	6	7	8
... 3	2	1		3	2 ...

13	14	15	16	17	18	19
... 2	1				5	4 ...

The first we may dispose of at once, since Alphabet 6 canot immediately precede Alphabet 3. In fact we may now take note that Column 6 must belong to Alphabet 1, for the only other alphabet to which it could possibly be assigned would be Alphabet 4, and since our set of columns belonging to Alphabet 4 is already complete, we are forced to conclude that Column 6 belongs to Alphabet 1.

A hypothesis of 6 alphabets requires 2 columns to be included by Alphabet 6 (see page 78). Therefore, if an assumption of 6 alphabets is made, both columns belonging to Alphabet 6 would have to fall within Columns 15, 16, or 17, which is impossible ; for, while we may assign Column 17 as one of those belonging to Alphabet 6, neither Column 15 nor 16 can belong to Alphabet 6, for there is not room enough for a sequence 6 5 4 3 2 1 to be completed between Columns 15 and 18.

What has been stated with regard to the incorrectness of a hypothesis of six alphabets applies likewise to hypothesis of seven alphabets.

We are forced, therefore, to conclude that the problem involves 5 alphabets. This being the case, it is obvious that we must have 9 columns assigned to Alphabet 1, and 7 columns to Alphabet 2. Now Alphabet 2, our former D Alphabet, already has 6 columns, so that we are lacking but 1 column for this alphabet, and the following analysis of the distribution makes Column 15 the most logical missing column of Alphabet 2. The only columns open for an assignment to Alphabet 2 are Columns, 15, 16, and 17. Since if Alphabet 2 does occur it must be followed by Alphabet 1, we may rule out Column 17 at once as belonging to Alphabet 2 since it is followed by Alphabet 5. We are left, therefore, Columns 15 and 16 as possibilities. Refer now to Table 2, and note that the index of coincidence for Column 15 gives better indications of its belonging with Alphabet 2 than does Column 16.

Since Alphabet 2 must be followed by Alphabet 1, Column 16 must be assigned to Alphabet 1 ; and Column 17, by elimination of all other hypotheses, must also be assigned to Alphabet 1.

Our distribution is, therefore, as shown, Fig. 15, where the alphabets are set off in irregular groups to correspond to a hypothetical numerical key.

We have here a distribution equivalent to the numerical key 5 1 3 5 2 6 4 2. But this is not correct, for our group of 7 columns is missing, and there are two cases of groups of 2 columns. It is obvious that the key must be corrected by shifting the cycle as shown. Fig. 16.

We have thus reconstructed the complete numerical key, and may now proceed to transcribe the message in groups in accordance therewith. Since the first group contains 7 letters, and since the letter S with which we started our first transcription (Fig. 9) is labelled 1, it is clear that we must start our second transcription with the two letters preceding S, i. e., the 25th and 26th letters of the cipher message, which are PM. Thus :

7	I	3	5	2	6	4
PMSIEET	P	DKU	LISYZ	HW	BRESAT	HRKZ
RGMNJGK	D	QKV	VMFQB	KE	NEIHAE	AAME

After this transcription a third set up is necessary, in which the sequences of letters are reversed within groups, in order to bring the cipher letters back into the original arrangement before transposition. The rearranged set up is as given in Fig. 17.

We are now confronted with a rather simple case of the analysis of five *reciprocal* and interrelated alphabets. They are composed of the consolidated frequency tables applying to the columns which belong in the same alphabets and are as given in Table 9.

It will be unnecessary in this paper to discuss the method of deciphering the message by an analysis of these five single frequency tables. Suffice it to indicate the values obtained from decipherment. They are given Table 10 where the values obtained from a knowledge of the reciprocal relation are placed within parentheses. Only five values remain unknown, all in Alphabet 5.

We may now attempt a reconstruction of the original, or primary alphabet, of which these are secondaries. Note the following values :

Alphabet	1	E = N
—	2	N = O
—	3	O = V
—	4	V = M
—	5	M = T

Now if E occurs in the upper half of Alphabet 1, the Table of Alphabets must contain a column like this :

<table>
<tr><td rowspan="2">Alphabet 1</td><td>E</td><td></td></tr>
<tr><td>N</td><td rowspan="2">Alphabet 2</td></tr>
<tr><td rowspan="2">Alphabet 3</td><td>O</td></tr>
<tr><td>V</td><td rowspan="2">Alphabet 4</td></tr>
<tr><td rowspan="2">Alphabet 5</td><td>M</td></tr>
<tr><td>T</td><td></td></tr>
</table>

Let us assume this to be correct. In Alphabet 3, E will again be in the upper half of the Alphabet. We have these values :

Alphabet	3	E = D
—	4	D = Z
—	5	Z = ?

But to this we may and two more values since we have the value of E in Alphabet 2. Thus :

Alphabet	1	K = A
—	2	A = E
—	3	E = D
—	4	D = Z
—	5	Z = ?

Since the upper line in Alphabet 3 is displaced but one letter to the right as compared with that of Alphabet 1, we have two columns in the table as follows :

	1 2	
Alphabet 1	EK	
	NA	Alphabet 2
Alphabet 3	OE	
	VD	Alphabet 4
Alphabet 5	MZ	
	T ?	

We may continue thus : moving K of line 1 to line 3 :

Alphabet	1	W = I
—	2	I = K
—	3	K = N
—	4	N = H
—	5	H = C

Hence we have this :

	1 2 3	
Alphabet 1	EKV	
	NAI	Alphabet 2
Alphabet 3	OEK	
	VDN	Alphabet 4
Alphabet 5	MZH	
	T?C	

The process is very simple and easy to continue. Finally we have this :

```
              1 2 3 4 5 6 7
              EKWFXLY
Alphabet 1
              NA I RQB J
                              Alphabet 2
              OEKWFXL
Alphabet 3
              VDNA I RQ
                              Alphabet 4
              MZHOEKW
Alphabet 5
              T . CSVDN
```

We may now continue from the sequences given already. Thus in the last line we see the sequence . . . S V D N, in the fourth line, V D N A I R Q. Hence, we may add A I R Q to the last line. The same process applied to the other lines gives us the result shown in Fig. 18.

We may fill in the rest from the Alphabets themselves, and we have the Fig. 19.

Taking Alphabet 1, a speedy reconstruction of the original rectangle is at once effected. (Fig. 20.)

The key word is EXPORTS. In conformity with the agreements of the system, the indicators should be KXY and indicate the following :

K = the initial letter of the distorted alphabet

X = the fifth letter in Alphabet 1, hence 5 Alphabets

Y = the seventh — — 1, — 7 groups

arranged as follows

E K W F X L Y

1 3 5 2 6 4 7

The indicators will be after either the 5th letter or the 19th (corresponding to the numerical value of the initial or final letter of the key word). We find KXY after the 19th letter.

We may now proceed to decipher the first few groups of the message and the entire solution is at hand. It is as shown Fig. 21.

The fatal defect in this system lies in the fact that a numerical key is used which introduces a frequently repeated cycle within a message. The determination of the length of this cycle, and its reconstruction by means of a comparison of alphabets based upon the Index of Coincidence enables a speedy solution to be attained. The many details involved in encipherment, concomitants of an attempt to make the entire operation dependent upon the knowledge of a single key word, makes this cipher impractical for field use. The ease with which a solution may be achieved makes it unsafe for use in the more important operations of the larger headquarters of the rear.

FIGURES

Fig. 1

T R E B I Z O N D
K L M P Q S U V W
X Y A C F G H J

Fig. 2

Alphabet 1	(1)	T K X R L Y E M A B P C I
	(2)	Q F Z S G O U H N V J D W

Fig. 3

Alphabet 1	(1)	T K X R L Y E M A B P C I	
	(2)	Q F Z S G O U H N V J D W	Alphabet 2
	(3)	I T K X R L Y E M A B P C	

Fig. 4

Alphabet 1	(1)	T K X R L Y E M A B P C I	
	(2)	Q F Z S G O U H N V J D W	Alphabet 2
Alphabet 3	(3)	I T K X R L Y E M A B P C	
	(4)	D W Q F Z S G O U H N V J	

Fig. 5

Numérical key	4	1	5	3	2	6
Alphabets	1-2-3-4	1	1-2-3-4-1	1-2-3	1-2	1-2-3-4-1-2

Fig. 6

Numérical key	4	1	5	3	2	6
Alphabets	1-2-3-1	1	1-2-3-1-2	1-2 3	1-2	1-2-3-1-2-3

Fig. 7

Numérical key.	4	1	5	3	2	6	4	1	5	3	2
Alphabets	1-2-3-1	1	1-2-3-1-2	1-2-3	1-2	1-2-3-1-2-3	1-2-3-1	1	1-2-3-1-2	1-2-3	1-2
Clear	E N E M	Y	I S I N T	R E N	C H	I N G A L O	N G W E	S	T E R N S	L O P	E O
Cipher	U M O H	O	W X D A F	S H B	D E	W M Y N O E	A R T U	R	Q H Z A X	G L V	U L

Fig. 8

4	1	5	3	2	6	4	1	5	3	2
H O M U	O	F A D X W	B H S	E D	E O N Y M W	U T R A	R	X A Z H Q	V L G	L U

Fig. 9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
S	I	E	E	T	P	D	K	U	L	I	S	Y	Z	H	W	B	R	E	S	A	T	H	R	K	Z	R	G
M	N	J	G	K	D	Q	K	V	V	M	F	Q	B	K	E	N	E	I	H	A	E	A	A	M	E	K	H
F	L	W	X	R	K	E	O	K	M	H	F	M	W	A	F	T	W	E	S	P	E	B	D	D	G	W	P
J	P	X	G	D	Z	V	W	U	X	L	Z	A	Y	U	E	N	I	L	H	A	I	U	U	A	E	A	B
R	E	P	W	K	F	V	J	J	K	I	P	E	M	E	N	F	S	B	V	Y	Z	K	W	D	M	K	V
L	O	D	O	O	B	F	M	B	B	Y	W	O	Q	Y	V	K	V	I	X	D	G	I	K	H	E	O	N
E	E	I	W	K	W	P	A	E	C	L	R	N	I	H	N	N	M	O	D	Q	N	I	K	A	O	J	K
E	O	Z	T	C	F	W	D	J	J	O	D	W	Z	A	U	E	S	Z	D	W	K	G	K	K	B	D	T
X	N	K	J	D	I	H	T	K	S	N	P	G	D	U	R	Q	F	M	D	O	N	A	Z	A	Z	M	W
C	L	R	H	E	O	F	Z	W	F	H	V	K	Z	Y	G	E	V	P	N	P	K	A	Q	A	H	M	D
C	C	K	K	U	G	D	J	W	I	L	I	A	B	E	C	E	S	G	S	P	F	E	P	K	O	P	I
S	H	H	O	D	N	D	M	K	F	I	S	Y	Q	M	Z	K	G	L	Q	G	K	T	W	Y	G	J	W
N	P	K	N	W	B	H	E	U	L	J	V	Q	Z	Z	W	I	M	L	W	W	N	J	U	C	D	Q	Q
K	K	F	D	G	W	P	M	F	S	K	I	E	B	C	C	D	X	L	F	M	D	O	D	O	E	A	N
K	H	M	H	F	Z	T	C	P	M	P	P	W	D	A	V	L	M	P	X	K	R	O	J	K	F	N	M
V	P	R	A	O	E	W	J	O	J	V	V	W	R	M	D	E	W	A	F	Y	W	H	X	E	N	M	E
N	A	P	R	N	P	V	C	U	C	L	H	Y	F	M	N	L	K	H	V	P	N	O	J	K	F	W	W
C	L	R	A	O	O	W	Z	V	J	V	V	W	R	M	D	E	W	A	F	Y	W	O	X	E	N	G	Z
F	K	V	W	P	U	X	N	U	M	A	Y	M	G	X	V	N	K	O	J	K	F	S	V	B	Z	R	N
L	E	I	O	N	G	M	N	V	F	T	D	H	G	B	J	O	L	I	P	O	W	N	P	P	W	K	N
R	E	P	M	D	W	X	Y	E	X	N	Z	O	N	U	E	V	O	P	W	U	Q	Q	Q	J	N	M	P
V	F	Q	J	W	N	K	K	O	L	I	P	O	W	K	O	V	B	H	F	Y	M	E	P	M	D	A	F
M	H	F	A	B	E	F	D	M	K	H	W	U	E	O	D	R	L	I	S	Y	D	K	V	Z	K	W	K
M	I	Q	X	K	T	H	Y	N	S	V	H	E	Q	A	A	E	V	I	X	P	Z	T	Q	K	I	A	M
F	T	T	A	L	O	V	J	K	V	H	D	U	E	T	C	L	M	H	V	W	R	H	F	U	N	N	G
F	C	K	K	E	E	S	Y	N	J	U	P	W	W	B	C												

Fig. 10

Groups	Alphabets
1	1
2	1 - 2
3	1 - 2 - 3
4	1 - 2 - 3 - 1
5	1 - 2 - 3 - 1 - 2
6	1 - 2 - 3 - 1 - 2 - 3
7	1 - 2 - 3 - 1 - 2 - 3 - 1

Frequency of alphabets

Alphabet	1	—	12	times
—	2	—	9	—
—	3	—	7	—

Fig. 11.

Basis of 4 Alphabets

Groups	Alphabets
1	1
2	1 - 2
3	1 - 2 - 3
4	1 - 2 - 3 - 4
5	1 - 2 - 3 - 4 - 1
6	1 - 2 - 3 - 4 - 1 - 2
7	1 - 2 - 3 - 4 - 1 - 2 - 3

Frequency of Alphabets.

Alphabet	1	—	10	times
—	2	—	8	—
—	3	—	6	—
—	4	—	4	—

Basis of 5 Alphabets

Groups	Alphabets
1	1
2	1 - 2
3	1 - 2 - 3
4	1 - 2 - 3 - 4
5	1 - 2 - 3 - 4 - 5
6	1 - 2 - 3 - 4 - 5 - 1
7	1 - 2 - 3 - 4 - 5 - 1 - 2

Frequency of Alphabets.

Alphabet	1	—	9	times
—	2	—	7	—
—	3	—	5	—
—	4	—	4	—
—	5	—	3	—

Basis of 6 Alphabets

Groups	Alphabets
1	1
2	1 - 2
3	1 - 2 - 3
4	1 - 2 - 3 - 4
5	1 - 2 - 3 - 4 - 5
6	1 - 2 - 3 - 4 - 5 - 6
7	1 - 2 - 3 - 4 - 5 - 6 - 1

Frequency of Alphabets.

Alphabet	1	—	8	times
—	2	—	6	—
—	3	—	5	—
—	4	—	4	—
—	5	—	3	—
—	6	—	2	—

Basis of 7 Alphabets

Groups	Alphabets
1	1
2	1 - 2
3	1 - 2 - 3
4	1 - 2 - 3 - 4
5	1 - 2 - 3 - 4 - 5
6	1 - 2 - 3 - 4 - 5 - 6
7	1 - 2 - 3 - 4 - 5 - 6 - 7

Frequency of Alphabets.

Alphabet	1	—	7	times
—	2	—	6	—
—	3	—	5	--
—	4	—	4	—
—	5	—	3	—
—	6	--	2	—
—	7	--	1	—

Fig. 12.

Columns	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Alphabets	A	C	B	D			B			A	C	B	D					A	C	B	D		C	B			D	
	5	4	3				3			5	4	3						5	4	3			4	3				

Fig. 13.

Hypothesis of 5 Alphabets

	Before reversing	After reversing
Groups	Alphabets	Alphabets
1	1	1
2	1 - 2	2 - 1
3	1 - 2 - 3	3 - 2 - 1
4	1 - 2 - 3 - 4	4 - 3 - 2 - 1
5	1 - 2 - 3 - 4 - 5	5 - 4 - 3 - 2 - 1
6	1 - 2 - 3 - 4 - 5 - 1	1 - 5 - 4 - 3 - 2 - 1
7	1 - 2 - 3 - 4 - 5 - 1 - 2	2 - 1 - 5 - 4 - 3 - 2 - 1

Frequency of Alphabets.

Alphabet	1	—	9	times
—	2	—	7	—
—	3	—	5	—
—	4	—	4	—
—	5	—	3	—

Hypothesis of 6 Alphabets.

	Before reversing	After reversing
Groups	Alphabets	Alphabets
1	1	1
2	1 - 2	2 - 1
3	1 - 2 - 3	3 - 2 - 1
4	1 - 2 - 3 - 4	4 - 3 - 2 - 1
5	1 - 2 - 3 - 4 - 5	5 - 4 - 3 - 2 - 1
6	1 - 2 - 3 - 4 - 5 - 6	6 - 5 - 4 - 3 - 2 - 1
7	1 - 2 - 3 - 4 - 5 - 6 - 1	1 - 6 - 5 - 4 - 3 - 2 - 1

Frequency of Alphabets.

Alphabet	1	—	8	times
—	2	—	6	—
—	3	—	5	—
—	4	—	4	—
—	5	—	3	—
—	6	—	2	—

Hypothesis of 7 Alphabets.

	Before reversing	After reversing
Groups	Alphabets	Alphabets
1	1	1
2	1 - 2	2 - 1
3	1 - 2 - 3	3 - 2 - 1
4	1 - 2 - 3 - 4	4 - 3 - 2 - 1
5	1 - 2 - 3 - 4 - 5	5 - 4 - 3 - 2 - 1
6	1 - 2 - 3 - 4 - 5 - 6	6 - 5 - 4 - 3 - 2 - 1
7	1 - 2 - 3 - 4 - 5 - 6 - 7	7 - 6 - 5 - 4 - 3 - 2 - 1

Frequency of Alphabets.

Alphabet	1	—	7	times
—	2	—	6	—
—	3	—	5	—
—	4	—	4	—
—	5	—	3	—
—	6	—	2	—
—	7	—	1	—

Fig. 14.

```
Columns    1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-25-26-27-28
Alphabets  5-4-3-2-1  3-2-1 -5 - 4 - 3 - 2 - 1              5 - 4 - 3 - 2 - 1 - 4 - 3 - 2 - 1 - 2 - 1
```

Fig. 15.

```
Columns    -1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-25-26-27-28
Alphabets  -5-4-3-2-1 |1|3-2-1| 5 - 4 - 3 - 2 - 1 | 2 - 1 | 1 - 5 - 4 - 3 - 2 - 1 | 4 - 3 - 2 - 1 | 2 - 1
Groups     -    5     |1|  3  |         5         |   2   |           6           |       4       |   2
```

Fig. 16.

```
27-28-1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16- 17-18-19-20-21-22-23-24-25-26
 2  1  5 4 3 2 1 |1| 3 2 1 | 5  4  3  2  1 | 2  1 | 1  5  4  3  2  1 | 4  3  2  1
        7        |1|   3   |       5       |   2  |         6        |     4
```

Fig. 19

```
       1 2 3 4 5 6 7 8 9 10 11 12 13
(1) { E K W F X L Y G P M  Z  H  O
    { N A I R Q B J T U C  S  V  D  }
                                    } (2)
(3) { O E K W F X L Y G P  M  Z  H  }
    { V D N A I R Q B J T  U  C  S  }
                                    } (4)
(5) { M Z H O E K W F X L  Y  G  P  }
    { T U C S V D N A I R  Q  B  J
```

Fig. 18

```
       1 2 3 4 5 6 7 8 9 10 11 12 13
(1) { E K W F X L Y       M  Z  H  O
    { N A I R Q B J T     C  S  V  D  }
                                      } (2)
(3) { O E K W F X L Y        M  Z  H  }
    { V D B A I R Q B J T       C  S  }
                                      } (4)
(5) { M Z H O E K W F X L  Y          }
    { T   C S V D N A I R  Q  B  J
```

Fig. 20

```
E X P O R T S
K L M N Q U V
w Y Z A B C D
F G H I J
```

Fig. 17.

Numerical key......	7	1	3	5	2	6	4
Alphabets...........	1 2 3 4 5 1 2	1	1 2 3	1 2 3 4 5	1 2	1 2 3 4 5 1	1 2 3 4
After reversing.....	P M S I E E T	P	D K U	L I S Y Z	H W	B R E S A T	H R K Z
Before —	T E E I S M P	P	U K D	Z Y S I L	W H	T A S E R B	Z K R H
	R G M N J G K	D	Q K V	V M F Q B	K E	N E I H A E	A A M E
	K G J N M G R	D	V K Q	B Q F M V	E K	E A H I E N	E M A A
	K H F L W X R	K	E O K	M H F M W	A F	T W E S P E	B D D G
	R X W L F H K	K	K O E	W M F H M	F A	E P S E W T	G D D B
	W P J P X G D	Z	V W U	X L Z A Y	U E	N I L H A I	U U A E
	D G X P J P W	Z	U W V	Y A Z L X	E U	I A H L I N	E A U U
	A B R E P W K	F	V J J	K I P E M	E N	F S B V Y Z	K W D M
	K W P E R B A	F	J J V	M E P I K	N E	Z Y V B S F	M D W K
	K V L O D O O	B	F M B	B Y W O Q	Y V	K V I X D G	I K H E
	O O D O L V K	B	B M F	Q O W Y B	V Y	G D X I V K	E H K I
	O N E E I W K	W	P A E	C L R N I	H N	N M O D Q N	I K A O
	K W I E E N C	W	E A P	I N R L C	N H	N Q D O M N	O A K I
	J K E O Z T C	F	W D J	J O D W Z	A U	E S Z D W K	G K K B
	C T Z O E K J	F	J D W	Z W D O J	U A	K W D Z S E	B K K G
	D T X N K J D	I	H T K	S N P G D	U R	Q F M D O N	A Z A Z
	D J K N X T D	I	K T H	D G P N S	R U	N O D M F Q	Z A Z A
	M W C L R H E	O	F Z W	F H V K Z	Y G	E V P N P K	A Q A H
	E H R L C W M	O	W Z F	Z K V H F	G Y	K P N P V E	H A Q A
	M D C C K K U	G	D J W	I L I A B	E C	E S G S P F	E P K O
	U K K C C D M	G	W J D	B A I L I	C E	F P S G S E	O K P E
	P I S H H O D	N	D M K	F I S Y Q	M Z	K G L Q G K	T W Y G
	D O H H S I P	N	K M D	Q Y S I F	Z M	K G Q L G K	G Y W T
	J W N P K N W	B	H E U	L J V Q Z	Z W	I M L W W N	J U C D
	W N K P N W J	B	U E H	Z Q V J L	W Z	N W W L M I	D C U J
	Q Q K K F D G	W	P M F	S K I E B	C C	D X L F M D	O D O E
	G D F K K Q Q	W	F M P	B E I K S	C C	D M F L X D	E O D O
	A N K H M H F	Z	T C P	M P P W D	A V	L M P X K R	O J K F
	F H M H K N A	Z	P C T	D W P P M	V A	R K X P M L	F K J O
	N M V P R A O	E	W J O	J V V W R	M D	E W A F Y W	H X E N
	O A R P V M N	E	O J W	R W V V J	D M	W Y F A W E	N E X H
	M E N A P R N	P	V C U	C L H Y F	M N	L K H V P N	O J K F
	N R P A N E M	P	U C V	F Y H L C	N M	N P V H K L	F K J O
	W W C L R A O	O	W Z V	J V V W R	M D	E W A F Y W	O X E N
	O A R L C W W	O	V Z W	R W V V J	D M	W Y F A W E	N E X O

Fig. 21.

Numerical key	1	3	5	2	6	4	7
Alphabets	1	1 2 3	1 2 3 4 5	1 2	1 2 3 4 5 1	1 2 3 4	1 2 3 4 5 1 2
Clear	A	H O S	T I L E R	E I	N F O R C E	D B R I	G A D E O C C
Substitution	K	V N H	G K Q I L	N K	E Q V K H N	O X X E	T E E I S M P
Transposition	K	H N V	L I Q K G	K N	N H K V Q E	E X X O	P S M I E E T
	U	P I E	S T H E R	I D	G E H I L L	S I X N	A U G H T T W
	P	U K D	Z Y S I L	W H	T A S E R B	Z K R H	K G J N M G R
	P	D K U	L I S Y Z	H W	B R E S A T	H R K Z	R G M N J G K
	O	H I L	L F I V E	N I	N E S E V E	N S W O	F B A T A V I
	D	V K Q	B Q F M V	E K	E A H 1 E N	E M A A	R X W L F H K
	D	Q K V	V M F Q B	K E	N E I H A E	A A M E	K H F L W X R
	A	A N D	I S I N T	R E	N C H I N G	T H E F	O U R S P U R
	K	K O E	W M F H M	F A	E P S E W T	G D D B	D G X P J P W
	K	E O K	M H F M W	A F	T W E S P E	B D D G	W P J P X G D
	S	P R O	J E C T I	N G	W E S T X E	N E M Y	A R T I L L E
	Z	U W V	Y A Z L X	E U	I A H L I N	E A U U	K W P E R B A
	Z	V W U	X L Z A Y	U E	N I L H A I	U U A E	A B R E P W K
	R	Y L O	C A T E D	E A	S T O F O R	C H A R	D N E A R H I
	F	J J V	M E P I K	N E	Z Y V B S F	M D W K	O O D O L V K
	F	V J J	K I P E M	E N	F S B V Y Z	K W D M	K V L O D O O
	L	L S I	X N A U G	H T	T H R E E A	N D N E	A R F I V E N
	B	B M F	Q O W Y B	V Y	G D X I V K	E H K I	K W I E E N O
	B	F M B	B Y W O Q	Y V	K V I X D G	I K H E	O N E E I W K
	I	N E T	W O X T H	E D	E F E A T E	D E N E	M Y C A V A L
	W	E A P	I N R L C	N H	N Q D O M N	O A K I	C T Z O E K J
	W	P A E	C L R N I	H N	N M O D Q N	I K A O	J K E O Z T C
	R	Y H A	S R E A P	P E	A R E D O N	L I N C	O L N H I G H
	F	J D W	Z W D O J	U A	K W D Z S E	B K K G	D J K N X T D
	F	W D J	J O D W Z	A U	E S Z D W K	G K K B	D T X N K J D
	W	A Y S	O U T H O	F G	E N E V A X	S E C O	N D X T H I S
	I	K T H	D G P N S	R U	N O D M F Q	Z A Z A	E H R L C W M
	I	H T K	S N P G D	U R	Q F M D O N	A Z A Z	M W C L R H E

PLAIN TEXT

A HOSTILE REINFORCED BRIGADE OCCUPIES THE RIDGE HILL SIX
NAUGHT TWO HILL FIVE NINE SEVEN SW OF BATAVIA AND IS
INTRENCHING THE FOUR SPURS PROJECTING WEST X ENEMY
ARTILLERY LOCATED EAST OF ORCHARD NEAR HILL SIX NAUGHT
THREE AND NEAR FIVE NINE TWO X THE DEFEATED ENEMY CAVALRY
HAS REAPPEARED ON LINCOLN HIGHWAY SOUTH OF GENEVA X SECOND.......

TABLES

Table 1.

Lenght of key	Lenght of cycle
2	3
3	6
4	10
5	15
6	21
7	28
8	36
9	45
10	55
11	66
12	78
13	91

Table 4.

Column 12

Columns	Frequencies	coïncidence	Différences	Indices of coïncidence
2	52	9	-25	-.48
3	52	13	-13	-.25
4	52	6	-34	-.65
5	52	8	-28	-.54
6	52	10	-22	-.42
7	52	16	- 4	-.08
8	52	6	-34	-.65
9	52	7	-31	-.60
11	52	9	-25	-.48
13	52	4	-40	-.77
14	52	9	-25	-.48
15	52	4	-40	-.77
16	52	11	-19	-.37
17	51	6	-33	-.65
19	51	8	-27	-.53
20	51	15	- 6	-.12
21	51	9	-24	-.46
22	51	10	-21	-.41
23	51	5	-36	-.70
24	51	11	-18	-.35
25	51	6	-33	-.65
26	51	9	-24	-.46
27	51	5	-36	-.70
28	51	10	-21	-.41

Table 3.

Column 10

Columns	Frequencies	coïncidence	Différences	Indices of coïncidence
1	52	17	- 1	-.02
2	52	10	-22	-.42
3	52	9	-25	-.48
4	52	7	-31	-.60
5	52	6	-34	-.65
6	52	5	-37	-.71
7	52	10	-22	-.42
8	52	11	-19	-.37
9	52	9	-25	-.48
11	52	8	-28	-.54
12	52	7	-31	-.60
13	52	3	-43	-.83
14	52	5	-37	-.71
15	52	8	-28	-.54
16	52	6	-34	-.65
17	51	10	-21	-.41
18	51	16	- 3	-.06
19	51	6	-33	-.65
20	51	11	-18	-.35
21	51	3	-42	-.83
22	51	6	-33	-.65
23	51	6	-33	-.65
24	51	6	-27	-.53
25	51	7	-30	-.59
26	51	6	-33	-.65
27	51	7	-30	-.59
28	51	8	-27	-.53

Table 2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Number of Columns	Number of different letters	Average Frequency per letter
1			3		2	4				1	2	2	3	2				2	2			2		1			26	12	2.16
2	1		2		3	2		3	2		2	3		2	2	3				1							»	12	2.16
3				1	1	2		1	2	1	4		1			3	2	3		1		1	1	1		1	»	16	1.62
4	4			1	1		2	2		2	2		1	1	3			1		1			3	2			»	14	1.86
5		1	1	4	2	1	1				4	1		2	3	1		1		1	1		2				»	15	1.75
6		2		1	3	2	2		1		1			2	3	2				1	1		3			2	»	14	1.86
7				3	1	3		3			1		1			2	1		1	1		4	3	2			»	13	2.00
8	1		2	2	1					4	3		3	2	1					1			1		3	2	»	13	2.00
9		1			3	1				2	4		1	1	2	1					5	3	2				»	12	2.16
10		1	2			3			1	4	2	3	3						3			2		2			»	11	2.36
11	1							4	4	1	1	4	1	2	1	1				1	1	3			1		»	14	1.86
12				3		2		2	2							5		1	2			4	2		1	2	»	11	2.36
13	2				3		1	1			1		2	1	3		2				2		5		3		»	12	2.16
14		3		2	2	1	2		1				1	1			3	2					3		1	4	»	13	2.00
15	4	2	1		2			2			2		4		1					1	3			1	2	1	»	13	2.00
16	1		4	3	3	1	1			1				3	1			1			1	3	2			1	»	14	1.86
17		1		1	6	1			1		2	3		4	1		1	1		1		2					25	13	1.92
18		1			1	1	1		1		2	2	4		1			1	3			3	3	1			»	14	1.78
19	2	1			2		1	3	5			4	1		2	3										1	»	11	2.27
20				3		4		2		1				1		1	1		4			3	2	3			»	11	2.27
21	3			1			1				2		1		2	5	1				1		3		5		»	11	2.27
22				2	2	2	1		1		3		1	4			1	2		1			3			2	»	13	1.92
23	3	1			2		1	3	2	1	2			1	4		1		1	2	1						»	14	1.78
24	1			2		1				2	3					3	3	1			2	2	2	2		1	»	13	1.92
25	4	1	1	2	2			1		1	6		2		1	1					1				1	1	»	14	1.78
26		1		2	4	2	2	1	1		1		1	4	2								1			3	»	13	1.92
27	4			1			1			2	3		4	2	1	1	1	2					3				»	12	2.08
28		1		1	1	1	2	1	1		2		2	4		2	1			1		1	3			1	»	16	1.56

Table 5

Columns	Total Frequencies per Column			Average Frequency	Coincidences per column			Différences			Totals of Differences	Average Differences	Average of Indices of coincidence
	7	12	20		7	12	20	7	12	20			
3	52	52	51	51.7	14	13	10	-10	-13	-21	-44	-14.7	-.285
6	52	52	51	51.7	11	10	7	-19	-22	-30	-71	-23.7	-.458
11	52	52	51	51.7	10	9	8	-22	-25	-26	-74	-24.7	-.479
14	52	52	51	51.7	9	9	7	-25	-25	-30	-80	-26.7	-.517
16	52	52	51	51.7	10	11	11	-22	-19	-18	-59	-19.7	-.382
21	51	51	50	50.7	9	9	5	-24	-24	-35	-83	-27.7	-.547
22	51	51	50	50.7	11	10	8	-18	-21	-26	-65	-21.7	-.428
24	51	51	50	50.7	13	11	12	-12	-18	-14	-44	-14.7	-.291
26	51	51	50	50.7	9	9	7	-24	-24	-29	-77	-25.7	-.507

Table 6

Column 19

Columns	Frequencies	Coincidences	Différences	Indices of coincidence
2	51	16	- 3	-.06
4	51	9	-24	-.47
5	51	8	-27	-.53
6	51	10	-21	-.41
8	51	5	-36	-.71
9	51	7	-30	-.59
11	51	15	- 6	-.12
13	51	9	-24	-.47
14	51	7	-30	-.59
15	51	10	-21	-.41
16	51	6	-33	-.65
17	50	8	-26	-.52
21	50	9	-23	-.46
22	50	6	-32	-.64
23	50	13	-11	-.22
25	50	10	-20	-.40
26	50	9	-23	-.46
27	50	6	-32	-.64
28	50	9	-23	-.46

Table 7

Column 21

Columns	Frequencies	Coincidences	Différences	Indices of coincidence
4	51	13	-12	-.24
5	51	10	-21	-.41
6	51	11	-18	-.35
8	51	10	-21	-.41
9	51	9	-24	-.47
13	51	16	- 3	-.06
14	51	7	-30	-.59
15	51	10	-21	-.41
16	51	7	-30	-.59
17	50	5	-35	-.70
22	50	9	-23	-.46
25	50	11	-17	-.34
26	50	7	-29	-.58
27	50	14	- 8	-.16
28	50	11	-17	-.34

Table 8

Columns	Total Frequencies per column			Average Frequency	Coincidences per column			Différences			Totals of Differences	Average Differences	Average of Indices of coincidence
	13	21	27		13	21	27	13	21	27			
4	52	51	51	51.3	14	13	17	-10	-12	0	-22	- 7.3	-.142
5	52	51	51	51.3	11	10	12	-19	-21	-15	-55	-18.3	-.357
6	52	51	51	51.3	13	11	10	-13	-18	-21	-52	-17.3	-.337
8	52	51	51	51.3	11	10	14	-19	-21	- 8	-48	-160	-.313
15	52	51	51	51.3	13	10	11	-13	-21	-18	-52	-17.3	-.337
25	50	50	50	50.3	11	11	13	-18	-17	-11	-46	-15.3	-.304
28	51	51	50	50.3	11	11	13	-18	-17	-11	-46	-15.3	-.304

Table 9

Alphabet 1 (Columns 5, 6, 9, 14, 16, 17, 22, 26, 28)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	10	5	16	26	12	11	2	6	3	17	4	6	25	12	6	6	7	»	5	8	9	19	»	1	13

Alphabet 2 (Columns 4, 8, 13, 15, 21, 25, 27)

A	B	C	D	E	F	G	H	1	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
22	3	4	7	9	»	5	6	»	9	19	»	17	6	12	7	4	3	»	3	7	»	15	3	9	9

Alphabet 3 (Columns 3, 7, 12, 20, 24)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
»	»	»	12	2	12	»	8	4	4	8	»	2	1	»	14	7	6	7	2	2	14	10	8	1	4

Alphabet 4 (Columns 2, 11, 19, 23)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	2	2	»	7	2	2	13	13	2	5	11	2	5	9	7	1	»	1	4	2	3	»	»	1	1

Alphabet 5 (Columns 1, 10, 18)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
»	2	5	»	3	8	1	»	2	5	6	7	10	2	1	»	»	3	8	»	»	7	3	4	»	»

Table 10

Alphabet 1.

Clear............	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher..........	K	L	M	O	N	R	T	V	W	Y	A	B	C	E	D	U	(X)	F	Z	G	P	H	I	Q	J	(S)

Alphabet 2.

Clear............	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher..........	E	X	P	H	A	Q	U	D	K	L	(I)	J	S	O	N	C	(F)	W	M	Y	G	Z	R	B	T	(V)

Alphabet 3.

Clear............	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher..........	W	Y	Z	E	D	I	J	S	F	(G)	N	Q	U	K	V	T	(L)	X	H	P	M	(O)	(A)	R	(B)	(C)

Alphabet 4.

Clear............	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher..........	O	F	G	Z	I	B	C	N	E	(X)	(R)	T	V	H	A	S	(W)	K	P	L	Y	M	Q	J	U	(D)

Alphabet 5.

Clear............	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	Q	X	Y	Z
Cipher..........	F	G	(H)	K	V	(A)	B	C	E	(P)	(D)	R	(T)	W	S	J		L	O	M		E	N	I		