Codebreakers: Arne Beurling and the Swedish Crypto Program during World War II

by Bengt Beckman

PROVIDENCE, RI, AMERICAN MATHEMATICAL SOCIETY,
2003. 259 PP., US $39, ISBN 0-8218-2889-4

REVIEWED BY HÅKAN HEDENMALM

The author of this book, Bengt Beckman, is one of early members of the Swedish cipher bureau FRA of Försvarsstaben (Defense Staff Headquarters), which was operational in 1941 but officially founded a year later. By the time Beckman came to FRA as a conscript in 1946, there was much discussion of Arne Beurling (1905–1986), the mathematics professor who had made himself famous at FRA by breaking the German code of the *Geheimschreiber* (developed by Siemens in the 1930s) at a time pivotal for Sweden during World War II. This feat is of the same order of magnitude as the British effort to break the *Enigma* code during the same war. In England as well as in Sweden, mathematicians played a vital role for the intelligence deciphering part of the war effort; perhaps the most famous mathematician working for the British at Bletchley Park was Alan Turing. The Swedish effort to keep a low profile with regard to this intelligence gathering was quite successful; indeed, the importance of Beurling's contribution to Sweden's ability to keep out of the war was, until recently, known only to narrow circles inside Sweden. By now, more than sixty years have passed, and the veil of secrecy has been lifted; Beckman, who stayed with FRA until 1991, is able to tell the story as he remembers it, from what he picked up a long time ago, as well as from recent in-depth interviews with people more closely involved.

This story first aired in a 1993 Swedish Television documentary *G som i hemlig* (G as in secret), produced by Beckman and Olle Häger. In the book, Beckman is able to tell a much more detailed story, of course. With the translation to English, commissioned by the American Mathematical Society, the material is now available to a considerably wider audience. The translator, Kjell-Ove Widman, who himself has been involved in cryptology at the Swiss company Krypto AG, has done a very thorough job and produced a very readable text. However, the style differs a little from the original: Beckman tells a story by the campfire, but Widman's translation sets higher literary standards. Having for the moment assumed a slightly critical stance, let me also mention that the map of Stockholm on the page following xviii places Karlaplan a bit off, somewhere in the forest area north of the Royal Institute of Technology (KTH); the mark should be placed a little bit further southeast. It is also unfortunate that the suggested explanation of Beurling's analysis is marred by cipher typos (on pp. 80, 82).

The book takes a historical perspective on ciphers and begins with an exercise to decipher a coded message from the 18th century. This is quite enjoyable; the cipher is of simple substitution type, and it is just a matter of running a frequency analysis to guess the most common letters of the cipher key. Then the perspective changes a little, and automatic ciphering machines enter the picture, along with the Swedish names Damm, Hagelin, and Glydén. Then, a description of radio signal interception and cryptanalysis before 1939 follows.

The Kingdom of Sweden was poorly prepared for the war that broke out on the European continent on September 1, 1939. The situation became particularly dire on April 9, 1940, when Germany invaded neighboring Denmark and Norway. As Sweden could not afford a massive military build-up, it became imperative to be able to second-guess the German intentions regarding Sweden. Then Sweden's foreign policy could be modified to be more palatable for the Germans, and hence avoid actual invasion. This was done quite successfully—German shipments of materials and supplies as well as of troops were permitted in sealed transit trains through Sweden—and it is commonly believed that this is the reason Sweden was able to remain outside the war.

But this is not the whole story. The invasion of Norway offered Sweden the chance not to second-guess but to actually read the potential enemy's cards. The diplomatic traffic between occupied Oslo and Berlin was transmitted along Swedish telegraph lines, and the Swedes were able to tap the messages. The only problem was that the messages were not in plain text; moreover, the encryption was not of simple substitution type, as could be seen from a simple frequency analysis. Given the sheer volume of encrypted traffic, it was suspected that a machine was doing the encryption automatically. One day in 1940 Beurling, who had already been involved with some simpler cryptanalysis tasks for the Swedish Defense Department, collected the tapped telegraph traffic at the Karlaplan office dated May 25 and May 27, 1940, which he believed to be essentially free of transcription errors. After a couple of weeks, he had more or less cracked the code. This was an impressive feat, especially compared with the British *Enigma* effort, which was based on the physical capture of an encryption machine from the Germans. If we think of the *Geheimschreiber* encryption as a kind of substitution cipher, then the cipher key apparently was changing with each new letter of the message. Also, the initial key settings were altered every few days. The way the *Geheimschreiber* was made, it would not begin cyclically repeating its cipher on any given message, for the number of possible encodings was much much bigger than the total quantity of information exchanged over the entire war.

Beurling never revealed how he performed his feat; he would say that a magician never reveals his tricks. Nevertheless, Beckman offers a possible explanation, based on a reconstruction attributed to Carl-Gösta Borelius. The encryption may have been perfect in theory, but in practice telegraph lines were not 100 percent reliable in those days, so the German telegraphers would frequently rerun parts of the message, using the *same* code. This allowed Beurling to get a foot in the door, and using some sound hypotheses regarding the nature of possible codes on teleprinters (where each letter corresponds to a sequence of five 0s and 1s)—essentially combinations of permutations and transpositions—he was able to complete his task. It should be noted that Beurling did this with a rather small data sample, and without actually having seen a *Geheimschreiber*. Today a *Geheimschreiber* is on display in the Beurling library of the Mathematics Department at Uppsala University in Sweden, where Beurling worked in the 1940s.

At first, the Swedes carried out the deciphering manually, in accordance with Beurling's instructions, but later, and certainly by 1942, machines—called *Apps*—were doing the job. The value of having cracked the *Geheimschreiber* depreciated toward the end of the war. The Germans sensed that their transmissions were being read, and reacted to it. By that time, however, the risk that Sweden would get dragged into the war was much reduced.

Beurling was a deep mathematician equipped with a difficult temperament. The stories about his disagreements, rows, or even outright fights with colleagues are widely known in mathematical circles in Scandinavia. Some of these stories are retold in this book. Beurling was apparently quite charming to the ladies, and this aspect of his life, based on interviews with Anne-Marie Yxkull Gyllenband, takes up a chapter. He married twice. His first wife is not mentioned by name in the book, but it is known that she worked as a physician, and Beurling had two children with her. Later, in 1950, he met his second wife, Karin Lindblad, at the party his student Lennart Carleson hosted to celebrate his thesis defense at Värmlands nation, one of the student clubs in Uppsala. As far as I know, Karin was a friend of Carleson's, and was Förste Kurator at Värmlands at the time, the highest post a student could assume at a student club in Uppsala. Karin and Arne remained together for the rest of their lives.

Beurling worked in three areas of mathematical analysis: potential theory, harmonic analysis, and complex analysis. His collaborators were few but well chosen: Ahlfors, Deny, Helson, and Malliavin. Probably it was his impressive collaboration and deep friendship with Lars Ahlfors that landed him the position of permanent member at the Institute for Advanced Study in Princeton, New Jersey, in 1954. In Princeton, he took over the office previously occupied by Albert Einstein. It is unfortunate that Beurling was not able to continue on American soil the extremely productive period he enjoyed in Uppsala in the 1940s, with students such as Göran Borg, Lennart Carleson, Yngve Domar, Carl-Gustav Esseen, and Bo Kjellberg. Had he been able to wield more influence in Princeton, the period of abstraction in mathematical analysis, which was such a dominant theme in the 1950s and 1960s, might have been balanced by a deep and elegant approach that focused not on form but on content.

Bengt Beckman has produced a fascinating book that acquaints us with some of the stars of 20th-century Scandinavian mathematics. In addition, we gain some insights into basic cryptology.

Department of Mathematics
The Royal Institute of Technology
S-10044 Stockholm, Sweden
e-mail: haakanh@math.kth.se