INTRODUCTION TO RSA ON THE HURRY

BURTON ROSENBERG
UNIVERSITY OF MIAMI

Contents

1. Necessary Number Theory

1.1. **Notation.** The typical notation for working modulo n is a tag such as,

$$y = ax + b \pmod{n}$$

While this makes clear in what algebraic system does one interpret the arithmetic. However, it is cumbersome and therefore I do not use this notation often. It just needs to be kept in mind what is the algebraic system, and there are often many.

I will write (a, b) for $\gcd(a, b)$.

1.2. **Bezout's Theorem.** A key theorem here is Bezout's, which notes that the greatest common divisor of two elements is the linear combination of the two elements. The euclidean algorithm that efficiently computes (a, b) can be extended to give the numbers s and t as described in Bezout's.

$$E(a, n) \to (s, t) \text{ s.t. } s\,a + t\,n = (a, n)$$

The group of units in $\mathcal{Z}_n$ is defined as $\mathcal{Z}_n^* = \{\, a \in \mathcal{Z}_n \,|\, (n, a) = 1 \,\}$. The Bezout result then gives a multiplicative inverse for any unit.

Date: November 19, 2021.

1.3. **Little Fermat Theorem.** Given $a \in \mathcal{Z}_n^*$ being invertible, the map $a(x) \mapsto a\,x$ is a permutation on $\mathcal{Z}_n$. Hence,

$$\begin{aligned} \Pi_{x \in \mathcal{Z}_n^*} x &= \Pi_{a \in \mathcal{Z}_n^*} a\,x \\ &= a^{\phi(n)} \Pi_{x \in \mathcal{Z}_n^*} x \end{aligned}$$

since this is entirely in the group of units we can cancel the large product across both sides, for all $a \in \mathcal{Z}_n^*$,

$$a^{\phi(n)} = 1$$

This is the Little Fermat Theorem (LFT).
For p a prime, $\phi(p) = p - 1$.
For distinct primes, p, q and $n = pq$, in $\mathcal{Z}_n$, among the $n-1$ non-zero elements that are not relatively prime to n are kp and $k'q$, for $k = 1, \ldots, q-1$ and $k' = 1, \ldots, p-1$. Therefore,

$$\phi(pq) = pq - 1 - (q-1) - (p-1) = pq - q - p + 1 = (p-1)(q-1)$$

1.4. **Square Roots mod $n = pq$.** In $\mathcal{Z}_n^*$, with n the product of two distint primes, there are four solutions to $x^2 = 1$.
Given the relation $x\,p + y\,q = 1$, the square is also equal to one. Then,

$$(x\,p + y\,q)^2 = (x\,p - y\,q)^2 = 1 \pmod n$$

so $\zeta = x\,p - y\,q$ is a square root of 1 mod pq, and is not 1 or -1. Note that,

$$\zeta + 1 = x\,p - y\,q + 1 = x\,p - y\,q + x\,p + y\,q = 2x\,p,$$

and

$$\zeta - 1 = x\,p - y\,q - 1 = x\,p - y\,q - x\,p - y\,q = -2y\,q.$$

Sincd $q \not| x$ and $p \not| y$, so, $(\zeta + 1, pq) = p$ and $(\zeta - 1, pq) = q$.
This result can also be shown using $x^2 - 1 = (x+1)(x-1) = 0 \pmod n$.

2. RSA cryptosystem

2.1. **Description of RSA.**

- Generation:
  1. Chose distinct primes $p, q \in \mathcal{Z}$ and let $n = pq$;
  2. Choose an $e \in \mathcal{Z}_{\phi(n)}^*$.
  3. Compute $d = e^{-1} \pmod{\phi(n)}$.
  4. The public key is (n, e).
  5. The secret key is (n, d).
- Encryption: For a message $m \in \mathcal{Z}_n^*$, the encryption is $c = m^e \pmod n$.
- Decryption: The decryption of $c \in \mathcal{Z}_n^*$ is $m = c^d \pmod n$.

As e and d are inverses in $\mathcal{Z}^*_{\phi n}$, then $(m^e)^d = m^{k\phi(n)+1} = (m^{\phi(n)})^k\, m = 1 \pmod{n}$.

2.2. **The security of RSA.** Given n and $\phi(n)$, then $p + q = n + 1 - \phi(n)$. The factors p, q are then the roots of the quadraic $(x - p)(x - q) = 0$. This form is expressable in n and $\phi(n)$.

$$(x - p)(x - q) = x^2 - px - qx + n = x^2 - (n + 1 - \phi(n))x + n$$

Therefore, given $n, \phi(n)$ we easily compute the factors p, q using the quadratic formula.

To keep d a secret, $\phi(n)$ must not be known. It is therefore necessary that the factors of n not be known. We have seen above, that knowing $\phi(n)$ and n gives the factors of n, so either we factor n or we know $\phi(n)$ by some other way.

However, perhaps d can be known without $\phi(n)$ being known. Write $ed - 1 = 2^s t$. Suppose a decryption exponent d is found out, by any method, with the property that for any $x \in \mathcal{Z}^*_n$,

$$x^{ed-1} = (x^t)^{2^s} = 1$$

There is a sequence leading to 1, that must pass through one fo the four square roots of one,

$$x^t, (x^t)^2, (x^t)^4, \ldots, \beta, \beta^2 = 1$$

If $\beta = \pm\zeta$, the non-trivial square root of one mod n, then we can factor n.

Therefore, we have a probabilistic factoring algorithm for n, if we have the exponent d, showing that calculation of the exponent d is at least as hard as factoring.