Rivest-Shamir-Adelman (RSA) Cryptosystem

Reading from Special Topics Textbook:

Chapter 1, Section 1.5, pp. 36-43.

Public Key Cryptosystem

- Idea discovered by Diffie-Hellman.
- Compute a **public key** *E* and **private** key *D*, where *E* is used to encrypt messages and *D* is be used to decrypt messages that have been encrypted using *E*.
- These keys need to be chosen so that it is computationally infeasible to derive *D* from *E*. Anyone with the public key *E* is able to encrypt a message, but only someone knowing *D* is able (in real time) to decrypt an encrypted message.
- Many public-key cryptosystems have been designed. In this course we cover the popular **RSA** public key cryptosystem due to Rivest, Shamir, and Adleman.

RSA Cryptosystem

1. Compute two large primes p and q and set $n = pq$.

2. The Euler Totient Function $\varphi(n)$ is the number of positive integers less than n that are co-prime (relatively prime) to n

   Chose the public key e to be a positive integer that is relatively prime to $\varphi(n) = (p - 1)(q - 1)$, i.e., $\gcd(e,\varphi(n)) = 1$.

3. Computer the private key using formula

$$d = e^{-1} \pmod{\varphi(n)}$$

PSN. Using Principle of Inclusion-Exclusion show that

$$\varphi(n) = (p - 1)(q - 1).$$

Implementation of RSA – Computing Large Primes *p* and *q*

- Small primes can be computed quickly. But how to compute a large prime p involving for example 500 digits.
- The solution is to randomly generate the 500 digits and use Miller-Rabin to test whether it is prime.
- The issue then becomes will a positive result occur, i.e., a prime be found, in reasonable time or are the prime numbers too sparse.
- It follows from one off the deepest theorems in mathematics known as the prime number theorem that they are not.

Prime Number Theorem

Let $\pi(n)$ be the number of primes less than or equal to *n*. The prime number theorem states that

$$\pi(n) \sim \frac{n}{\ln n}$$

This means take on the order log *n* numbers less than or equal to *n* you are likely to find a prime. But log *n* is on order the number of digits.

Implementation of RSA – Computing Private Key from Public Key

PSN. Describe algorithm for computing private key $d = e^{-1} \pmod{\Phi(n)}$

RSA
Encryption and Decryption of Messages

Message m is encrypted using formula:

$$c \equiv m^e \pmod{n}.$$

Encrypted message c is decrypted using formula:

$$m \equiv c^d\ (mod\ n).$$

Theorem on which correctness of RSA is based

Theorem 1.5.5 Let $n = pq$ where p and q are two prime numbers, let e be an integer that is relatively prime with $\varphi(n)$, and let d be its multiplicative inverse mod $\varphi(n)$, that is, $ed \equiv 1 \pmod{\varphi(n)}$. Then, for any integer m,

$$m^{ed} \equiv m \pmod{n}.$$

Euler’s Totient Theorem

To prove the Theorem will need to apply a generalization of Fermat’s Little Theorem due to Euler called Euler’s Totient Theorem.

Theorem (Euler). Let n and b be relatively prime numbers. Then

$$b^{\varphi(n)} \equiv 1 \pmod{n} .$$

Note that $\varphi(n) = n - 1$ for n prime so we obtain Fermat’s Little Theorem as a corollary.

Proof of Euler's Totient Function

Let $Z_n^* = \{r_1, r_2, \dots, r_{\varphi(n)}\}$ be the set of number between 1 and *n* – 1, inclusive, that are relatively prime to *n*. For example

$$Z_{12}^* = \{1,5,7,11\}$$

Let $b \in Z_n^*$. Then, b is invertible mod *n.*

b^{-1} can be computed using extended Euclid GCD.

Proof of Euler's Totient Theorem cont'd

Since b is invertible mod *n*, it follows that $br \pmod{n}$ determines a permutation of Z_n^*, i.e.,

$$\{br_1 (\mathrm{mod}\, n), br_2 (\mathrm{mod}\, n), \ldots, br_{\varphi(n)} (\mathrm{mod}\, n)\}$$

$$= \{r_1 (\mathrm{mod}\, n), r_2 (\mathrm{mod}\, n), \ldots, r_{\varphi(n)} (\mathrm{mod}\, n)\}$$

Therefore,

$$(br_1)(br_2) \cdots (br_{\varphi(n)}) \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$$

$$\Rightarrow b^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}$$

$$\Rightarrow b^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof of Theorem 1.5.5

Since $ed \equiv 1 \pmod{\varphi(n)}$, it follows that

$$ed = \varphi(n)k + 1,$$

for some integer k.

Proof. Case gcd(m,n) = 1

First suppose that gcd(m,n) = 1. Then, applying Theorem 1.5.2 (Euler's Totient Theorem), we

$$
\begin{aligned}
m^{ed} &= m^{\varphi(n)k + 1} \\
&= (m^{\varphi(n)})^{k} m \\
&\equiv (1)^{k} m \ (mod\ n) \\
&= m \ (\text{mod } n)
\end{aligned}
$$

Case gcd(m,n) > 1

Then we have two subcases:

1. n divides m.

2. either m is divisible by q but not p or n is divisible by p but not q.

Subcase 1. n divides m

$$m^{ed} \equiv 0^{ed} \equiv 0 \equiv m \pmod{n}.$$

Subcase 2. Either m is divisible by q but not p or n is divisible by p but not q.

Assume without loss of generality that m is divisible by q but not p. Then, by Fermat's little theorem (Corollary 1.5.3),

$$m^{p-1} \equiv 1 \pmod{p}. \qquad (1)$$

Applying (1) we obtain:

$$m^{k\varphi(n)} = m^{k(p-1)(q-1)} \equiv (m^{p-1})^{k(q-1)} \equiv (1)^{k(q-1)} \equiv 1 \pmod{p}.$$

It follows that

$$m^{k\varphi(n)} = jp + 1 \qquad (2)$$

for some integer j. Multiplying both sides of (2) by m we obtain:

$$m^{k\varphi(n)+1} = jpm + m.$$

But, since m is divisible by q, jpm is divisible by n, so that we have:

$$m^{ed} = m^{k\varphi(n)+1} \equiv (m^{k\varphi(n)})m \equiv (1)m \equiv m \pmod{n}.$$

Prime Number Dilemma

Should you say "All prime numbers are odd except one“?

Or "All prime numbers are odd except two?"