

Introduction to Modern Cryptography

You Lin¹

¹School of Physics and Astronomy
University of Minnesota
Minneapolis, Minnesota 55455

Last modified May 15, 2004.

Abstract

A very simple introduction to cryptography. People can understand how number theory can be put into computer security.

1 Brief Overview

Computer information can be simplified to a set of integer numbers. Cryptography, in general, is a way to encode these numbers, make them unreadable during transmission, and then decode them after received.

Encoding and decoding, if put into mathematical language, are just two functions with adjustable parameters. These adjustable parameters can be called *keys*. As a simplified example, we assume a is information before encoding, b is information after encoding, then encoding:

$$b = a + k_1$$

decoding:

$$a = b + k_2$$

Here, k_1 is called *encoding key* and k_2 , *decoding key*. Obviously, if $k_2 = -k_1$, this process will work correctly.

This process is oversimplified and, apparently, the sender and receiver has to negotiate keys before real transmission. Anyone who intercepted the encoding key k_1 will be able to calculate decoding key k_2 and the cryptography is cracked. It seems that sending encoding key is inevitable. So if we can make the decoding key virtually impossible to be calculated from the encoding key, we'll be safe.

2 Euler's theorem

Well, Euler's name is pretty familiar to scientists. Although he lived centuries ago, his contribution still affects today's world. In this section, we're going to talk about one of his work in number theory that shapes current computer cryptographic world.

Since we'll deal with all integer numbers, we assume all symbols represent integer numbers from now on.

Definition of Remainder and Module

- If $a = kp + c$, and $0 \leq c < p$, then c is the *remainder* of a with module p . e.g. $27 = 2 \times 13 + 1$, then the remainder of 27 with module 13 is 1.
- If a and b has the same remainder with module p , we write $a = b, (\text{mod } p)$. e.g. $40 = 27, (\text{mod } 13)$.

Before I present the theorem, I assume you know what *prime numbers* and *composite numbers* are.

Theorem 1. [Fermat-Euler] $n^{p-1} = 1 \pmod{p}$ if p is a prime number and $n \not\equiv 0 \pmod{p}$.

Proof. • We can define remainder function f of x , so $x = f(x) \pmod{p}$.

- Now define a group $\mathbb{G} = \{1, 2, \dots, p-1\}$, $\forall a, b \in \mathbb{G}$ define group product: $a \times b \equiv f(ab)$.
- Obviously, serie $f(n^0), f(n^1), \dots, f(n^N), \dots$, is periodic. Just label smallest period N . Then $f(n^N) = 1$.
- It seems we can generate a subgroup \mathbb{G}_a of \mathbb{G} such that $\mathbb{G}_0: \{f(n^k), k = 0, 1, \dots, +\infty\}$. Recall that the number of elements in a group is called the rank of the group, we can verify
 - Rank of \mathbb{G}_0 is exactly N .
 - Rank of \mathbb{G} is exactly $p-1$.
- Then by group theory, N is a factor of $p-1$. Thus $f(n^{p-1}) = 1$ or $n^{p-1} = 1 \pmod{p}$.

3 RSA Cryptography

How does Euler's theorem apply in cryptography? From Euler's theorem, if p, q are different prime numbers,

- Case $a \not\equiv 0 \pmod{p}$, and $a \not\equiv 0 \pmod{q}$:
 $a^{k(p-1)(q-1)} = 1 \pmod{p}$ and $a^{k(p-1)(q-1)} = 1 \pmod{q}$, $\Rightarrow a^{k(p-1)(q-1)} = 1 \pmod{pq}$.
- Case $a \equiv 0 \pmod{p}$, and $a \not\equiv 0 \pmod{q}$:
 $a^{k(p-1)(q-1)} = 1 \pmod{q}$, $\Rightarrow a = \lambda p$; $a^{k(p-1)(q-1)} = kq + 1$, $\Rightarrow a^{k(p-1)(q-1)+1} = a(kq + 1) = \lambda p(kq + 1) = \lambda k p q + \lambda p$, $\Rightarrow a^{k(p-1)(q-1)+1} = \lambda k p q + a$.
- Case $a \equiv 0 \pmod{p}$, and $a \equiv 0 \pmod{q}$:
 $a = 0 \pmod{pq}$

thus, for all cases:

$$a^{k(p-1)(q-1)+1} = a \pmod{pq}$$

Assume $de = k(p-1)(q-1) + 1$, if we define $a(0 \leq a < pq)$ is the message that needs to be encrypted, and b is the encrypted message, then encoding:

$$b = \text{mod}(a^d, pq)$$

Decoding:

$$a = \text{mod}(b^e, pq)$$

The point is p, q are very large prime numbers and $e \gg d$. Encoding key pair is (d, pq) and decoding pair is (e, pq) . The receiver send encoding pair to sender and keep decoding pair secret (not sent). Even if the encoding pair is intercepted, one have to factorize pq before calculating decoding key e .

So for a cracker, the most challenging thing is to factorize a large number.

Mathematician have developed a lot of methods for factorization.

4 Known Factorization Algorithms

There's no universal way of efficiently factorizing a large number. Additional information must be provided before one can use any of the algorithms.

The simplest method of finding factors is *direct search factorization*, or *trial division*.

The fastest fully proven deterministic algorithm is the Pollard-Strassen method (Pomerance 1987; Hardy et al. 1990).

5 Application

- This encryption-decryption method is widely used on internet security, such as SSH, https protocols.
- The level of security is determined by the digits of the primes that consist the key. The more the digit, the harder it will be cracked.
- As an example, I got a pair of encoding key

$$d = 19 \quad , \quad pq = 708769961907180595350100233381261559$$

using the Elliptic Curve Method (ECM for short) [1], I got

$$p = 692686090402164613 \quad , \quad q = 1023219567604826443$$

then

$$e = 447644186467693006505807100236381371$$

Thus the decoding pair is found.

6 Quantum Computer

Such cryptography is safe until quantum computer comes into being. Quantum Turing machine was discovered by P. Shor in the Bell Laboratory of AT&T in 1994 to be able to compute factorization much faster than current computer. Besides cryptography, quantum computer will make more insight into the basics of quantum mechanics. This is why we, physicists will be interested in it.

There are several fundamental physical questiones that need to be answered. Two of them which have been identified as the most crucial are error correction and the decoherence problem.

References

- [1] Lenstra, H. W. Factoring integers with elliptic curves. *Annals of Mathematics* 126 (1987), 649-673.