Introduction to Cryptography

Alvin Lin

January 2018 - May 2018

Cryptography and Mathematics

Greatest Common Divisor

The greatest common divisor is the largest number that divides evenly into two numbers a and b. In general, we will denote the greatest common divisor of a and b as $gcd(a, b)$. Formally:

$$gcd(a, b) = max[k, \text{such that } k|a \text{ and } k|b]$$

Properties:

- $gcd(0, 0) = 0$
- Because we require that the greatest common divisor be positive:

$$gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b)$$

- In general, $gcd(a, b) = gcd(|a|, |b|)$
- Because all non-zero numbers divide 0, we have $gcd(a, 0) = |a|$.
- Two integers a and b are **relatively prime** if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if $gcd(a, b) = 1$.

Modular Arithmetic

Modular arithmetic is extremely important for aymmetric cryptography (RSA, elliptic curves, etc). Some historical ciphers can be elegantly described with modular arithmetic. Generally speaking, most cryptosystems are based on sets of numbers that are discrete and finite.

Let a, r, m be integers and $m > 0$. We write

$$a \equiv r \mod (m)$$

if $(r - a)$ is divisible by m. m is called the modulus and r is called the remainder.

- $12 \equiv 3 \mod (9)$
- $34 \equiv 7 \mod (9)$
- $-7 \equiv 2 \mid (0)$

The remainder is not unique. It is somewhat surprising that for every given modulus m and a number a, there are infinitely many valid remainders. By convention, we usually agree on the smallest positive integer r as the remainder. This integer can be computed as:

$$a \equiv qm + r$$

where $0 \leq r \leq m = 1$. This is just a convention. Algorithmically, we are free to choose any other valid remainder to compute our crypto functions. Properties:

- $(a + b) \mod (m) \equiv a \mod (m) + b \mod (m)$
- $(a \cdot b) \mod (m) \equiv a \mod (m) \cdot b \mod (m)$

Modular Division

Rather than performing a division, we prefer to multiply by the inverse:

$$\frac{b}{a} \equiv b \times a^{-1} \mod (m)$$

The inverse a^{-1} is defined such that:

$$a \times a^{-1} \equiv 1 \mod (m)$$

The inverse of a number $a \mod (m)$ only exists if and only if:

$$gcd(a, m) = 1$$

Example:

$$5/7 \mod (9)$$

the inverse of $7 \mod (9)$ is 4, since $7 \times 4 \equiv 28 \equiv 1 \mod (9)$, hence:

$$5/7 \equiv 5 \times 4 = 20 \equiv 2 \mod (9)$$

Modular Reduction

Modular reduction can be performed at any point during a calculation.

$$3^8 = 3^4 \times 3^4 = 81 \times 81 \equiv 4 \times 4 \mod (7) = 16 \mod (7) = 2 \mod (7)$$

An Algebraic View on Modulo Arithmetic: The Ring $\mathbb{Z}_m$

The integer ring $\mathbb{Z}_m$ has the following properties:

- **Closure:** We can add and multiply any two numbers and the result is always in the ring.
- **Addition and multiplication are associative:** For all $a, b, c \in \mathbb{Z}_m$:

  $$a + (b + c) = (a + b) + c \quad a \times (b \times c) = (a \times b) \times c$$

  and addition is **commutative**: $a + b = b + a$
- **The distributive law holds:** $a \times (b + c) = (a \times b) + (a \times c)$ for all $a, b, c \in \mathbb{Z}_m$
- There is the **neutral element 0** with respect to addition. For all $a \in \mathbb{Z}_m, a + 0 \equiv a \mod (m)$.
- For all $a \in \mathbb{Z}_m$, there is always an **additive inverse** element a such that $a + (-a) \equiv 0 \mod (m)$.
- There is the **neutral element 1** with respect to multiplication. For all $a \in \mathbb{Z}_m, a \times 1 \equiv a \mod (m)$
- The **multiplicative inverse** a^{-1} $a \times a^{-1} \equiv 1 \mod (m)$ exists only for some, but not for all, elements in $\mathbb{Z}_m$.

Roughly speaking, a ring is a structure in which we can always add, subtract, and multiply, but we can only divide by certain elements (namely by those for which a multiplicative inverse exists). We consider the ring $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. The elements 0, 3, and 6, do not have inverses since they are not coprime to 9.

Shift (or Caesar) Cipher

The shift cipher is an ancient cipher allegedly used by Julius Caesar. To use it, each plaintext letter is replaced by another one. The replacement rule is very simple: take the letter that follows after k positions in the alphabet. Note that letters wrap around the end of the alphabet, which can be elegantly expressed as reduction modulo 26.

- Encryption: $y = e_k(x) \equiv x + k \mod (26)$
- Decryption: $x = d_k(y) \equiv y - k \mod (26)$

The shift cipher is not secure since it is vulnerable to an exhaustive key search since the key space is only 26. It is also vulnerable to letter frequency analysis, similar to any attack against substitution ciphers.

Affine Cipher

The Affine cipher is an extension of the shift cipher, rather than just adding the key to the plaintext, we also multiply by the key. We use a key consisting of two parts: $k = (a, b)$.

- Encryption: $y = e_k(x) \equiv ax + k \mod (26)$
- Decryption: $x = d_k(y) \equiv a^{-1}(y - k) \mod (26)$

Since the inverse of a is needed for decryption, we can only use values for which $gcd(a, 26) = 1$.

Vigenére Cipher

The Vigenére Cipher is one of the simplest and best known polyalphabetic substituion ciphers. In this scheme, each plaintext letter is Caesar-shifted by a different amount according to the key, which is usually a repeating keyword.

Hill Cipher

The Hill Cipher was developed by Lester Hill in 1929. It's strength was that it completely hid single-letter frequencies. It was strong against a ciphertext-only attack but easily broken by a known plaintext attack. The Hill cipher is done by taking a matrix as the key:

$$K = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Given the plaintext HELP, we split it into 1×2 column vectors so that they can be multiplied by the key vector:

$$\begin{bmatrix} H \\ E \end{bmatrix}, \begin{bmatrix} L \\ P \end{bmatrix} \rightarrow \begin{bmatrix} 7 \\ 4 \end{bmatrix}, \begin{bmatrix} 11 \\ 15 \end{bmatrix}$$

The ciphertext is produced by multiplying the key matrix with the column vectors.

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 11 \end{bmatrix} \mod (26)$$
$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 0 \end{bmatrix} \mod (26)$$

This yields the cipher text 18-11-11-0 or RKKA. Decryption is done by computing the inverse of the key matrix K^{-1} and repeating the same process.

The Euclidean Algorithm

Computing the greatest common divisor of two numbers a and b is easy for small numbers. We can factor both numbers and look for the highest one that they share in common. Factoring is complicated and often infeasible for large numbers. The Euclidean algorithm follows from the idea that $gcd(a, b) = gcd(a - b, b)$. The core idea is to reduce the problem of finding the gcd of two numbers to that of the gcd of two smaller numbers. We repeat this process recursively until we reach $gcd(b, 0) = b$.

Example

$$gcd(710, 310)$$

$$\begin{aligned} 710 &= 2 \times 310 + 90 \\ 310 &= 3 \times 90 + 40 \\ 90 &= 2 \times 40 + 10 \\ 40 &= 4 \times 10 \end{aligned}$$

$$gcd(710, 310) = 10$$

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech