Introduction to Cryptography

Angelo Panariti

February 14, 2024

1 The modulo operator

Let $a, r, m \in Z$ and $m > 0$, we write $a \equiv mod\ m$. If m divides $(a - r)$

$$m|(a - r)$$

1.1 Exercise

$$a = 13, m = 9, r =?$$

$$13 \equiv 4\ mod\ 9$$

$$a - r = (13 - 4) = 9$$

1.2 Computation of the remainder

given: $a, m \in Z$

$$a = qm$$

1.2.1 Example

$$a = 42, m = 9$$

$$42 = 4 \cdot 9 + 6 \rightarrow 6 \equiv r = 6$$

Check $(42 - 6) = 36, 9/36$

$$42 = 3 \cdot 9 + 15 \rightarrow r = 15$$

Check $(42 - 15) = 27, 9/27$

$$42 = 5 \cdot 9 + (3 \cdot 3) \rightarrow r = 3$$

Check $(42 - 3) - 39, 9/39$.
The remainder is not unique.

1.3 Equivalence Classes

Ex: $a = 12$, $m = 5$

$$12 \equiv 2 mod 5$$

$$12 \equiv 7$$

1.3.1 Definition

The set $\{..., -8, -3, 2, 7, 12, 17, ...\}$ forms an equivalence class modulo 5. All members of the class behave equivalent modulo 5. Let's look at all the equivalence classes modulo 5..

$$A = \{..., -10, -5, 0, 5, 10, ...\}$$
$$B = \{..., -9, -4, 1, 6, 11, 16, ...\}$$
$$C = \{..., -8, -3, 2, 7, 12, ...\}$$
$$D = \{..., -7, -2, 3, 8, 13, ...\}$$

$13 \cdot 16 - 8 = 200 \equiv 0 mod 5$

If we replace every number of this expression with the respective number in the equivalence class, we get:

$3 \cdot 1 = 3 - 3 \equiv 0 mod 5$

$8 \cdot 6 - (-7) = 48 + 7 = 55 \equiv 0 mod 5$

1.4 Important application

Ex:

$$3^8 \ mod \ 7 \equiv ?$$

1.4.1 First way

$$3^8 = 6561 \equiv \ 2$$

1.4.2 Second way

$$3^8 = 3^4 \cdot 3^4 = \ 81 \cdot 81 \equiv 4 \cdot 4 = 16 \equiv \ 2 \ mod \ 7$$

2 Rings: An Algebraic View on Modular Arithmetic

2.1 Definition

The integer ring Z_m consists of-

1. $Z_m = \{0, 1, 2, \ldots, m-1\}$
2. Two operators "+" and "$\cdot$" $sothatforall$a,b,c $\in Z_m$
   (a) $a + b \equiv c \ mod \ m$
   (b) $a \cdot b \equiv \ d \ mod \ m$

2.2 Example for multiplicative inverses

$$m = q$$

$$2 \cdot 2^{-1} \equiv 1 \ mod \ 9$$

$$2 \cdot 5 \equiv 1 \ mod \ 9$$

$$2^{-1} \equiv 5 \ mod \ 9$$

3 Shift (or Caesar) Cipher

Idea: shift every letter in the alphabet by a certain number of letters. For example, let's take a variable $k = 3$ (an arbitrary number). So for instance, A is replaced with D, B is replaced with E, X is replaced with A (at the end of the alphabet, we just just "wrap around" and start at the beginning again), et cetera (modulo 26).

3.1 Shift Cipher

Let $x, y, k \in Z_26$

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

3.2 Affine Cipher

$$k = (a, b)$$

$$y \equiv a \cdot x + b \ mod \ 26$$

$$y - b \equiv a \cdot x$$

3.3 Two attacks possible

1. frequency analysis
2. brute-force attack

4 Stream Ciphers

Streaming bits, flowing one after another. A stream cipher encrypts bits individually and its equation is pretty similar to the Shift Cipher one:

Encryption:

$$y_i = e(x_i) \equiv x_i + s_i \ mod 2$$

Decryption:

$$x_i = d(y_i) \equiv y_i - s_i \ mod 2$$

Question: Why are decryption and encryption the same operation?

$$d(y_i) \equiv y_i - s_i \ mod 2$$
$$\equiv (x_i + s_i) + s_i \ mod 2$$
$$\equiv x_i + 2s_i \ mod 2$$
$$\equiv x_i \ mod 2$$

$$x_i, y_i, z_i \in Z = \{0, 1\}$$

mod 2 addition and subtraction are the same operation.
Closer look at the mod2 add:

x	s_i	y_i mod 2
0	0	0
0	1	1
1	0	1
1	1	0

mod2 addition is the same as the XOR operation.
Example: encryption of ASCII letter "A"

$$x_7...x_1 = 1000001$$
$$s_7...s_1 = 0101101$$
$$s_7...s_1 = 1101100$$

Question: how to generate the key stream bits s_i? Somehow related to randomness!

5 Random numbers generators (RNG)

We distinguish between three types of RNGs:

1. True random numbers generators (TRNG)
    - True random numbers stem from physical processes, e.g: coin-flipping, dice rolls, etc.
2. Pseudo random number generators (PRNG)
    - PRNs are computed, i.e, they are deterministic. (if you can compute something, it's not really random). Often they are computed with the following function, namely: $s_0 = seed$, each subsequent $s_i+1 = f(s_i)$, recursively being computed.
- Ex: rand() function in ANSI C, it has a fixed $s_0 = 123456$, $s_{i+1} = 1103515245s_i + 12345 \ mod \ 2^31$
3. Cryptographically secure PRNGs (CSPRNG)

- CPRNGs are PRNs, but they are not deterministic. They are not computed deterministically, but rather based on the hardware's random number generator. They are therefore not truly random. So they are computed with an additional property: the numbers are unpredictable
- Informal definition: given n output bits, $s_i, s_i + 1, ..., s_{i+n-1}$, it is computationally infeasible to construct s_n

6 One Time Pad (OTP)

- Goal: build a "perfect" encryption algorithm.
- Definition: A cipher is unconditionally secure (or information theoretically secure) if it cannot be broken by infinite computing resources.
- Definition: The One Time Pad (OTP) is a stream cipher where:
  1. The first stream bits s_i stem from a TRNG
  2. Each key stream bit is used only once

  – Big drawback: key is as long as the message. Ex: encryption of a $400MB$ file $\rightarrow 8 \cdot 400MB = 3.2GBit$ of key

7 Linear Congruential Generator (LCG)

- Idea: Use a key-stream s_i from a PRNG.

$$S_g = seed$$

$$S_{i+1} = A \cdot S_i + B \ mod \ m, A, B, S_i, \in Z_m$$

key $k = (A, B)$. Remark: A, B, S_i are $[log_2 m]$ bits long.
Attack example: Oscar knows: $x_1, x_2, x_3.1) Oscar computes S_1, S_2, S_3$

$$S_2 \equiv A^1 \cdot S_1 + B^1 \ mod \ m$$

$$S_2 \equiv A \cdot S_1 + B \ mod \ m$$

Linear equation system with 2 unknowns:

$$A = (S_2 - S_3) \cdot (S_1 - S_2)^{-}1 \ mod \ m$$

$$B = S_2 - S_1(S_2 - S_3)(S_1 - S_2)^{-}1 \ mod \ m$$