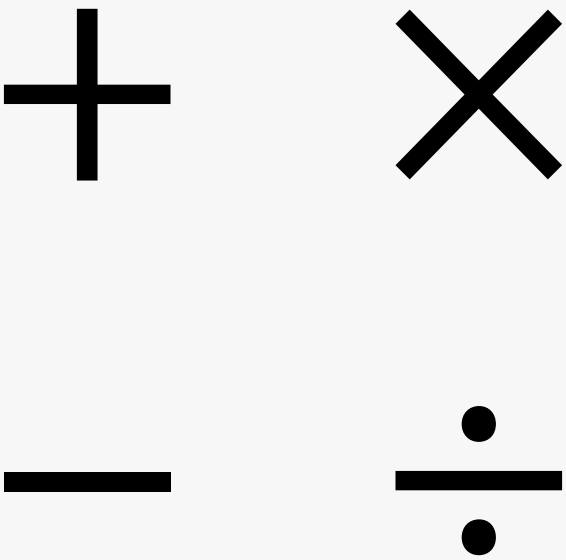


Outline

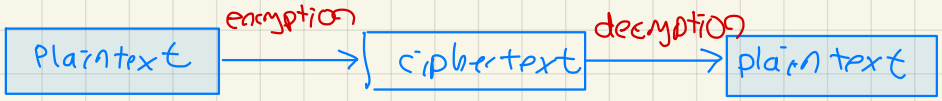
- What is cryptography
- Ciphers
- Cryptanalysis
- Shift cipher
- Modular arithmetic
- Group

What is cryptography ?

- Protocols for secret communication, under the presence of eavesdropper

- Idea : Transform original message before sending it

- Basic terms :



secure key : ① mutual (shared key (symmetric)
② (public key, private key) (assymmetic)
encryption decryption

cryptanalysis : Attack on the cryptography scheme
Read : even without secure key
Change : change the original msg
Forge : send msg to Bob in the name of Alice

Encryption and decryption are known to be public

Security of cryptosystem is based on secure key.

Shift Cipher

Alphabets : A B C D E F . . . X Y Z

secure key : K is an integer from 0 to 25

Encryption : Each letter in the plaintext, replaced it with the letter K position to the right in the alphabet list.

k=1 k=2

A → B → C
B → C → D
C → D
D → E

Plaintext : HELLO
k=1, ciphertext : IFMMO
k=2, ciphertext : JGNNP

X → Y
Y → Z
Z → A

Decryption : "shift to left by K position"

Crytoanalysis : Brute Force attack
Try all possible keys 26

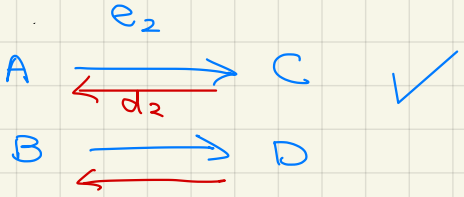
Formal Definitions

$e_k(m)$ is an encryption function that maps plaintext m to ciphertext c with the key k

$d_k(m)$ is a decryption function maps ciphertext → plaintext with the key k.

inverse of $e_k(m)$

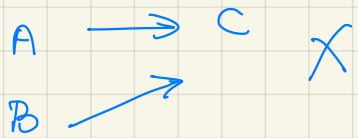
$m = d_k e_k(m)$



e_k is a one-to-one function

If $e_k(m) = e_k(m')$ then

$m = d_k(e_k(m)) = d_k(e_k(m')) = m'$



K : space of keys
M : space of plaintexts
C : space of ciphertexts
e : encryption scheme
d : decryption scheme

A (K, M, C, e, d) cipher is "successful"

(1) easy to compute ciphertext $e_k(m)$, $k \in K$, $m \in M$ — Alice

(2) easy to decrypt ciphertext if key k is known — Bob

(3) difficult to decrypt ciphertext without key k. — Eve

(4) secure against known plaintext attack

(5) secure against chosen plaintext attack.

easy vs difficult

Understand Integers

Several "hard" problems provide crypto keys

Notation: $\mathbb{Z}$

Divisibility

- a divides b $(a|b)$, a does not divide b $(a \nmid b)$

$\rightarrow b = ac$ for some integer c

- statement not an operation
- a is a divisor of b

Remainder

- $n = qd + r$

d is divisor (modulus, m)
q is quotient (NJA)
r is remainder (residue)

$$13 \overline{)37} \quad 2$$
$$26$$
$$11 \leftarrow \text{remainder}$$

- Given n, d, there are infinite posibilities for q, r

$37 = 2 \cdot 13 + 11$
$37 = 3 \cdot 13 - 2$

- By convention, $0 \leq r < d$

Modular Arithmetic

modulus

$a, b \in \mathbb{Z}$, $m \in \mathbb{Z}$

$a \equiv b \bmod m$ (a congruent to b modulo m)

if $m \mid a-b$

Example: $17 \equiv 7 \bmod 5$ $(5 \mid 17-7)$

$19 \not\equiv 6 \bmod 11$ $(11 \nmid 19-6)$

Reduce modulo m

a reduce modulo m: take the remainder of division of a by m

$37 \bmod 13 = 11$

$50 \bmod 26 = 24$

$-1 \bmod 26 = ?$ 25

$64 \bmod 26 = ?$ (12)

$64 - 26 = 38$

$38 - 26 = 12$

$-1 + 26 = 25$

Shift ciphers using modular arithmetic

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1.7: Assigning numbers to letters

Encryption : plaintext + k mod 26

Decryption : ciphertext − k mod 26

$\mathbb{Z}/26\mathbb{Z} = \{0, 1, 2, \ldots, 25\}$

Set of remainders modulo 26