

# Some Number Theory

## Modulo Operation:

**Question:** What is  $12 \bmod 9$ ?

**Answer:**  $12 \bmod 9 \equiv 3$  or  $12 \equiv 3 \pmod{9}$

**Definition:** Let  $a, r, m \in \mathbb{Z}$  (where  $\mathbb{Z}$  is a set of all integers) and  $m > 0$ . We write

$a \equiv r \pmod{m}$  if  $m$  divides  $r - a$ .

$m$  is called the *modulus*.

$r$  is called the *remainder*

$$a = q \cdot m + r \qquad 0 \leq r < m$$

# Number Theory (cont.)

**Example:**  $a = 42$  and  $m=9$

$$42 = 4 \cdot 9 + 6 \text{ therefore } 42 \equiv 6 \pmod{9}$$

**Ring:**

**Definition:** The ring  $Z_m$  consists of

1. The set  $Z_m = \{0, 1, 2, \dots, m-1\}$
2. Two operations “+” and “ $\times$ ” for all  $a, b \in Z_m$  such that

- $a + b \equiv c \pmod{m} (c \in Z_m)$
- $a \times b \equiv d \pmod{m} (d \in Z_m)$

**Example:**  $m = 9$        $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$$6 + 8 = 14 \equiv 5 \pmod{9}$$

$$6 \times 8 = 48 \equiv 3 \pmod{9}$$

## Properties of the ring $Z_m = \{0, 1, \dots, m-1\}$

1. The additive identity “0”:  $a + 0 = a$
2. The additive inverse of  $a$ :  $-a = m - a$  s.t.  $a + (-a) \equiv 0 \pmod{m}$
3. Addition is closed i.e if  $a, b \in Z_m$  then  $a + b \in Z_m$
4. Addition is commutative  $a + b = b + a$
5. Addition is associative  $(a + b) + c = a + (b + c)$
6. Multiplicative identity “1”:  $a \times 1 \equiv a \pmod{m}$
7. The multiplicative inverse of  $a$  exists if  $\gcd(a, m) = 1$  and denoted as  $a^{-1}$  s.t.  $a^{-1} \times a \equiv 1 \pmod{m}$
8. Multiplication is closed i.e if  $a, b \in Z_m$  then  $a \times b \in Z_m$
9. Multiplication is commutative  $a \times b = b \times a$
10. Multiplication is associative  $(a \times b) \times c = a \times (b \times c)$

## Some Remarks on the ring $Z_m$

- Roughly speaking a ring is a mathematical structure in which we can add, subtract, multiply, and even sometimes divide.

**Example:** Is the division  $4/15 \pmod{26}$  possible?

In fact,  $4/15 \pmod{26} = 4 \times 15^{-1} \pmod{26}$

Does  $15^{-1} \pmod{26}$  exist ?

It exists only if  $\gcd(15, 26) = 1$ .

$15^{-1} \pmod{26} = 7$

therefore,  $4/15 \pmod{26} = 4 \times 7 \pmod{26} = 28 \equiv 2 \pmod{26}$

- The modulo operation can be applied whenever we want  
 $(a + b) \pmod{m} = [(a \pmod{m}) + (b \pmod{m})] \pmod{m}$   
 $(a \times b) \pmod{m} = [(a \pmod{m}) \times (b \pmod{m})] \pmod{m}$

## Exponentiation in $Z_m$

**Example:**  $3^8 \bmod 7 = ?$

$$3^8 \bmod 7 = 6561 \bmod 7 = 2 \text{ since } 6561 = 937 \times 7 + 2.$$

Or

$$3^8 = 3^4 \times 3^4 = 3^2 \times 3^2 \times 3^2 \times 3^2$$

$$3^8 \bmod 7 = [(3^2 \bmod 7) \times (3^2 \bmod 7) \times (3^2 \bmod 7) \times (3^2 \bmod 7)] \bmod 7$$

$$3^8 \bmod 7 = 2 \times 2 \times 2 \times 2 \bmod 7 = 16 \bmod 7 = 2$$

The ring  $Z_m$  and thus the modulo arithmetic is of central importance to modern public-key cryptography. In practice, the order of the integers involved in PKC are in the range of  $[2^{160}, 2^{1024}]$ . Perhaps even larger

# Classical Cryptosystems

## Shift Cipher:

Letters of the alphabet are assigned a number as below

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

## Algorithm:

Let  $P = C = K = \mathbb{Z}_{26}$  and  $x \in P, y \in C, k \in K$

*Encryption:*  $E_k(x) = x + k \pmod{26}$ .

*Decryption:*  $D_k(x) = x - k \pmod{26}$ .

# Classical Cryptosystems – Shift Cipher

**Remark:** When  $k = 3$  the shift cipher is given a special name - *Caesar Cipher*.

**Example:** Let the key  $k = 17$

Plaintext:  $X = A T T A C K = (0, 19, 19, 0, 2, 10)$ .

Ciphertext :  $Y = (0+17 \bmod 26, 19+17 \bmod 26, \dots)$

$Y = (17, 10, 10, 17, 19, 1) = R K K R T B$

## Attacks on Shift Cipher

1. Exhaustive Search: Try all possible keys.  $|K|=26$ .  
Nowadays, for moderate security  $|K| \geq 2^{80}$ ,  
for recommended security  $|K| \geq 2^{100}$ .
2. Letter frequency analysis (Same plaintext maps to same ciphertext)

# Classical Cryptosystems – Affine Cipher

## Algorithm:

Let  $P = C = \mathbb{Z}_{26}$  and  $x \in P, y \in C$

*Encryption:*  $E_k(x) = y = \alpha \cdot x + \beta \pmod{26}$ .

The key  $k = (\alpha, \beta)$  and  $\alpha, \beta \in \mathbb{Z}_{26}$

**Example:**  $k = (\alpha, \beta) = (13, 4)$

INPUT = (8, 13, 15, 20, 19)  $\Rightarrow$  ERRER

ALTER = (0, 11, 19, 4, 17)  $\Rightarrow$  ERRER

There is no one-to-one map btw plaintext and ciphertext space. What went wrong?

*Decryption:*  $D_k(x) = x = \alpha^{-1} \cdot y + \beta$

# Classical Cryptosystems – Affine Cipher

## Key Space:

$\beta$  can be any number in  $Z_{26}$ . 26 possibilities

Since  $\alpha^{-1}$  has to exist we can only select integers in  $Z_{26}$

s.t.  $\gcd(\alpha, 26) = 1$ . Candidates are

$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

Therefore, the key space has  $12 \cdot 26 = 312$  candidates.

## Attack types:

1. *Ciphertext only*: exhaustive search or frequency analysis
2. *Known plaintext*: two letters in the plaintext and corresponding ciphertext letters would suffice to find the key.

**Example** : plaintext: IF=(8, 5) and ciphertext PQ=(15, 16)

$$8 \cdot \alpha + \beta \equiv 15 \pmod{26}$$

$$5 \cdot \alpha + \beta \equiv 16 \pmod{26} \Rightarrow \alpha = 17 \text{ and } \beta = 9$$

What happens if we have only one letter of known plaintext?

# Classical Cryptosystems – Affine Cipher

## Attack types:

3. *Chosen plaintext*: Chose A and B as the plaintext. The first character of the ciphertext will be equal to  $0 \cdot \alpha + \beta = \beta$  and the second will be  $\alpha + \beta$ .
4. *Chosen ciphertext* : Chose A and B as the ciphertext.

## Substitution Ciphers

Each letter in the alphabet is replaced (substituted) by another letter. More precisely, a permutation of the alphabet is chosen and applied to the plaintext.

The shift and affine ciphers are examples of substitution ciphers.

Since ciphertext preserves the statistic of the language used in

The plaintext, the frequency analysis is an effective way of

Breaking substitution ciphers.

<http://www.sherlockian.net/canon/stories/danc.html>

# Block Ciphers

- In the substitution ciphers, changing one letter in the plaintext changes exactly one letter in the ciphertext.
- This greatly facilitates finding the key using frequency analysis.
- Block ciphers prevents this by encrypting a block of letters simultaneously.
- Many of the modern (symmetric) cryptosystems are block ciphers. DES operates on 64 bits of blocks while AES uses 128 bits of blocks(192 and 256 are also possible).

## Example: Hill Cipher

The key is an  $n \times n$  matrix whose entries are integers in  $Z_{26}$ .

# Block Ciphers – Hill Cipher

**Example:** Let  $n=3$  and the key matrix be

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

and the plaintext be  $ABC = (0, 1, 2)$  then the encryption operation is a vector-matrix multiplication

$$(0,1,2) \times \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (0,23,22) \pmod{26} \Rightarrow AXW \text{ (ciphertext)}$$

In order to decrypt we need the inverse of key matrix  $M$ , which is

$$N = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}$$

## Block Ciphers – Hill Cipher

If we change one letter in the plaintext, all the letters of the ciphertext will be affected.

Let the plaintext be BBC instead of ABC then the ciphertext

$$(1,1,2) \times \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (1,25,25) \pmod{26} \Rightarrow \text{BZZ (ciphertext)}$$

Claude Shannon, in *Communication theory of secrecy systems*  
Bell Systems Technical Journal 28, (1949), 656-715,

introduced properties that a good cryptosystems should have:

- 1. Diffusion:** one character change in the plaintext should effect as many ciphertext characters as possible, and v.v.
- 2. Confusion:** The key should not relate to the ciphertext in a simple way.

# **RSA Public Key Cryptosystem**

Based on *Integer Factorization* problem

Choose two prime numbers:  $p$  and  $q$  (keep them secret!!)

Calculate the modulus  $n = pq$  (make it public)

Calculate  $\Phi(n) = (p-1)(q-1)$  (Euler Totient function, secret)

Select a random integer such that  $e < \Phi$  and  $\gcd(e, \Phi) = 1$ .

Calculate the unique integer  $d$  such that  $ed \equiv 1 \pmod{\Phi}$ .

**Public key:**  $(n, e)$

**Private key:**  $(d)$

# **RSA Encryption**

**User B encrypts a message  $m$  for User A**

Obtains A's authentic public key  $(n, e)$

Represents the message as an integer  $m$  in the interval  $[0, n - 1]$

Computes the exponent  $c = m^e \bmod n$

Sends  $c$  (ciphertext) to A.

**User A decrypts  $c$  using his private key**

Computes the exponent  $m_ = c^d \bmod n$

In fact,  $m_ = m$ .

# Why RSA works?

**Fact 1.**  $ed \equiv 1 \pmod{\Phi} \Rightarrow ed = 1 + k\Phi$ .

**Fact 2.**  $m^{p-1} \equiv 1 \pmod{p}$  (by Fermat's Little theorem)

**From Fact 2.**  $m^{1+k(p-1)(q-1)} \equiv m \pmod{p}$

$$c^d \pmod{n} = m^{ed} \pmod{n} = m^{1+k\Phi} \pmod{n}$$

$$= m^{1+k\Phi} \pmod{n} = m^{1+k(p-1)(q-1)} \pmod{n} = m$$

# Modular Exponentiation in RSA

The most time consuming operation in RSA cryptography

## How to perform Modular Exponentiation?

**Example:**  $c = m^{53} \bmod n$   $53 = (110101)_2$

Scan the bits of the exponent from left-to-right

$$c = m$$

$$c = m^2 \cdot m = m^3$$

$$c = m^6$$

$$c = m^{12} \cdot m = m^{13}$$

$$c = m^{26}$$

$$c = m^{52} \cdot m = m^{53}$$

**Modular multiplication is the most important operation !!**

## **RSA (cont'd)**

Most popular PKC in practice

Tens of dedicated crypto-processor is specifically designed to perform modular multiplication in a most efficient way.

**Disadvantage:** Long key length,  
complex key generation scheme.

For acceptable level of security for commercial applications  
1024 – bit keys are used.

In constrained devices such as smart cards, cell phones and PDAs, it is hard to store, communicate keys and handle operations involving long integers

# Alternative PKCs

- **El-Gamal (Discrete-Log based) Cryptosystems**

Also suffers from long keys

- **NTRU (Lattice Based)**

Utilizes short keys

Propriety (License issues prevent from wide implementation)

Recently, a weakness found in the signature scheme

- **Elliptic Curve Cryptosystems**

Emerging public key cryptography standard for constrained devices.