# Cryptography and Network Security

Concepts of Network Security

- data confidentiality
  - confidentiality
  - privacy
- data integrity
  - data integrity
  - system integrity
- data availability

Data Availability:

- Data is made to be available for authorised person

Data Authentication

- Data is need to be sent by authorised person

Data Accountability

- maintain the track records of activities being performed

Security Attacks:

- passive attacks
- Active attacks

Passive attacks:

- unauthorised won't modify it
- Dilection of this attack is difficult
- we can supress by cryptography algos

Types
- reading msg content
- Traffic Analysis

Active Attacks:

- unauthorised user will alter the message

Types
- masquerade
- replay
- denial of service
- modifying message content

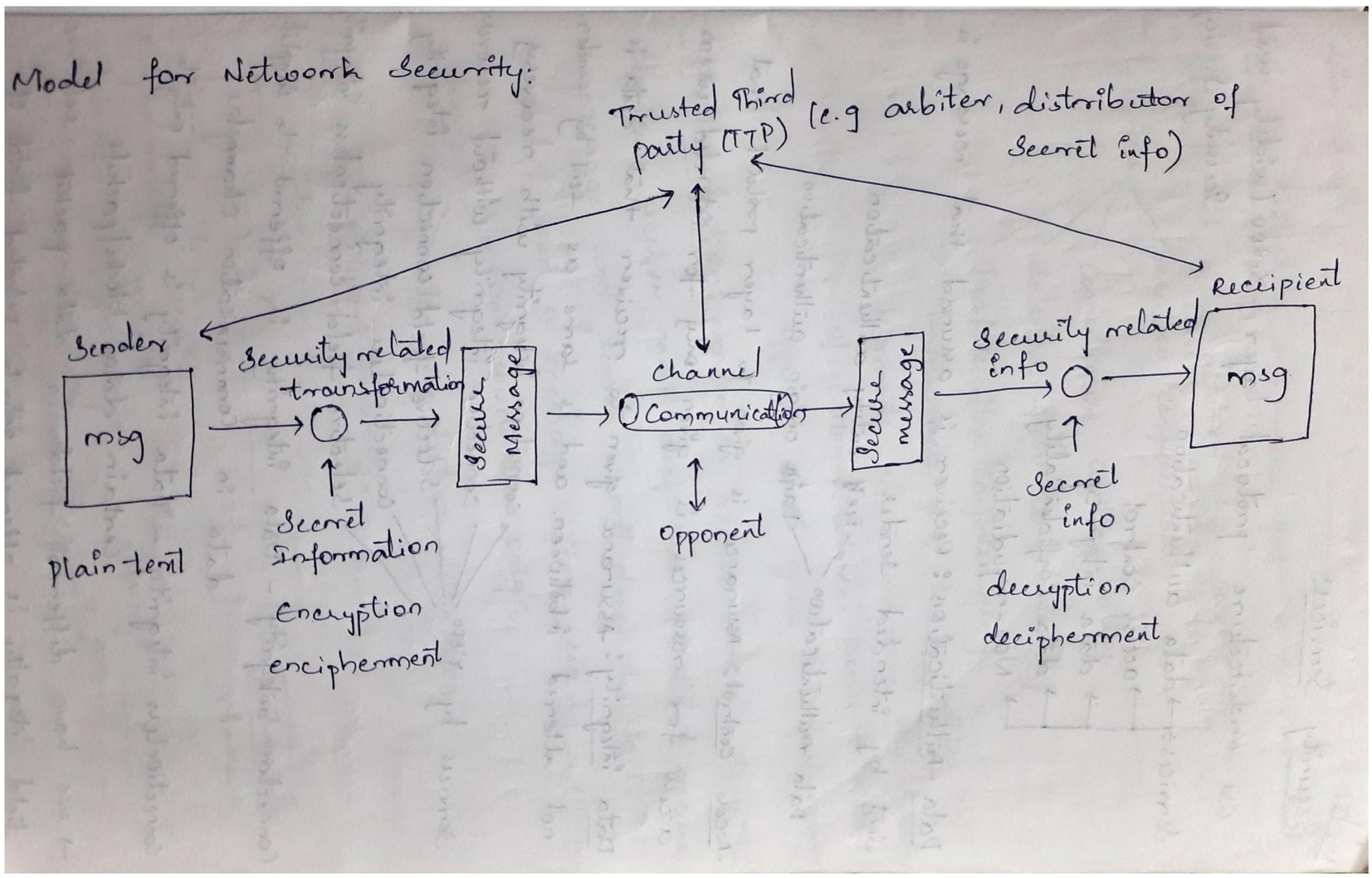
| Cryptography | Normal |
|---|---|
| plain text | original msg |
| cipher text | Secure msg |

Security related transformation → cryptography

encipherment → process of converting plain text to cipher text

Decipherment → process of converting cipher text to plain text.

## Model for Network Security:



16/6/22

## Security Services:

OSI Architecture protocal layer - X.800 (widely used Security Service)

Services:
- data authentication
- access control
- data integrity
- data confidentiality
- Non-repudiation

Data Authentication: Receiver is assured that message is sent by intended sender

Data Authentication
- Peer entity authentication
- Data origin authentication

Access control: Assurance is given to Layer protocol that access for resources is given only for intended users

Data integrity: Assurance given to receiver that data is not altered inbetween. and is same as sent by sender.

Services by X.800
- connection integrity with recovery
- connection integrity without recovery
- selective field connection integrity
- connectionless integrity
- selective field connectionless integrity

Connection Integrity - Data integrity is offered to Complete data in Communication channel

Connectionless integrity - Data integrity is offered only to certain data blocks/packets

→ we have different fields in data packet. selective field integrity is offered only to selected fields of

data packet.

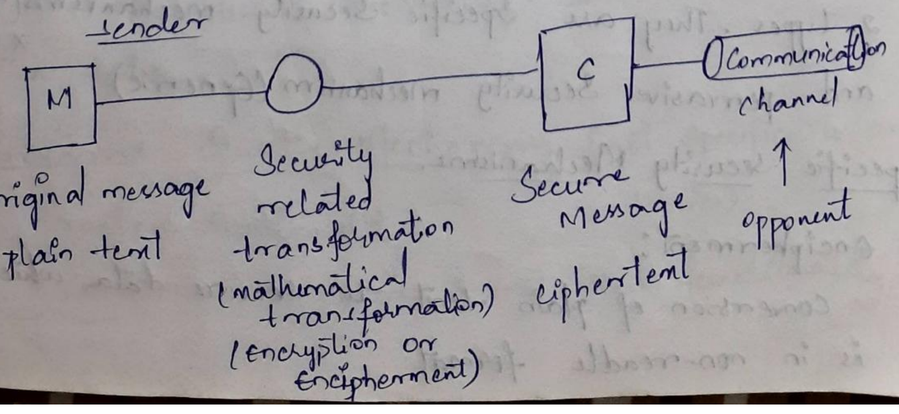
**Data Confidentiality:** Assurance given to receiver that data is not being altered by opponent.

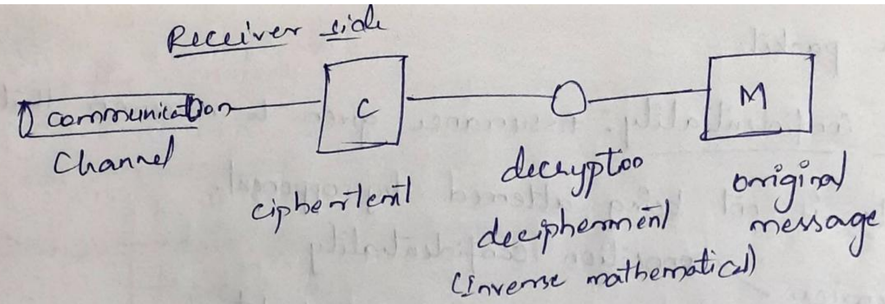
Services
- connection confidentiality
- Connectionless confidentiality
- Selective field confidentiality
- Traffic flow confidentiality
  - ↳ Assurance given to 2 parties that opponents cannot observe the transfer of patterns between them so that opponent cannot guess the next message

**Non-Repudiation:** Sender or receiver cannot deny the services. Receiver cannot deny that he didn't receive a message and sender cannot deny the fact that he didn't send a message after sending a message.

Services
- Non-repudiation, origin
- Non-repudiation, destination

**Model for Network Security:**






Symmetric model:

Same encryption and decryption method is used on both sender and receiver side by sharing a same key using Trusted Third party (TTP), distributor, arbiter.

Asymmetric model:

Here message is encrypted using public key of receiver and receiver decrypts the message with his private key. Here also third parties maintain public key's of all users

17/8/22

Security Mechanisms:

→ Security Mechanisms are broadly classified into 2 types. They are Specific security mechanisms (for X.800) and perrvasive Security mechanism (Generic)

Specific security Mechanisms:

1. Encipherment:
   Conversion of plain text to secure data which is in non-readle format.

2. Digital signature:

It is a procedure to add a additional message to original message so that it acts as signature to ensure a specific sender

3. access control

4. Data integrity

5. ~~Authentication~~ Exchange

exchanging some blocks between sender and receiver before original message to prove the authentication

6. Traffic padding:

It is a mechanism where some bits are padded in b/w msg such that opponent cannot analyze the msg.

7. Routing control:

It is a mechanism where after a security breach is happened, this allows the source to select a physically secure channel to send data to receiver

8. Notarization:

TTP (Trusted Third party) are used to transfer the data

Pervasive security Mechanism (not specific to any service)

1. Trusted Functionality

Communication peers trust this functionality.

2. using Security label
3. event detection
4. Security audit trial
5. Security recovery (some mechanisms are available to recover after a Security breach)

## Number Theory Concepts:

### 1. Divisibility:

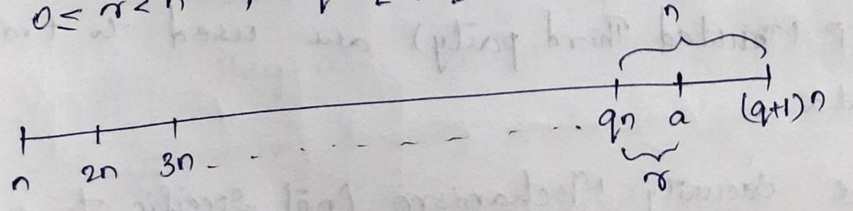
Properties:

- If $a/1$ then $a = \pm 1$
- If $a/b$ and $b/a$ then $a = \pm b$
- Any $b \neq 0$ divides $0$
- If $a/b$ and $b/c$ then $a/c$
- If $b/g$ and $b/h$ then $b/(m.g + n.h)$

### Divisibility algorithm:

$a = q * n + r$

$0 \leq r < n$ , $q = \lfloor n/a \rfloor$



## Modular arithmetic

11 mod 7 = 4

-11 mod 7 ⇒ (-11+7) mod 7 ⇒ (4+7) mod 7 ⇒ 3

2. Congruence:

if a mod n = b mod n then $a \equiv b \bmod n$

73 mod 23 = 4 $\quad 73 \equiv 4 \bmod 23$

4 mod 23 = 4

properties:

- $a \equiv b \pmod n$ if $n \mid (a-b)$
- $a \equiv b \pmod n$ implies $b \equiv a \bmod n$
- $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$
- $(a \bmod n + b \bmod n) \bmod n = (a+b) \bmod n$
- $(a \bmod n - b \bmod n) \bmod n = (a-b) \bmod n$
- $(a \bmod n \times b \bmod n) \bmod n = (a \times b) \bmod n$

## Exponentiation

$11^7 \bmod 13 = (11^{4+2+1}) \bmod 13$

$11 \bmod 13 = 11$

$11^2 \bmod 13 = 4$

$11^4 \bmod 13 = (11^2 \cdot 11^2) \bmod 13$

$= (4 \cdot 4) \bmod 13$

$= 3$

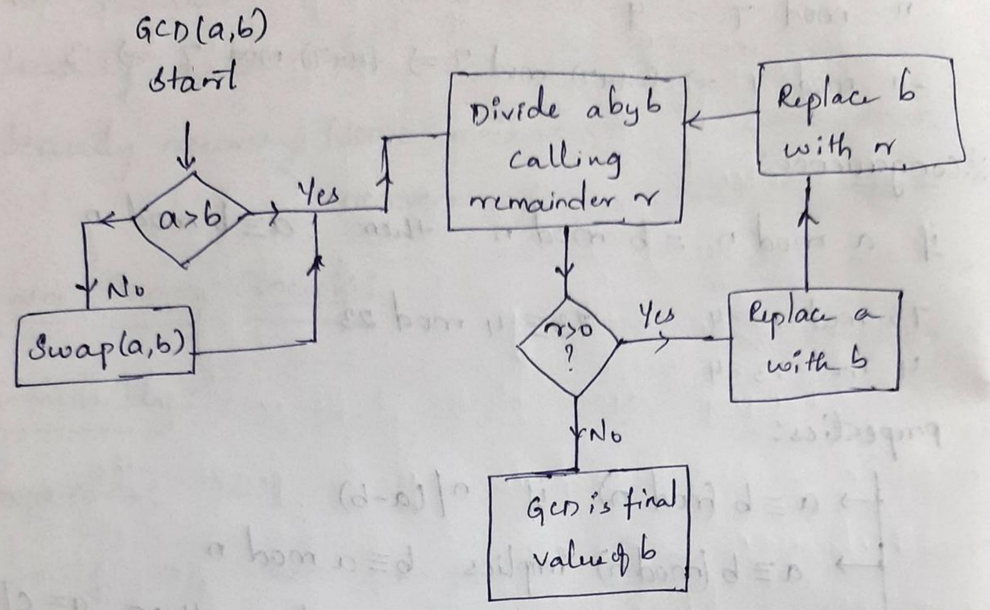
ans: $(3 \times 4 \times 11) \bmod 13 = 2$

4×4×4×11

4
64
×11
704
13

13)704(54
65
54

# Euclidean Algorithm




GCD (20,75)

Swap
a = 75
b = 20

divide r = 15 q = 3

a = 20
b = 15

divide q = 1 r = 5

a = 15
b = 5

divide q = 3 r = 0

5 is GCD

$a = q_1 b + r_1 \quad 0 < r_1 < b$

$b = q_2 r_1 + r_2 \quad 0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3 \quad 0 < r_3 < r_2$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n \quad 0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1} r_n + 0 \quad 0 < r_n$

$gcd(a,b) = r_n$

## Recursive function

```
GCD (a,b){
    if (a<b) {
        swap (a,b)
        if (b==0)
            return
        if (a%b==0)
            return b
        Return GCD (b, a%b)
}
```

## Modular Arthmetic (cont)

### Additive Inverse

if $(x+y) \bmod n = 0$

x's additive inverse is y

if $n = 8$

| | |
|---|---|
| 0 | 8 |
| 1 | 7 |
| 2 | 6 |
| ⋮ | |
| 7 | 1 |

} additive inverse

For all numbers additive inverse is there

### Multiplicative Inverse

if $(x * y) \bmod n = 1$

then y is multiplicative inverse of x

$1 \times 1 \bmod 8 = 1$

$3 \times 3 \bmod 8 = 1$

$5 \times 5 \bmod 8 = 1$

$2 \times ? \bmod 8 = 1$

$4 \times ? \bmod 8 = 1$

∴ it may have (or) may not for an element x multiplicative inverse

ex: n = 11

| | |
|---|---|
| 0 | x |
| 1 | 1 |
| 2 | 6 |
| 3 | 4 |
| 4 | 3 |
| 5 | x |
| 6 | 2 |
| 7 | x |
| 8 | x |
| 9 | x |
| 10 | x |

## Extended Euclidean Algorithm

d = gcd(a,b)

d = xa + by

gcd (1547, 560)

1547 = 2.560 + 427

560 = 1.427 + 133

427 = 3.133 + 28

133 = 4.28 + 21

28 = 1.21 + 7

21 = 3.7 + 0

7 = 28 - 1.21

= 28 - 1. (133 - 4.28)

23/08

## Extended Euclidean Algorithm

$d = \gcd(a,b)$ $a > b$

$d = ax + by$

ex: $\gcd(1547, 560) = 7$

to find: $x, y$ where $d = ax + by$ & $x, y$ are integers

ex: $7 = 1547x + 560y$

$\gcd(1547, 560)$

$1547 = 2 \cdot 560 + 427$

$560 = 1 \cdot 427 + 133$

$427 = 3 \cdot 133 + 28$

$133 = 4 \cdot 28 + 21$

$28 = 1 \cdot 21 + 7$

$21 = 3(7) + 0$ → GCD

$\rightarrow 21(1547 - 2 \cdot 560) - 16 \cdot 560 = 21 \cdot 1547 - 58 \cdot 560$

$\rightarrow 5 \cdot 427 - 16(560 - 1 \cdot 427) = 21 \cdot 427 - 16 \cdot 560$

$\rightarrow 5(427 - 3 \cdot 133) - 133 = 5 \cdot 427 - 16 \cdot 133$

$\rightarrow 7 = 28 - (133 - 4 \cdot 28) = 5 \cdot 28 - 133$

$\rightarrow 7 = 28 - 1 \cdot 21$

$7 = 21 \times 1547 - 58 \times 560$

Euclidean algorithm

$q_1 = \lfloor a/b \rfloor$

$r_1 = a \bmod b$ $a = q_1 b + r_1$

$r_2 = b \bmod r_1$ $b = q_2 r_1 + r_2$

$r_3 = r_1 \bmod r_2$

$\vdots$

$r_{n+1} = r_{n-1} \bmod r_n$

Extended Euclidean algorithm

| i | calculate | |
|---|---|---|
| -1 | $r_{-1} = a$ | $x_{-1} = 1 \quad y_{-1} = 0$ |
| 0 | $r_0 = b$ | $x_0 = 0 \quad y_0 = 1$ |
| 1 | $r_1 = a \bmod b$ | $x_1 = x_{-1} - q_1 x_0$ |
| | $q_1 = \lfloor a/b \rfloor$ | $y_1 = y_{-1} - q_1 y_0$ |
| 2 | $r_2 = b \bmod r_1$ | $x_2 = x_0 - q_2 x_1$ |
| | $q_2 = \lfloor b/r_1 \rfloor$ | $y_2 = y_0 - q_2 y_1$ |
| 3. | $r_3 = r_1 \bmod r_2$ | $x_3 = x_1 - q_3 x_2$ |
| | $q_3 = \lfloor r_1/r_2 \rfloor$ | $y_3 = y_1 - q_3 y_2$ |
| ⋮ | | |
| n | $r_n = r_{n-2} \bmod r_{n-1}$ | $x_n = x_{n-2} - q_n x_{n-1}$ |
| | $q_n = \lfloor r_{n-2}/r_{n-1} \rfloor$ | $y_n = y_{n-2} - q_n y_{n-1}$ |

$r_{n+1} = r_{n-1} \bmod r_n$

GCD $\quad r_n = 0$

find GCD (1759, 550) = 1

| i | $r_i$ | $q_i$ | $x_i$ | $y_i$ |
|---|---|---|---|---|
| -1 | 1759 | | 1 | 0 |
| 0 | 550 | | 0 | 1 |
| 1 | 109 | 3 | 1 | -3 |
| 2 | 5 | 5 | -5 | 16 |
| 3 | 4 | 21 | 106 | -339 |
| 4 | 1 gcd | 1 | -111 | 355 |
| 5 | 0 | 4 | x | y |

$x_1 = x_{-1} - q_1 x_0 = 1 - 3(0) = 1$

$y_1 = y_{-1} - q_1 y_0 = 0 - 3(1) = -3$

$x_2 = x_0 - q_2 x_1 = 0 - 5(1) = -5$

$y_2 = y_0 - q_2 y_1 = 1 - (-3)5 = 16$

$x_3 = x_1 - q_3 x_2 = 1 - 21(-5) = 106$

$y_3 = y_1 - q_3 y_2 = -3 - 21(16) = -339$

$x_4 = x_2 - q_4 x_3 = -5 - 1(106) = -111$

$y_4 = y_2 - q_4 y_3 = 16 - 1(-339) = 355$

$1 = -111 \times 1759 + 355 \times 550$

for each of the following eqns find x

$3x \equiv 4 \bmod 5$

$x = 3$

$9x \equiv 3 \bmod 7$

$x = 5$

$7x \equiv 6 \bmod 9$

$x = 6$

15 9
24 10
73 17
~~43~~ 24
52 31
2240 38+7
1760 45

find GCD(2740, 1760) using extended euclidean algorithm also find x & y

| i | $r_i$ | $q_i$ | $x_i$ | $y_i$ |
|---|---|---|---|---|
| -1 | 2740 | | 1 | 0 |
| 0 | 1760 | | 0 | 1 |
| 1 | 980 | 1 | 1 | -1 |
| 2 | 780 | 1 | -1 | 2 |
| 3 | 200 | 1 | 2 | -3 |
| 4 | 180 | 3 | -7 | 11 |
| 5 | 20 | 1 | 9 | -14 |

1-0

1 + 980

$-980 \times 2$

$-1960$

24/8 Prime numbers

if P has devisors only ±1 and ±P

Given any integer a can be factorred as prime number power some integer

$$a = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_n^{a_n}$$

$14 = 2^1 \times 7^1$

$15 = 3^1 \times 5^1$

$28 = 2^2 \times 7^1$

P is a set of prime numbers then any integer a can be expressed as $a = \prod_{p \in P} p^{a_p}$ where each $a_p \geq 0$

Multiplication of two numbers can be expressed as

$216 = 2^3 \times 3^3$

$300 = 2^2 \times 3^1 \times 5^2$

$18 = 2^1 \times 3^2 \times 5^0$

$gcd(300, 18) = 2^1 \times 3^1 \times 5^0$

we have to select prime factor power minimum out of the two, with prime factorization we can easily find gcd of two numbers.

$k = gcd(a, b)$

then $k_p = \min(a_p, b_p)$ for all p

## Fermat's Theorem:

If p is a prime number and a is an integer not divisible by p then $a^{p-1} \equiv 1 \bmod p$

### alternate form

$$a^p \equiv a \bmod p$$

Ex: a = 7 and p = 19

$$7^{18} \equiv 1 \bmod 19$$

(or)

$$7^{19} \equiv 7 \bmod 19$$

Here, the cases fail when a is divisible by p.

## Euler's totient function

→ It is represented as $\phi(n)$

→ $\phi(n)$ is defined as the number of numbers that are less than n that are relatively prime to n.

if n=5 then $\phi(n) = \{1, 2, 3, 4\}$

if n is prime then $\phi(n) = n-1$

if n=8 then $\phi(n) = \{1, 3, 5, 7\}$ so $\phi(n) = 4$.

n=14 $\{1, 3, 5, 9, 11, 13\}$ $\phi(n) = 6$

two prime numbers P, q } different prime numbers

if a number n = pq

$$\phi(n) = \phi(p) \times \phi(q)$$

$$\phi(n) = (p-1)(q-1)$$

p=2 q=7

$\phi(14) = (2-1) \times (7-1) = 1 \times 6 = 6$

$\phi(22) = (2-1) \times (11-1)$

$\phi(22) = 10$

Eulen's Theorem

→ for every a and n that are relatively prime to each other

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

alternative form

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

$a = 3, n = 10$

$\phi(n) = (2-1)(5-1) = 4$

$3^4 \bmod 10 = 1$

$3^5 \equiv 3 \bmod 10$

Properties of prime numbers

There are 2 useful properties of prime numbers that allows Rabin miller to construct the algorithm

1) n is odd then n can be expressed as

$n-1 = 2^k q$ where $k \geq 0$ and q is odd

i) $n = 7$

$6 = 2^1 \times 3$ here $k=1, q=3$

ii) $n = 11$

$10 = 2^1 \times 5$ here $k=1, q=5$

iii) $n = 13$

$12 = 2^2 \times 3$

$k=2 \quad q=3$

q is odd and k cannot be zero also

for x ✗.

1) If p is prime, a is a positive integer less than p then $a^r \bmod p = 1$

if and only if $a \bmod p = 1$ or $a \bmod p = -1 \bmod p$

Ex: $p = 7$, $a = 6$

$6^r \bmod p = 1$ as $6 \bmod 7 = 6 \Rightarrow 6 \bmod 7 = -1 \bmod 7$

$p = 11$, $a = 3$

$11^r \bmod 3 \neq 1$ as $3 \bmod 11 = 3 \neq -1 \bmod 11$
$\neq 1$

2) If p is a prime number greater than 2

$p - 1 = 2^k q$ with $k > 0$ and $q$ is odd

Let a be an integer $1 < a < p-1$ then one of the following conditions is true

1. $a^q \equiv 1 \bmod p$
2. one of the number $a^q, a^{2q}, a^{4q} \ldots a^{2^{k-1}q} \equiv -1 \bmod p$
$= p-1$

formally $a^{2^{j-1}q} \equiv -1 \bmod p = p-1 \quad 1 \leq j \leq k$

→ Rabin miller algorithm is constructed in a way to say a number may be prime

if these 2 properties fail then we say it is a composite number.

## Rabin miller Algorithm

Test(n)

Find integers k,q with $k>0$, q odd so that

$n-1 = 2^k q$

Select a random integer $1 < a < n-1$

if $a^q \bmod n = 1$ then return ("inconclusive")

for $j=0$ to $k-1$ do

if $a^{2^j q} \bmod n = n-1$ then return ("inconclusive")

return ("composite")

Ex: $n = 2047$, Let random number selected = 2

Here the output will be inconclusive.

$n-1 = 2046$

$2046 = 2 \times 1023$

$k=1 \quad q=1023$

if $a=2$

$2^{1023} \bmod 2047 = 1 \Rightarrow$ says it may be prime

But 2047 is a Composite number.

30/8

## Residue classes mod n (set of residues)

$[0] \; [1] \; \ldots \; [n-1]$ where

$[r] = \{a : a \text{ is an integer}; a \equiv r \bmod n\}$

The residue classes mod 4 are

$[0] = \{\ldots\ldots -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\ldots\}$

$[1] = \{\ldots\ldots -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\ldots\}$

$[2] = \{\ldots\ldots -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\ldots\}$

$[3] = \{\ldots\ldots -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\ldots\}$

## Chinese Remainder Theorem (CRT)

Any integer can be constructed from a pair of integer mod residue class, the pair is relatively prime and the residue class are relatively prime

$x \equiv \underset{a_1}{5} \bmod \underset{\text{mod1(m1)}}{8}$

$x \equiv \underset{a_2}{3} \bmod 5 \text{ mod}_2$

x can be reconstructed from 5, 3 and residue classes

$a_1 = 5,\ a_2 = 3,\ m_1 = 8,\ m_2 = 5$

$M = m_1 \times m_2$

$= 8 \times 5$

$M = 40$

$M_1 = \frac{M}{m_1} = \frac{40}{8} = 5$

$M_2 = \frac{M}{m_2} = \frac{40}{5} = 8$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 \ (\text{Mod } M)$

~~$x = 5 * 5 *$~~

$M_1 y_1 \equiv 1 \bmod m_1$ $\qquad$ $M_2 y_2 \equiv 1 \bmod M_2$

$5 y_1 \equiv 1 \bmod 8$ $\qquad$ $8 y_2 \equiv 1 \bmod 5$

$y_1 \equiv 5 \bmod 8$ $\qquad$ $y_2 \equiv 2 \bmod 5$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod M$

$= (5 \times 5 \times 5 + 3 \times 8 \times 2) \bmod 40$

$x = (125 + 48) \bmod 40$

$x = 173 \bmod 40$

$x = 13 \bmod 40$

$13 \bmod 40$ → $5 \bmod 8$, $3 \bmod 5$

Ex: $973 \bmod 1813$

find the pair $973 = (-,-)$ where $m_1 = 37$ and $m_2 = 49$

$973$ → $a_1 \bmod 37$, $a_2 \bmod 49$

$M_1 = \frac{M}{m_1} = \frac{37 \times 49}{37} = 49$

$M_2 = \frac{M}{m_2} = \frac{37 \times 49}{49} = 37$

$M_1^{-1} \equiv \_\_ \bmod m_1$

$M_1^{-1} \equiv \frac{34}{99 \times 34} \bmod 37$

$M_2^{-1} = \frac{\_\_}{37 \times 4} \bmod m_2$

$M_2^{-1} \equiv 4 \bmod 49$

$973 \begin{cases} \equiv 54 \bmod 37 \\ \equiv 4 \bmod 49 \end{cases}$

$\Rightarrow 973 \equiv 11 \bmod 37$
$973 \equiv 42 \bmod 49$ $\Big\rangle$ $973 \equiv (11, 42)$

Let $M = \prod_{i=1}^{k} m_i$

where $m_i$ are relatively prime

i.e, $\gcd(m_i, m_j) = 1 \quad i \neq j$

any integer in $Z_k$ can be represented by k-tuple.

$A \leftrightarrow (a_1, a_2, \ldots a_k)$

where $A \in Z_M$ and $a_i = A \bmod m_i$ for $1 \le i \le k$

Ex: use CRT to find x,

$x \equiv 3 \bmod 7$

$x \equiv 3 \bmod 13$

$a_1 = 3, \; a_2 = 3, \; m_1 = 7, \; m_2 = 13$

$M = m_1 \times m_2$

$= 7 \times 13$

$M = 91$

$M_1 = \frac{M}{m_1} = 13$

$M_2 = \frac{M}{m_2} = 7$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod M$

$M_1 y_1 \equiv 1 \bmod m_1$ $\quad$ $M_2 y_2 \equiv 1 \bmod m_2$

$13 y_1 \equiv 1 \bmod 7$ $\quad$ $7 y_2 \equiv 1 \bmod 13$

$y_1 \equiv 6 \bmod 7$ $\quad$ $y_2 \equiv 2 \bmod 13$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod M$

$\equiv (3 \times 13 \times 6 + 3 \times 7 \times 2) \pmod{91}$

$\equiv (234 + 42) \pmod{91}$

$\equiv 276 \bmod 91$

$x \equiv 3 \bmod 91$

$3 \bmod 91$ → $3 \bmod 7$, $3 \bmod 13$

## Discrete logarithms

$Z_n = \{$ the collection of numbers that are Relatively Prime to $n \}$

$Z_{14} = \{1, 3, 5, 9, 11, 13\}$

Given

1) $n = 2, 4, p^k, 2 \cdot p^k$ for $k \in N$ and $p$ is odd prime

2) Given $\alpha \in Z_n^*$ is a generator (primitive root)

3) $B \in Z_n^*$ (not necessarily a generator)

Compute $\log_{\alpha} \beta$.

i.e., find $a$ such that $\alpha^a = \beta$

Ex: Given $n = 9$

$Z_n = \{1, 2, 4, 5, 7, 8\}$

$\phi(n) = 6$

$\alpha = 2$

$2^0 \bmod 9 \equiv 1$ $\quad 0 \Rightarrow \log_2 1$

$2^1 \bmod 9 \equiv 2$ $\quad 1 \Rightarrow \log_2 2$

$2^2 \bmod 9 \equiv 4$ $\quad 2 \Rightarrow \log_2 4$

$2^3 \bmod 9 \equiv 8$ $\quad 3 \Rightarrow \log_2 8$

$2^4 \bmod 9 \equiv 7$ $\quad 4 \Rightarrow \log_2 7$ ✗

$2^5 \bmod 9 \equiv 5$ $\quad 5 \Rightarrow \log_2 5$

from $2^0$ to $2^{\phi(n)-1}$ we are able to generate all numbers in $\phi(n)$, $\therefore \alpha$ is a generator

| logarithm | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| number | 1 | 2 | 4 | 8 | 7 | 5 |

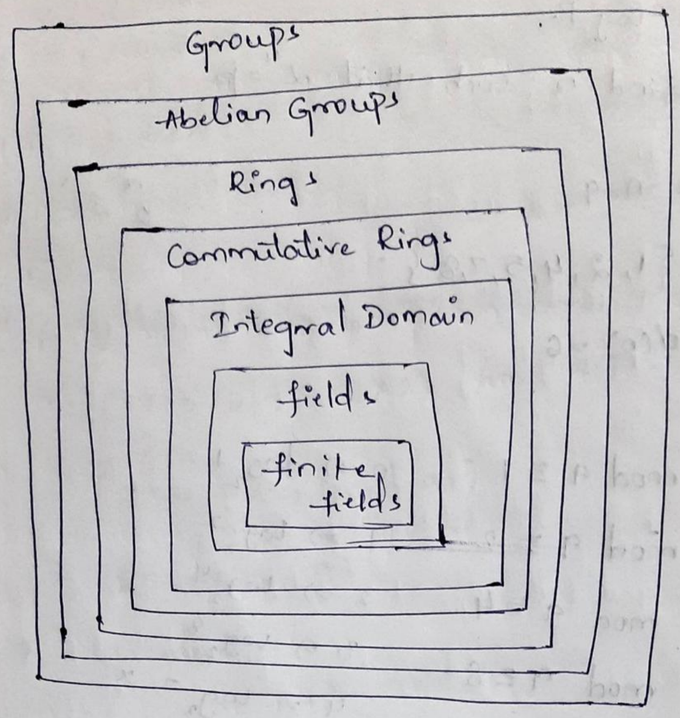
1) multiplicative

2) exponentiation

3) generating 1024 prime number using rabin miller.

4) chinese remainder theorem

5/9/22




## Groups

denoted by $\{G, \cdot\}$ is a set of elements with binary operation $\cdot$, binary operation limits to addition, permutation

Axioms that groups hold:

$(a,b)$ ordered pair, $a.b$

$A_1$: If $a$ and $b \in G$ then $a.b$ belongs to $G$

$A_2$: $a.(b.c) = (a.b).c$ $\forall$ $a,b,c$ in $G$

$A_3$: Identity element: there is an element $e$ in $G$ such that $a.e = e.a = a$ $\forall$ $a$ in $G$

$A_4$: Inverse element: for each $a$ in $G$ there is an inverse $a'$ such that

$$a.a' = a'.a = e$$

## Abelian Groups:

It satisfies the axioms of groups

$A_5$: commutative : $a.b = b.a \quad \forall \; a,b \in G$

$A_1$: $\{3,2,1\} . \{1,3,2\} = \{2,3,1\}$

$A_2$ : $a.(b.c) = (a.b).c$

$\{1,2,3\} . (\underset{2,3,1}{\{3,2,1\}} . \{1,3,2\}) = \{2,3,1\}$

$(\underset{3,2,1}{\{1,2,3\}} . \{3,2,1\}) . \{1,3,2\} = \{2,3,1\}$

$A_3$ : $\{1,2,3,\ldots n\}$

$A_5$ : $a.b \neq b.a$

$\{3,2,1\} . \{1,3,2\} = \{2,3,1\}$

$\{1,3,2\} . \{3,2,1\} = \{3,1,2\}$

∴ The permutation is a group but not abelian group

## Cyclic Groups:

A group is called cyclic if every element in $G_1$ is a power of $a^k$, k is an integer and a is a fixed element $\in G_1$

Ex: $n=5 \quad Z_p = \{1,2,3,4\}$

Consider $a=2$

$2^0, 2^1, 2^2, 2^3$ should produce all elements in group

$2^0 \bmod 5 = 1$

$2^1 \bmod 5 = 2$

$2^2 \bmod 5 = 4$

$2^3 \bmod 5 = 3$

∴ It is a cyclic Group.

## Rings:

- It is an abelian group with some additional conditions

Represented by $\{R, +, \times\}$

$A_1$ to $A_5$ should be satisfied

$A_1 - A_5$ : R is an abelian group w.r.t addition i.e., R satisfies axioms $A_1$ to $A_5$ for the additive group

$M_1$: If a and $b \in R$, then $a.b \in R$

$M_2$: Associativity of multiplication

$$a(bc) = (ab)c$$

$M_3$: Distributive class

$$a(b+c) = ab + ac \quad \forall\ a,b,c$$

$$(a+b)c = ac + bc \quad \forall\ a,b,c$$

+ - talking about distributive

x - talking about closure and Associativity

### Commutative Ring:

$M_4$: commutativity of multiplication

$$ab = ba \quad \forall\ a,b \in R$$

ex: Let s be the set of even integers. s is a commutative ring.

07/09/22

### Standard Notations

→ N: set of positive integers $\{1, 2, 3, \ldots\}$

→ $\mathbb{Z}$: set of all integers $\{\ldots -2, -1, 0, 1, 2, \ldots\}$

→ $\mathbb{Q}$: set of all Rational number

→ $\mathbb{R}$: set of Real numbers

→ $\mathbb{C}$: set of complex numbers

## Integral domain

An integral domain, which is a commutative ring that obeys following axioms

$M_5$ : Multiplicative Identity

↳ There is an element 1 in R such that

$a1 = 1a = a, \forall a \in R$

$M_6$ : No Zero divisors: If $a, b \in R$ & $ab = 0$, then either $a = 0$ or $b = 0$

Ex: Z is a integral domain

Fields:

- Type 1
- Type 2 - Galois field, GF(2), Binary field
- Type 3 - GF(p), p prime, $GF(p^n)$

A field F, denoted by $\{F, +, \times\}$, is a set of elements with two binary operations, called addition and multiplication, such that $\forall a, b, c \in F$ the following axioms are obeyed

(A1 - M6) i.e, F is a integral domain

$M_7$: Multiplicative inverse: $\forall a \in F$ (except 0), $\exists a^{-1} \in F$ such that $aa^{-1} = (a^{-1})a = 1$

Ex:- Q, R, C are fields

Z is not a field because every integer does not have a multiplicative inverse.

→ In cryptographic algorithms, we use fields.

Arithemetic on polynomials

Let R be an arbitary ring. A polynomial over R is a expression of the form.

$$f = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n$$

where n is a non-negative integers. the coefficients $a_i$ $(0 \le i \le n)$ are elements of R and x is symbol not belonging to R, called an indeterminate over R.

→ Type 1 - coefficient can be any number

→ Type 2 - coefficients are 0 or 1, coefficient mod 2.

Ex: Let $f(x) = x^3 + x^2 + 2$, $g(x) = x^2 - x + 1$

S is set of integers

Type 1

$f(x) + g(x) = x^3 + 2x^2 - x + 3$

$f(x) - g(x) = x^3 + x + 1$

$f(x) * g(x) = x^5 + 3x^2 - 2x + 2$

$f(x) / g(x) \Rightarrow Q = x + 2$

$R = x$

Definition $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{n} b_i x^i$

$$f + g = \sum_{i=0}^{n} (a_i + b_i) x^i$$

Type 2 - GF(2) or GF(p) where p is only 2

$f(x) = x^3 + 2x + 1$

$g(x) = x^2 - x + 2$

---

$f(x) + g(x) = \square x^3 + x^2 + x + 3$ mod 2

$= x^3 + x^2 + x + 1$

→ polynomial arithmetic in which the arithmetic on the coefficient is performed modulo P, that is the coefficients are in GF(P) - Type 2

→ polynomial arithmetic in which the coefficients are in GF(P) & the polynomial are defined modulo a polynomial m(x) whose highest power.

Ex: over GF(2)

$f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

$g(x) = x^3 + x + 1$

$f(x) + g(x) = x^7 + x^5 + x^4$

$f(x) - g(x) = x^7 + x^5 + x^4$

$f(x) * g(x) = x^{10} + x^4 + x^2 + 1$

$f(x) / g(x) = x^4 + 1$

GCD and inverse on Type 2 polynomials

Divisibility

Let F denote a field from now on, we consider polynomials over fields. we say that the polynomial $g \in F(x)$ divides $f \in F[x]$ if:

Let $g \neq 0$ be polynomial in $F[x]$. Then for any $f \in F(x)$ there exist polynomial $q, r \in F[x]$ such that $f = qg + r$, where $\deg(r) < \deg(g)$

using the division algorithm, we can show that every ideal of $F[x]$ is principal.

09/09/22

GF(2) Addition (XOR) mod 2

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

multiplication (AND)

| x | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

GF(2) - mod 2

GF($2^n$) - mod m(x) - represents irreducable polynomial
↳ we cannot factor that polynomial into 2 to 3 factor which has degree less than highest degree.

GF($2^3$) : n=3 $m(x) = x^3+x+1$

$f(x) = x^2+x+1$ 111 = 7

$g(x) = x^2+1$ 101 = 5

$f(x)+g(x) = x^2+x+1+x^2+1$

$= 2x^2+x+2$

$= x$

$= 2$

In GF($2^3$) addition of 7 and 5 is 2

$f(x).g(x) = (x^2+x+1).(x^2+1)$

$= x^4+x^3+x^2+x^2+x+1$

$= x^4+x^3+2x^2+x+1$

$= x^4+x^3+x+1 \mod x^3+x+1$

$= -x^2-x$

$= x^2+x$

$= 6$

| | | | |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | x |
| 0 | 1 | 1 | x+1 |
| 1 | 0 | 0 | $x^2$ |
| 1 | 0 | 1 | $x^2+1$ |
| 1 | 1 | 0 | $x^2+x$ |
| 1 | 1 | 1 | $x^2+x+1$ |

$$
\begin{array}{r}
x+1 \\
x^3+x+1 \overline{)\, x^4+x^3+x+1} \\
\underline{-x^4+x^2+x} \\
x^3-x^2+1 \\
\underline{-x^3+x+1} \\
-x^2-x
\end{array}
$$

mod 8 ($Z_8$)

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | (1) | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 0 |
| 3 | 0 | 3 | 6 | (1) | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | (1) | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 0 | 5 | 4 | 3 | 2 | (1) |

$GF(2^3)$

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | (1) | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 3 | (1) | 7 | 5 |
| 3 | 0 | 3 | 6 | 5 | 7 | 4 | (1) | 2 |
| 4 | 0 | 4 | 3 | 7 | 6 | 2 | 5 | (1) |
| 5 | 0 | 5 | (1) | 4 | 2 | 7 | 3 | 6 |
| 6 | 0 | 6 | 7 | (1) | 5 | 3 | 2 | 4 |
| 7 | 0 | 7 | 5 | 2 | (1) | 6 | 4 | 3 |

when we move to gallorian fields we can find multiplicative inverse of all elements.

→ In mod($Z_8$) frequency of elements is not uniformly distributed. (there is a chance of guessing)

| integer | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| freq in $Z_8$ | 22 | 4 | 8 | 4 | 12 | 4 | 8 | 4 |
| freq in $GF(2^3)$ | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |

→ $GF(2^3)$ makes cryptograph more powerful so that there will be a less chance of guessing the message.

Ex: $x \equiv 1 \bmod 5$, $x \equiv 1 \bmod 7$, $x \equiv 3 \bmod 11$

$a_1 = 1, a_2 = 1, a_3 = 3$

$m_1 = 5, m_2 = 7, m_3 = 11$

$M = m_1 \times m_2 \times m_3 = 5 \times 7 \times 11 = 385$

$M_1 = \frac{M}{m_1} = \frac{5\times7\times11}{5} = 77$

$M_2 = \frac{M}{m_2} = \frac{5\times7\times11}{7} = 55$

$M_3 = \frac{M}{m_3} = \frac{5\times7\times11}{11} = 35$

$M_1y_1 \equiv 1 \bmod 5$ $\quad M_2y_2 \equiv 1 \bmod 7$ $\quad M_3y_3 \equiv 1 \bmod 11$

$77\,y_1 \equiv 1 \bmod 5$ $\quad 55\,y_2 \equiv 1 \bmod 7$ $\quad 35\,y_3 \equiv 1 \bmod 11$

$y_1 \equiv 3 \bmod 5$ $\quad 6\,y_2 \equiv 1 \bmod 7$ $\quad 2\,y_3 \equiv 1 \bmod 11$

$y_2 \equiv 6 \bmod 7$ $\quad y_3 \equiv 6 \bmod 11$

$X = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

$= 1\times77\times3 + 1\times55\times6 + 3\times35\times6$

$= 1191 \bmod 385$

$= 36 \bmod 385$

$36 \bmod 385 \equiv 1 \bmod 5,\ 1 \bmod 7,\ 3 \bmod 11$

Ex: $x \equiv 3 \bmod 7,\ x \equiv 3 \bmod 13,\ x \equiv 0 \bmod 12$

$a_1 = 3,\ a_2 = 3,\ a_3 = 0$

$m_1 = 7,\ m_2 = 13,\ m_3 = 12$

$M = 7\times13\times12 = 1092$

$M_1 = 13\times12 = 156$

$M_2 = 7\times12 = 84$

$M_3 = 7\times13 = 91$

$M_1y_1 \equiv 1 \mod 7$ $\frac{144}{6}$ $\frac{}{24}$ $M_2y_2 \equiv 1 \mod 13$ $M_3y_3 \equiv 1 \mod 12$

$156\ y_1 \equiv 1 \mod 7$ $84\ y_2 \equiv 1 \mod 13$

$2\ y_1 \equiv 1 \mod 7$ $6\ y_2 \equiv 1 \mod 13$

$y_1 \equiv 4 \mod 7$ $y_2 \equiv 11 \mod 13$

$X = a_1M_1y_1 + a_2M_2y_3 + a_3M_3y_3$

$X = 3 \times 156 \times 4 + 3 \times 84 \times 11 + 0$

$X = 4644 \mod 1092$

$X = 276 \mod 1092$

12/9/22

## Symmetric Encryption

→ or conventional / private-key / single-key

→ sender and recipient share a common key

→ all classical encryption algorithms are private-key

→ was only type used prior to 70's

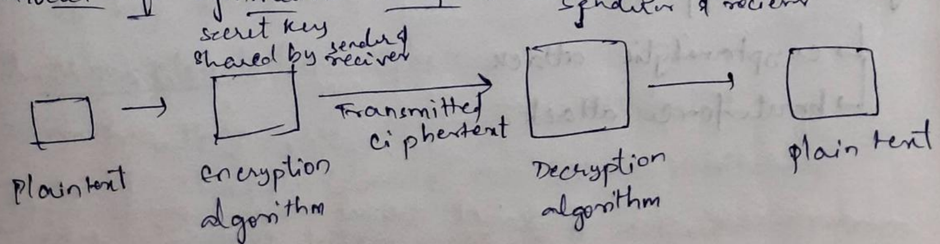
key - info used in cipher known only to sender/receiver

Cryptanalography - study of encryption and decryption

Cryptoanalysis (code breaking) - study of methods of deciphering ciphertext without knowing key

Cryptology - field of both cryptography and cryptanalysis

Model of symmetric Encryption



→ Two requirement for secure use of symmetric encryption
  ↳ a strong encryption algorithm
  ↳ a secret key known only to sender/receiver.

Encryption algo's operations
→ substitution - each letter is replaced with other letter in message
→ Transposition - Re-arranging letters in original message

Mathematically we write

$Y = E_k(X)$ X - original msg Y - ciphertext msg

$X = D_k(Y)$ k - same key.

→ characterize cryptographic system by
  ↳ type of encryption operations used
    ↳ substitution/transposition/product
  ↳ number of keys used
    ↳ single-key or private / two-key or public
  ↳ way in which plaintext is processed
    ↳ block/stream.

Cryptanalysis
→ objective to recover key not just messages
→ general approaches
  ↳ cryptanalytic attack
  ↳ brute-force attack.

## classical substitution ciphers

↳ where letters of plaintext are replaced by other letter or numbers

### 1. Ceaser cipher

→ earliest known substition cipher
→ by Julius Ceaser
→ replaces each letter by 3rd letter
Ex: meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB

$C = (p+k) \bmod 26$

$p = (C-k) \bmod 26$

→ can define transformation as
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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
→ than have Caeser cipher as
$C = E(p) = (p+k) \bmod 26$
$p = D(c) = (C-k) \bmod 26$
→ only 26 possible ciphers
→ couch simply try each in turn
→ a bruth force search
→ given ciphertext, we can check the messages with 26 key and hacker can decrypt the message.

### 2. Monoalphabetic cipher

→ rather than just shifting the alphabet
→ could shuffle (jumble) the letters arbitarily.
→ each plaintext letter maps to a different random cipher text letter

→ hence key is 24 letters long

Plain abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJW

→ because of characteristics of english language, we can still break the code.

→ in English e is by far the most common letter
followed by T, R,

## playfair key Matrix

→ a 5x5 matrix of letters based on a keyword

→ fill in letters of keyword

→ fill rest of matrix with other letters

Eg:- using the keywork MONARCHY

| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

→ plaintext is encrypted two letters at a time

- if a pair is a repeated letter, insert filler like 'x'
- if both letters fall in same row, replace each letter with letter right to it.
- if both letters are in same column then replace each letter with letter below it
- if both are different letters rows and columns replace with a element in same row but colu is of other element.

Ex: NIT WARANGAL X

AGQ ZRMRAINSU

Ex:
Play-fair matrix:

| | | | | |
|---|---|---|---|---|
| J/k | C | D | E | F |
| U | N | P | Q | S |
| Z | V | W | X | Y |
| R | A | L | G | O |
| B | I | T | H | M |

plain text: I only regret that I have but one life to give for my country.

ciphertext: M APAZ OQHGJH WIGH T IGXC JZM LQC ATJF ML AHXC SMO BV FRSPIOZ

16/9/22

## polyalphabetic ciphers

→ polyalphabetic substitution ciphers
→ improve security using multiple cipher alphabets
→ make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
→ use a key to select which alphabet is used for each letter of the message
→ use each alphabet in turn

## Vigenere cipher

→ simplest polyalphabetic substitution cipher

→ effectively

Encryption

key is given → sample

key: Sample samples

Plain: Iam in warangal

Cipher: (S+I) mod 26 (plain + key(letter) mod 26

Decryption

plain: (cipher - key(letter) mod 26

frequency cannot be found easily.

## Autokey cipher

→ plain text characters is used as key for rest of the message after the key is completed.

→ keyword is prefixed to msg as a key.

## One-Time Pad

→ some key is arbitarily selected and for one message one key is selected.

→ It makes frequency analysis very tough for the cryptanalysis.

→ sharing the key everytime is a problem here, It depends on TTP, every time a message has to TTP has to

generate a key and share between Sender & Receiver.

## Hill Cipher

→ key is taken as a matrix based on the block size of message.

→ encryption algorithm takes m successive plain text and substitute for them m cipher text letters.

→ each character is assigned a numeric value

(a=0, ..... z=25)

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26$$

$C = kP \bmod 26$

$P = k^{-1}C \bmod 26 \quad = k\,k^{-1}P = P$

key k

$$k^{-1} = (\det k)^{-1} (-1)^{i+j} (D_{ji})$$

where $D_{ji}$ is sub determinant - ~~forward~~ formed by deleting $i^{th}$ row & $j^{th}$ column of k.

$\det(k^{-1})$ → multiplicative inverse of $(\det k) \bmod 26$

for decrypting:

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} * \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

Example:

$P = EG \qquad k = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \qquad k^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$

$C = k \times P \bmod 26$

$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 4 \\ 6 \end{pmatrix} \bmod 26 = \begin{pmatrix} 24 \\ 16 \end{pmatrix}$

$\det(k) = 15 - 6 = 9$

$(\det k)^{-1} = 9x \_ \bmod 26$

$= 3$

$k^{-1} = 3 \times \begin{bmatrix} 5 & -2 \\ -3 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -6 \\ -9 & 9 \end{bmatrix} = \begin{bmatrix} 15 & 20 \\ 17 & 9 \end{bmatrix}$

$P = k^{-1} C \bmod 26$

$= \begin{bmatrix} 15 & 20 \\ 17 & 9 \end{bmatrix} \begin{pmatrix} 24 \\ 16 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 4 \\ 6 \end{pmatrix}$

$P = EG$

## Transposition Ciphers

→ The original plain text characters are just rearranged
→ also called as transposition ciphers.
→ They are easy to break as frequency of letters in plain text and cipher text are same.

## Rail Fence Cipher

→ write message letters out diagonally over a number of rows

→ then read off cipher row by row

→ m a m
e t e f t e t h e o g a a r t
c a r t p y

Cipher: mmthgretefeteoaateartpy

## Row Transposition Ciphers

→ a more complex transposition

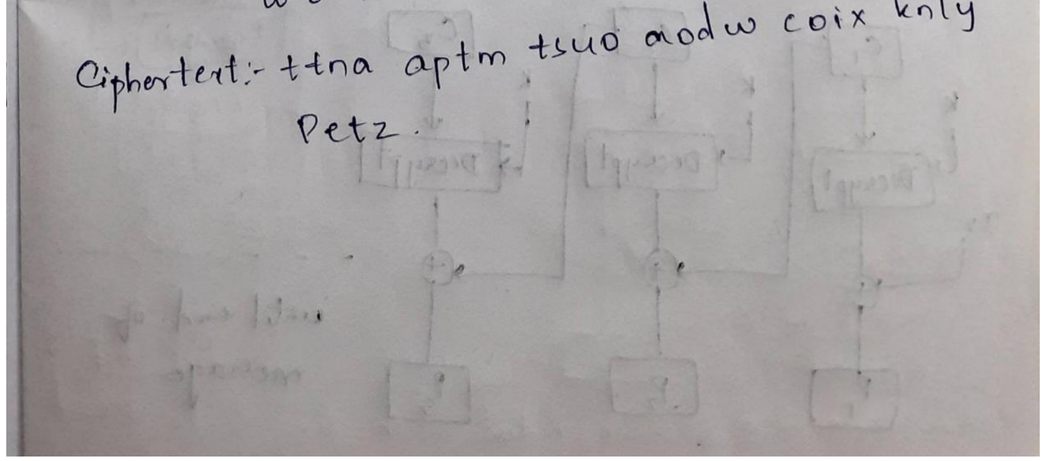
→ write letters of message out in rows over a specified number of columns

→ then reorder the columns according to some key before reading off the rows

key: 3 4 2 1 5 6 7

Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

Ciphertext:- ttna aptm tsuo aodw coix knly
Petz.



20/9/22

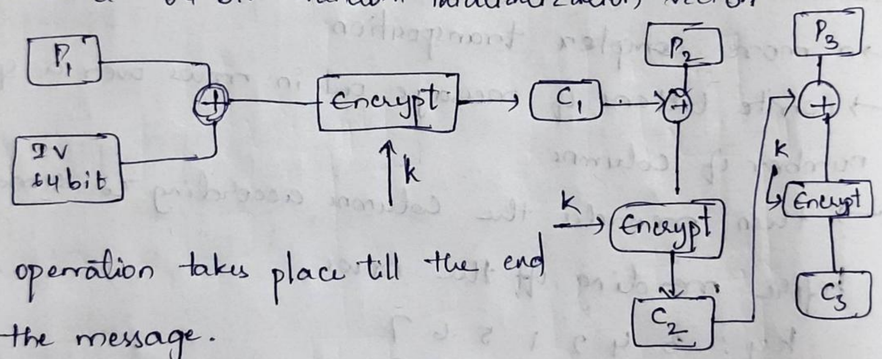
## Block cipher Modes of Operation:

1. ECB mode:
→ when you have less amount of data
msg is divided into blocks of bits, same key is used for all blocks and the plain text is encrypted.

2. Cipher block chaining mode: (CBC mode):

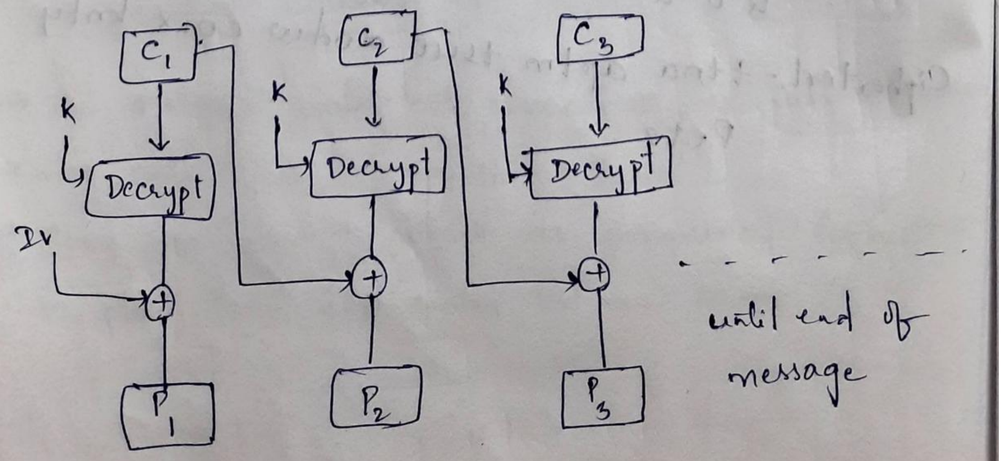
$P_1$ - 64 bit

generate a 64 bit random initialization vector



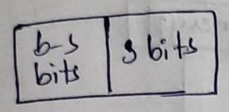

this operation takes place till the end of the message.

key and IV has to be shared by trusted third party among two parties

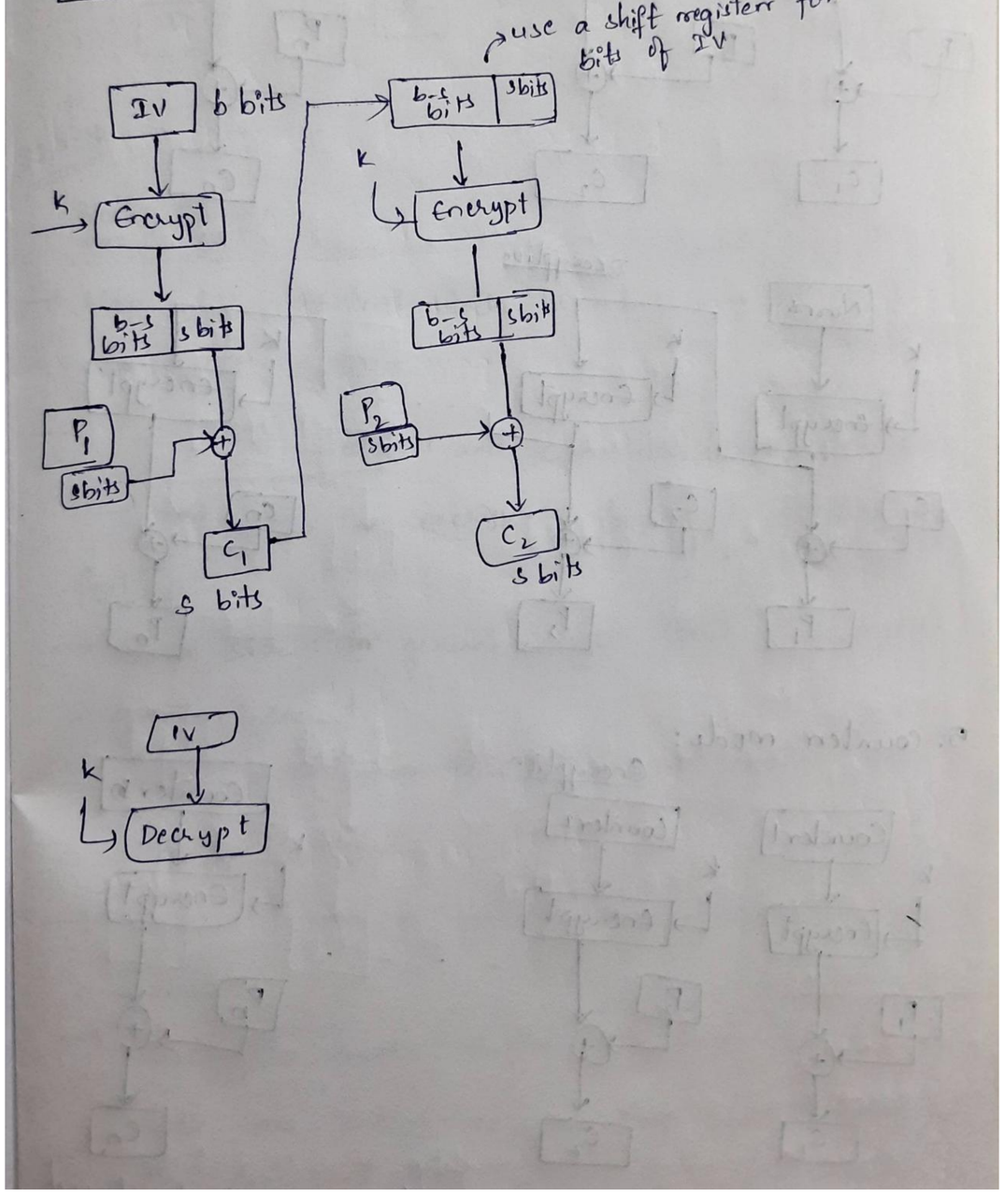


## 3. Cipher Feedback mode (CFB mode):

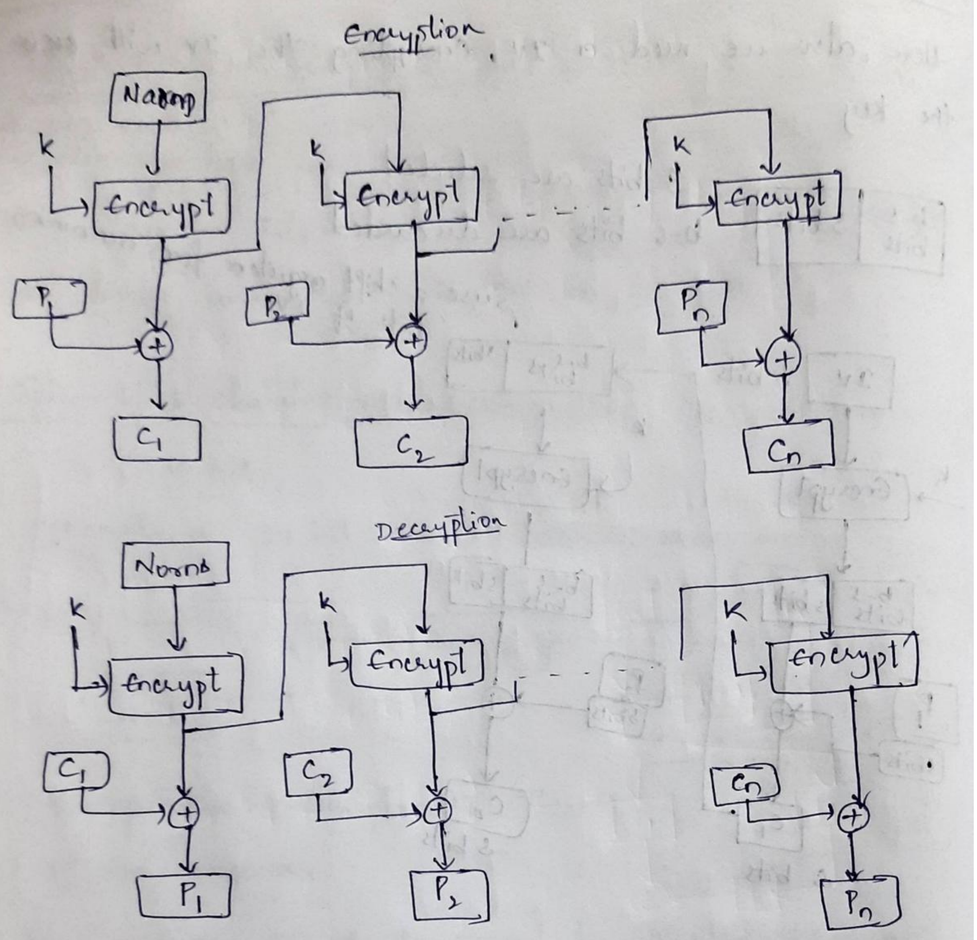
Here, also we need a IV. Encrypting the IV with the key



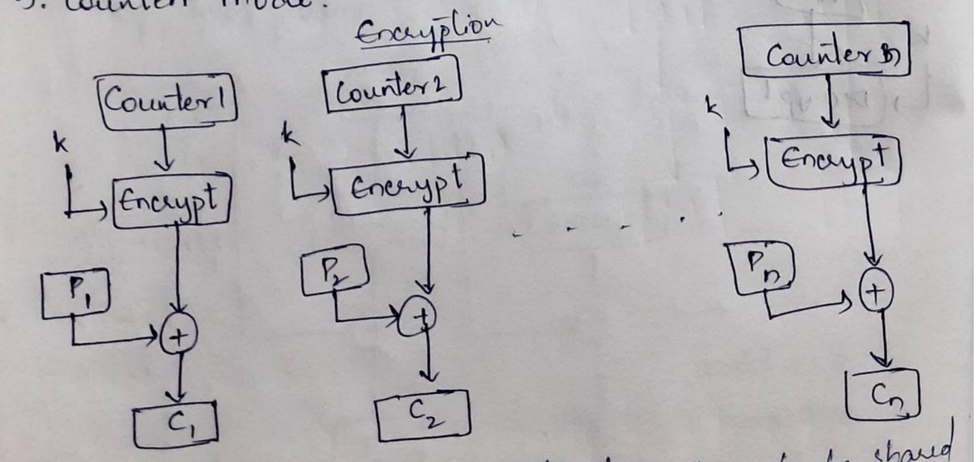

s bits are selected
b-s bits are discarded



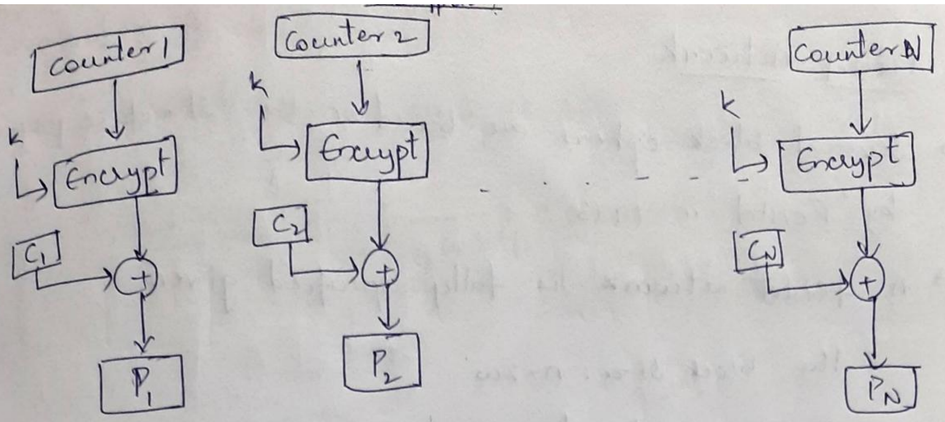
4. Output Feedback mode (OFB mode):




5. Counter mode:




Apart from key, counter initialization has to be shared between two parties.




22/9/22

## Block ciphers

→ Map n-bit plain text blocks to n-bit ciphertext blocks (n - block length)

→ For n-bit plaintext and ciphertext block and a fixed key, the encryption function is bijection.

features:-

→ Block size : In general longer block sizes mean greater security

→ key size : Larger key size means greater security (larger key space)

→ Number of rounds : multiple rounds after increasing security

→ Encryption modes : define how msg's larger than block are encrypted, very imp for security of the encrypted msg.

## Feistel Network

→ several block ciphers are based on the structure proposed by Feistel in 1973

→ A feistel network is fully specified given

- the block size: $n = 2w$
- no. of rounds = $d$
- $d$ round function, $t_1, \ldots t_d : (0,1)^w \rightarrow (0,1)^w$

used in DES, IDEA, RC5 not used in ~~AES~~.

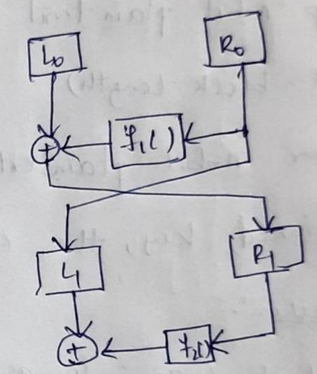
• encryption

- $L_1 = R_0 \quad R_1 = L_0 \oplus f_1(R_0)$

$L_2 = R_1 \quad R_2 = L_1 \oplus f_2(R_1)$

⋮

$L_d = R_{d-1} \quad R_d = L_{d-1} \oplus f_d(R_{d-1})$

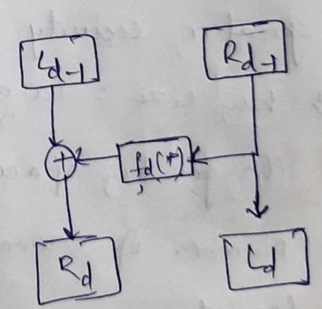



• Decryption

- $R_{d-1} = L_d \quad L_{d-1} = R_d \oplus f_d(L_d)$

⋮

- $R_0 = L_1 ; \quad L_0 = R_1 \oplus f_1(L_1)$



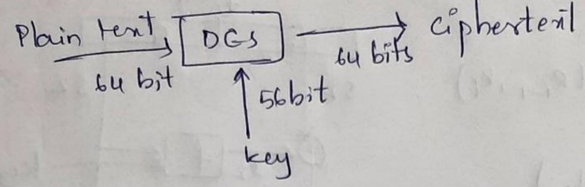

## DES Features:

• Features

- Block size = 64 bits
- key size = 56 bits (in reality, 64 bits, but 8 are used as parity-check bits for error control)

- number of rounds = 16

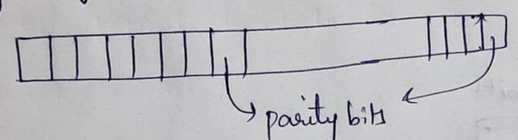
- 16 intermediary keys, each 48 bits



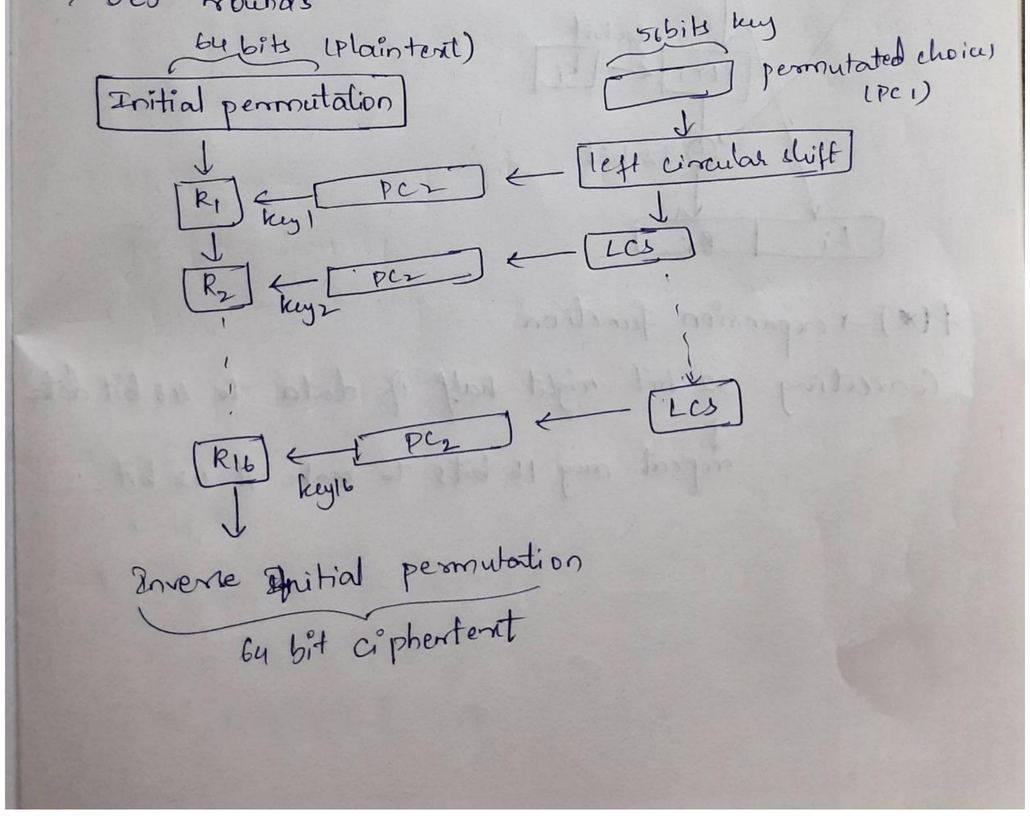

In key, every 8th bit is parity bit of 7 bits

So key size = 64 - 8 = 56 bits

→ each paritycheck bit is XOR of previous 7 bits




→ DES rounds



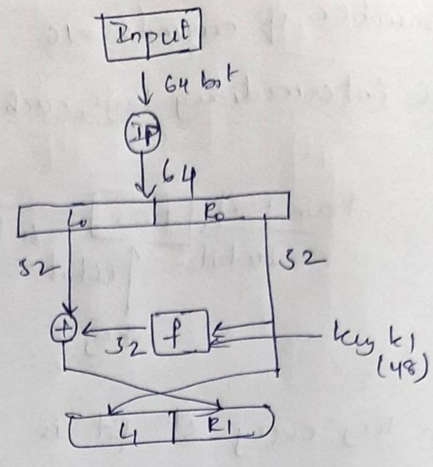
## Details:

$IP(x) = L_0 R_0$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

$Y = IP^{-1}(R_{16} L_{16})$

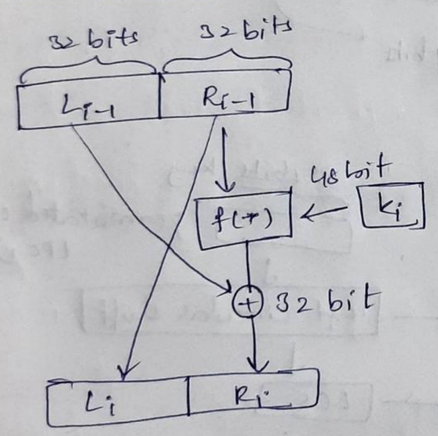



Initial permutation

58 - 1st bit

50 - 2nd bit

## DES Round i

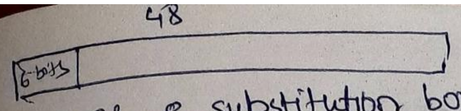



f(*) → expansion function

Converting 32 bit right half of data to 48 bit data

↓

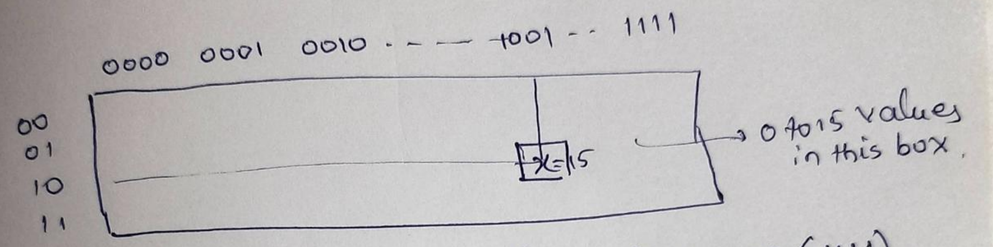
repeat any 16 bits to make it 48 bit




uses 8 substitution boxes = 8×6 = bits

↓ each 6 bits.

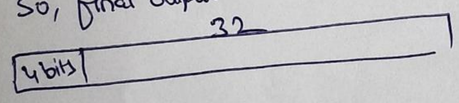
Eg: 110010 → column
row
} for substitution box.

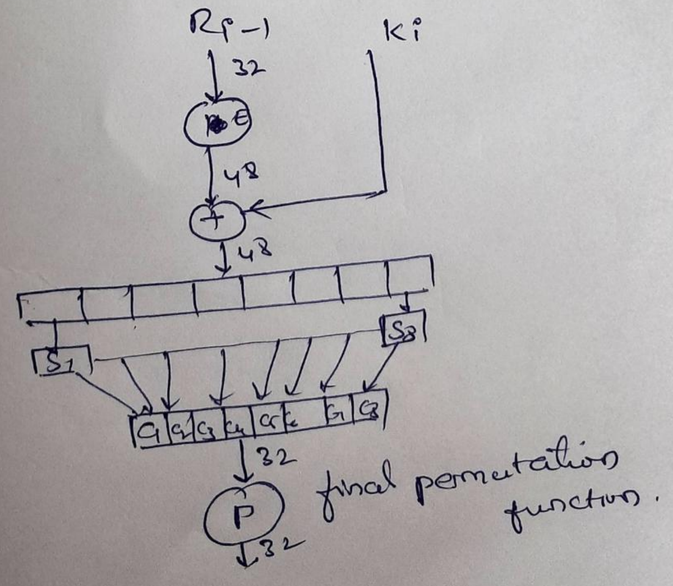



Replace 6 bits (110010) by 15 (1111) [4 bits]

output : Each box = 4

So, final output 8×4 = 32 bits.



DES Weak Keys

0101 0101 0101 0101

FE FE FE FE FE FE FE FE

E0 E0 E0 E0 F1 F1 F1 F1

1F 1F 1F 1F 0E 0E 0E 0E

need to be avoided