Page NO.

1. 1 to 20 – Mid Term
2. 21 to 52- Final Term


MD IFTAKHAR KABIR SAKUR

25th BATCH

COMPUTER AND COMMUNICATION ENGINEERING

International Islamic University Chittagong


# COURSE CODE: CCE-4825

# COURSE TITLE: Cryptography and Network Security

COURSE TEACHER:

Ahmad

Lecturer
ETE

CCE-4825 (Midterm) 21.02.24

[Cryptography & Network Security]

Aut-22 2(b)
Spr-23 2(a)

## Cipher Text:

→ Replace each letter in Alphabet with the letter standing three places [every with question] further down the alphabet.

→ For each plaintext letter 'p' substitute the ciphertext letter 'c':

C = Cipher Text = E(P+K) mod 26 = Encryption

P = Plain Text = (C-K) mod 26 = Decryption

Example:- K=3

Encrypt "Neso Academy" using ceaser cipher

Plain Text:- N E S O A C A D E M Y

Encryption:-

N = (13+3) mod 26 = 16 = Q

E = (4+3) mod 26 = 7 = H

S = (18+3) mod 26 = 21 = V

O = (14+3) mod 26 = 17 = R

A = (0+3) mod 26 = 3 = D

C = (2+3) mod 26 = 5 = F

A = D

D = (3+3) mod 26 = 6 = G

E = (4+3) mod 26

= 7 = H.

M = (12+3) mod 26

= 15 = P

Y = (24+3) mod 26

= 1 = B

∴ Cipher Text :- QHVRDFDGHPB

Decryption process :-

Q H V R D F D G H P B

$Q = (16-3) \bmod 26 = 13 = N$

$H = (7-3) \bmod 26 = 4 = E$

$V = (21-3) \bmod 26 = 18 = S$

$R = (17-3) \bmod 26 = 14 = O$

$D = (3-3) \bmod 26 = 0 = A$

$F = (5-3) \bmod 26 = 2 = C$

$D = A$

$G = (6-3) \bmod 26 = 3 = D$

$H = (7-3) \bmod 26 = 4 = E$

$P = (15-3) \bmod 26 = 12 = M$

$B = (1-3) \bmod 26 = -2 \Rightarrow 24 = Y$

∴ NEXT ACADEMY.

## Brute Force on ceaser cipher:-

Aut-22 3(a)
Spr-23 2(b)

## Playfair:-

→ Diagram
→ Ignore repeating letter in matrix.
→ Same column |↓| wrap around.
→ Same row |→| wrap around.
→ Rectangle |⇄| swap [IF 1,2 condition is not working]

(1) Plain Text:- Attack

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

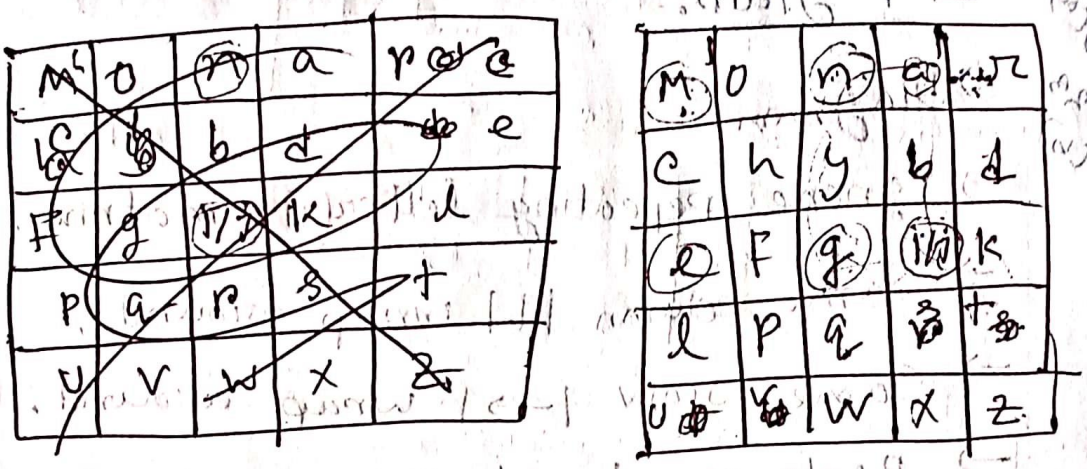
Ans:-
Plain: Balloon
Dia: Ba ll oo n

Diagraph:- At ta CK

Encrypted:- tc

[1] Keyword:- Monarchy

plainText:- Instruments



plain Text:- Instruments

Diagraph:- In st ru me nt sz → Filler letter

Decryption:- gr xa td mz cl mg rq tn

## Hill Cipher:-

Encryption process:- $(P \times K) \bmod 26$ (P → plain Text, K → keyword)

Decryption process:- $P \times K \times K^{-1} \bmod 26$

**Example:-**

Encrypt "pay more money" using Hill cipher

Key $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$

**Solution:-**

**PlainText:-**

| p | a | y | m | o | r | e | m | o | n | e | y |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 15 | 0 | 24 | 12 | 14 | 17 | 4 | 12 | 14 | 13 | 4 | 24 |

Here: matrix 3×3 matrix

Plain Text: pay mor emo ney

[If ends with 2 letters the add 'x' as Filler letter]

Cipher Text:- rpl mwb (Kas) pdh

-[Ans]:

Encryption:- pay

$$(C_1 C_2 C_3) = (P_1 P_2 P_3) \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \bmod 26$$

$$(C_1 C_2 C_3) = (\underset{p}{15} \underset{a}{0} \underset{y}{24}) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26 \rightarrow \text{(key matrix)}$$

$$= (15\times17+0\times21+24\times2 \quad 15\times17+0\times18+24\times2 \quad 15\times5+0\times21+24\times19)$$

$$= (303 \quad 303 \quad 531) \bmod 26$$

$$= (17 \quad 17 \quad 11)$$

$$= (r \; r \; l)$$

$$\text{mor} = (12 \; 14 \; 17) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$$= (12\times17+14\times21+17\times2 \quad 12\times17+14\times18+17\times2 \quad 12\times5+14\times21+17\times19) \bmod 26$$

$$= (532 \quad 490 \quad 677) \bmod 26$$

$$= (12 \; 22 \; 1).$$

$$= (M \; W \; B)$$

(To be continued)

**Decryption:-** $P = C \times K^{-1} \mod 26$

Formula:- $K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$

P. $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

$$\text{Det} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \mod 26$$

$$= \{17(18\times19 - 21\times2) - 17(21\times19 - 2\times21) + 5(21\times2 - 2\times18)\} \mod 26$$

$$= (5100 - 6069 + 30) \mod 26$$

$$= -939 \mod 26$$

$$= -3$$

$$= -3 + 26 = 23$$

$\Rightarrow$ Adj K =

| | | | | |
|---|---|---|---|---|
| 17 | 17 | 5 | 17 | 17 |
| 21 | 18 | 21 | 21 | 18 |
| 2 | 2 | 19 | 2 | 2 |
| 17 | 17 | 5 | 17 | 17 |
| 21 | 18 | 21 | 21 | 18 |

Adj K = $18\times19 - 2\times21$ $\quad 2\times5 - 17\times19$ $\quad 17\times21 - 18\times5$

$21\times2 - 19\times21$ $\quad 19\times17 - 5\times2$ $\quad 5\times21 - 21\times17$ mod 26

$21\times2 - 2\times18$ $\quad 2\times17 - 17\times2$ $\quad 17\times18 - 21\times17$

$$= \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{bmatrix}$$

$$= \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \mod 26$$

So, $K^{-1} = \frac{1}{23} \times \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \mod 26$

$$= 17 \times \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \quad [\because 23^{-1} \bmod 26 = 17]$$

$$= \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix} \mod 26$$

$$\therefore K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

So, the plainText:- pay more money

CipherText:- RRL MWBK ASPDH

Solution:-

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

$$(C_1 C_2 C_3) = (R\ R\ L) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (17\ 17\ 14) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (587\ 442\ 544) \bmod 26$$

$$= (15\ 0\ 24)$$

$$= (P\ A\ Y)$$

(To be continued)

## Rail Fence cipher

→ Depth will be given
→ Based on depth the sequence will have to be written.

Depth :- 3

Plain Text:- I read cryptography

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | | | | d | | | p | | | | r | | | | y |
| | r | | a | | c | | y | | t | | g | | a | | h |
| | | e | | | | r | | | | o | | | | p | |

Cipher Text:- Idpryrdcytgahero

[Row অনুযায়ী]

Decryption:-

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x | | | | x | | | | | | | | | | | |
| | x | | x | | x | | | | | | | | | | |
| | | x | | | | x | | | | | | | | | |

[x দিয়ে Blueprint করে নাও then row অনুযায়ী cross মুছলাতে value বসাতে হবে

| | | | | | |
|---|---|---|---|---|---|
| I | | | | d | |
| | r | | a | | |
| | | e | | | |

## Rail-column Transposition Technique:-

→ Sender & receiver ला Fixed अशा आकार

→ Write:- Row by Row

→ Read:- Column by Column

→ Key:- Order of the Column. [Q]

Example:- Key:- 4 3 1 2 5 6 7

Message:- Kill corona virus at twelve am tomorrow

| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| K | i | l | l | c | o | r |
| o | n | a | v | i | r | u |
| s | a | t | t | w | e | l |
| v | e | a | m | to | o | m |
| o | r | r | o | w | y | z |

↳ [Pragas letter to Fill empty]

∴ Cipher Text:- latorlv tmo lnaer kosvo clwtw

Oreoy r ulmz

Encryption-2

Decryption:-

| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| l | a | t | a | r | l | v |
| t | m | o | i | n | a | e |
| r | k | o | s | v | o | c |
| i | w | t | w | o | r | e |
| o | p | u | i | m | y | z |

## Vernam cipher

$C_i = P_i \oplus K_i$

(*) Key :- Deceptive

PlainText :- we are discovered

Key :-

| D | e | c | e | p | t | i | v | e | d | e | c | e | p | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | 15 | 19 |

Plain Text

| w | e | a | r | e | d | i | s | c | o | v | e | r | e | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 22 | 4 | 0 | 17 | 4 | 3 | 8 | 18 | 2 | 14 | 21 | 4 | 17 | 4 | 3 |

Cipher Text

| 25 | 8 | 2 | 21 | 19 | 22 | 16 | 39 | 6 | 17 | 25 | 6 | 21 | 19 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| z | i | c | v | t | w | q | r | g | r | z | g | v | t | w |

$3+22 = 25 \bmod 26$

$= 25$

$4+4 = 8 \bmod 26$

$= 8$

Decrypting:- ⊕ $P_i = (C_i - K_i) \bmod 26$

তাহলে value গুলোকে ঘুরে বসালে Decrypt value পাওয়া যায়।

## Cryptography

Eg Crypt means → Hidden

graphy means → writing

→ Securing info, datas to communication.

→ Sender will send without any problem. And receiver will receive without any problem.

Spring 23 (1c)

Feature:-

→ Confidentiality

→ Integrity :-> Info can't be modified

→ Non-repudiation :- Can't deny to send Info.

→ Authentication :- The identities of sender & receiver.

## Cyber Security:-

The technique of protecting internet connected systems.

Cyber → Systems, networks, programs. & data

Security → protection of all these.

## Cyber security Goals:-

Aut-22 2(b)

CIA Triad

Apr-23 21(a)

Confidentiality:- equivalent to privacy

Integrity:- Data is authentic, No modification.

Availability:- Available of Information.

### Attacks

Passive:- Unauthorized Access

Active:- Changing the information.

### Apr-23 21(a) Cyber Threats Types

- → Malware
- → phising
- → Man in the middle
- → DDos
- → Brute Force
- → SqL injection
- → DNS attack

## OSI security:-

- Security Attack → Compromises the security
- Security mechanism → protecting a system
- Security service

### (1) Security Attack:-

(a) Passive Attack:-

(i) Eavesdropping (Intercept & listen without concent)

(ii) Traffic Analysis (Analyze network to gather info).

~~(b) Active Analysis.~~

(b) Active Attack:-

(i) Masquerade (Attacker pretends as authentic sender)

(ii) Replay (Intercept a transmitted message & delays or replays it)

(iii) Modification of ~~change~~ message

(iv) Denial OF Service:- Attacker sends large volume of traffic.

AUT-22

## passive vs Active

| Passive | Active |
|---|---|
| (1) Hard to Detect | (1) Hard to prevent |
| (2) Neither sender nor receiver is aware of the attack. | (2) Difficult to prevent, Physical, software & network vulnerabilities. |
| (3) Encryption prevents | (3) Detect & recover |
| (4) More emphasis | (4) Deterrent effect contribute to prevent |

SPR-22 2(b)

(2) Security services:- Different services available to maintain the security. 5 types.

(i) Authentication

(ii) Access control

(iii) Data confidentiality

(iv) " integrity (Data is not changed)

(v) Non-repudiation (verifiable record to make sure authentic sender sent message)

Sept-22 2(b)

## 3] Security Mechanism:-

(i) Encryption

(ii) Digital Signature

(iii) Traffic padding (Add extra data in network traffic stream)

(iv) Routing protocol (Secure routes when a gap in security is suspected)

---

### A Model for Network Security

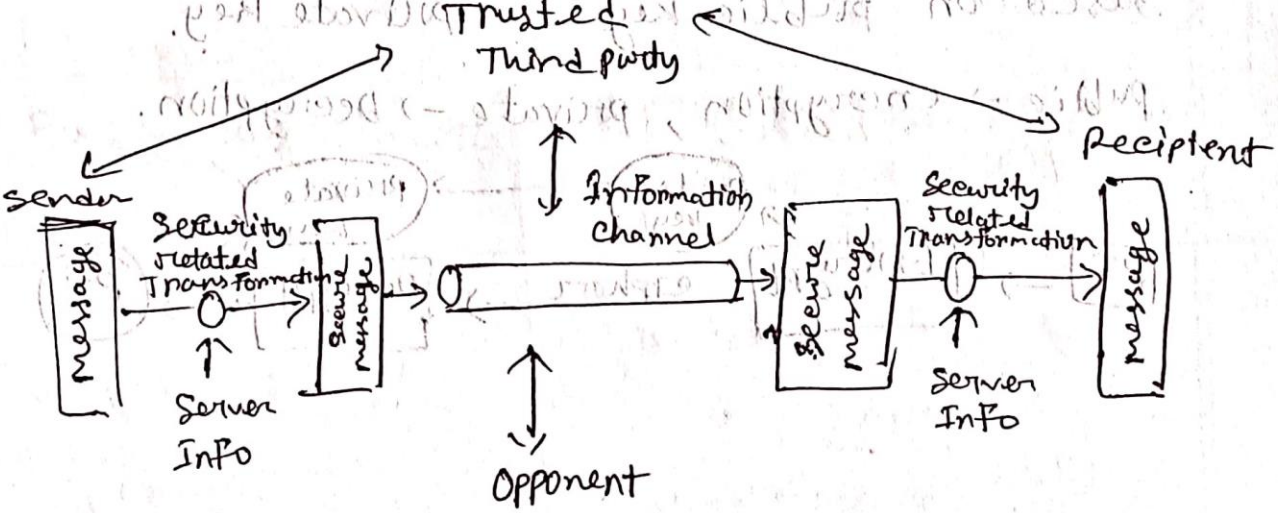
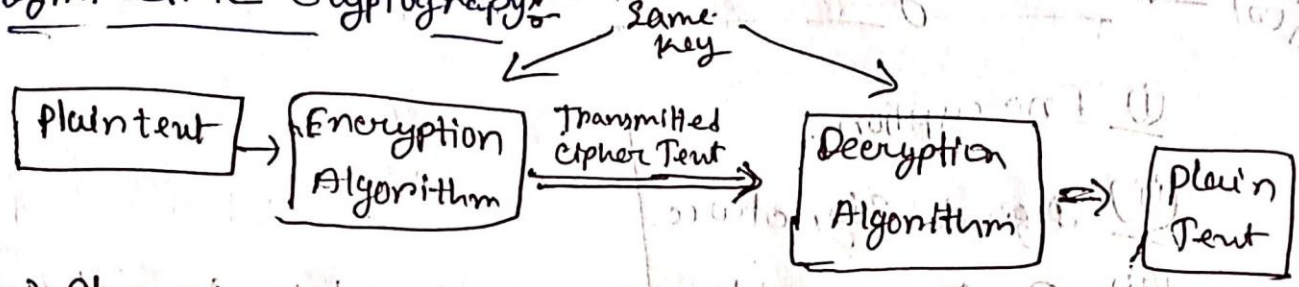



Fig:- Model for Network Security.

Aut-22 2(a) Spring-1(a)

Symmetric cryptography:-

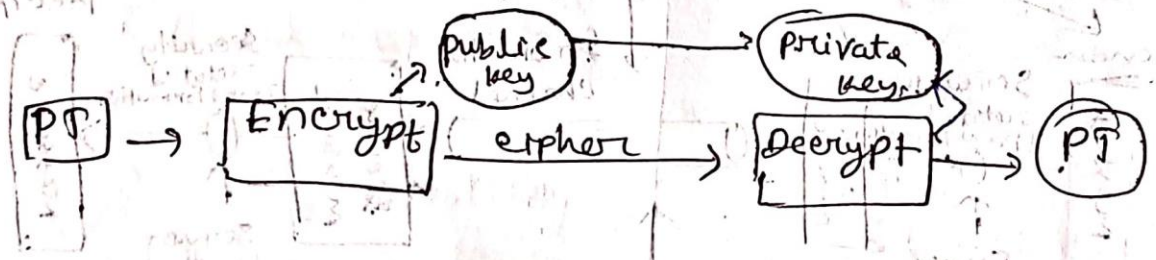



→ Change of any message in order to protect it from reading by anyone. Same key for Encrypt & ~~key~~ decryption.

Assymetric cryptography:-

Based on public key & private key.

Public → encryption, private → Decryption.



Spr-23 3(a)

## Block vs Stream

| Block | Stream |
|---|---|
| ① Converts by taking plain text's block at a time. | ① Converts by taking 1 byte of plain text |
| ② 64 bits or more | ② 8 bits. |
| ③ Complexity → simple | ③ Complexity → more |
| ④ Confusion & defusion | ④ Only confusion |
| ⑤ Reverse encrypted text is hard. | ⑤ Easy. |
| ⑥ Fixed-length blocks | ⑥ bit or byte at a time. |

# Cryptography

## FINAL

### AES [Advanced Encryption Standard]

=> Encryption algorithm worldwide use 2YI

### Symmetric Key block cipher:-

Some keys are used for encryption + decryption.

Fixed - block size = 128 bits [16 bytes = 4 words] 1 word = 32 bits = 4 bytes

| Rounds | no. of bits in key |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

AES-128 version
AES-192 version
AES-256 version

### General Design of AES

128 bit plain Text:-

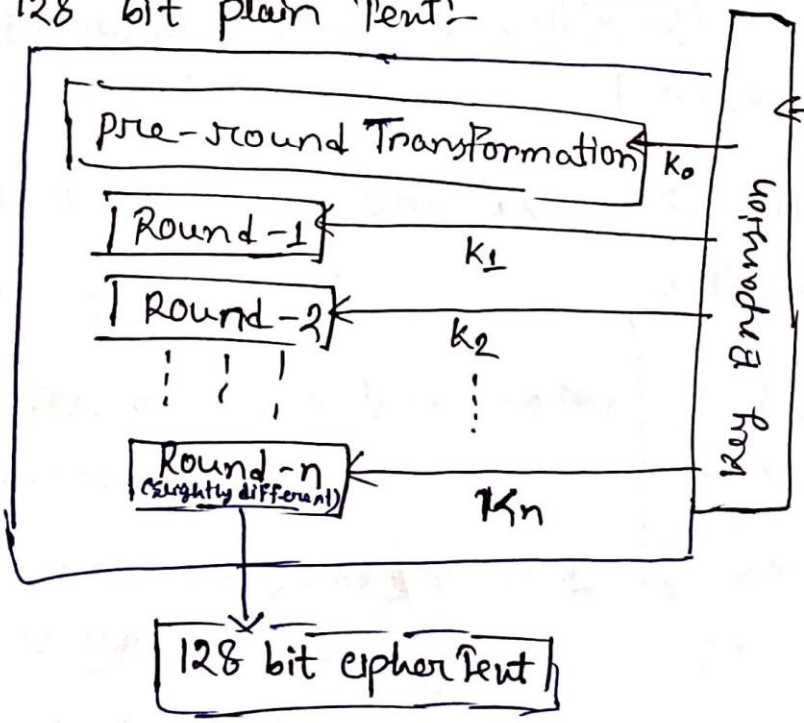



Fig:- General Design of AES Encryption

1 byte = 8 bits

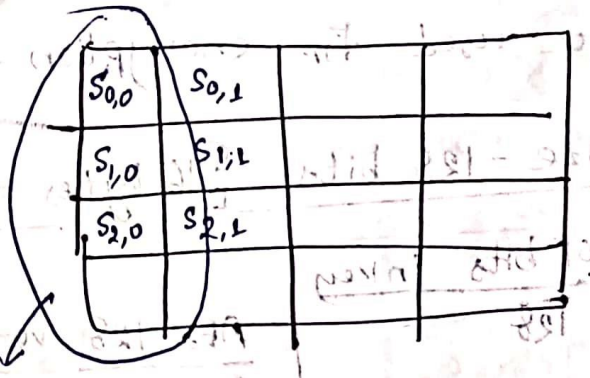
1 word = 4 bytes
= 4 x 8 = 32 bit

Block size = 128 bits

* No. of keys generated by key expansion = (No. of rounds + 1)

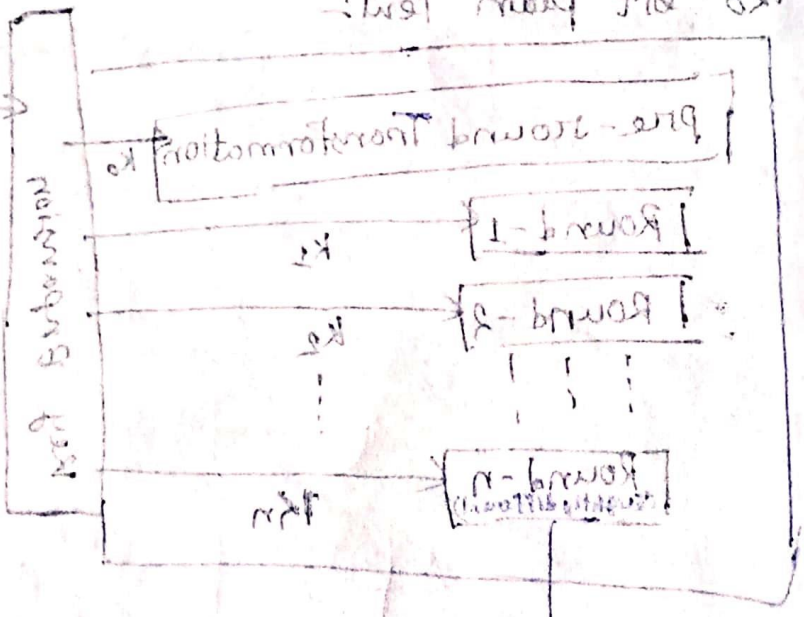
16 bytes (4×4) matrices

Input Array :- (4×4 = 16 bytes, 128 bits or 4 words)




1 word = 4 bytes

| Rounds | |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |



Steganography:- The practice of concealing information within another message or physical object to avoid detection.

The difference between cryptography & steganography:

| cryptography | Steganography |
|---|---|
| ① Secure content message | ① Hide the existence message. |
| ~~② Hidden message is not apparent~~ | ~~② Enc~~ |
| ② Encrypted message visibly scrambled. | ② Hidden message is not apparent. |
| ③ Ciphertext is obvious but unreadable | ③ Difficult to detect without specific tools. |
| ④ Secure data transmission, authentication etc. | ④ Digital right management. |
| ⑤ Symmetric, asymmetric encryption, hashing, digital signature. | ⑤ Embedding data in LSB |

| | |
|---|---|
| ⑤ Hiding | ⑤ can be combined with cryptography |
| ⑥ Can be combined with steganography. | |

The difference between cryptography & steganography:

| Cryptography | Steganography |
|---|---|
| ① Secure content message | ① Hide the existence message. |
| ② Encrypted message visibly scrambled. | ② Invisible |
| ③ Ciphertext is obvious but unreadable. | ③ Hidden message is not apparent (text) |
| ④ Secure data transmission, authentication etc. | ④ Difficult to detect without specific tools. |
| ⑤ Symmetric, asymmetric encryption. Involving digital signatures. | ⑤ Digital image message. |
| | ⑥ Embedding data in LSB |

# DES

→ 64 bit plain Text block.

↳ 16 rounds, each round is a Feistal round.

**Steps:-**

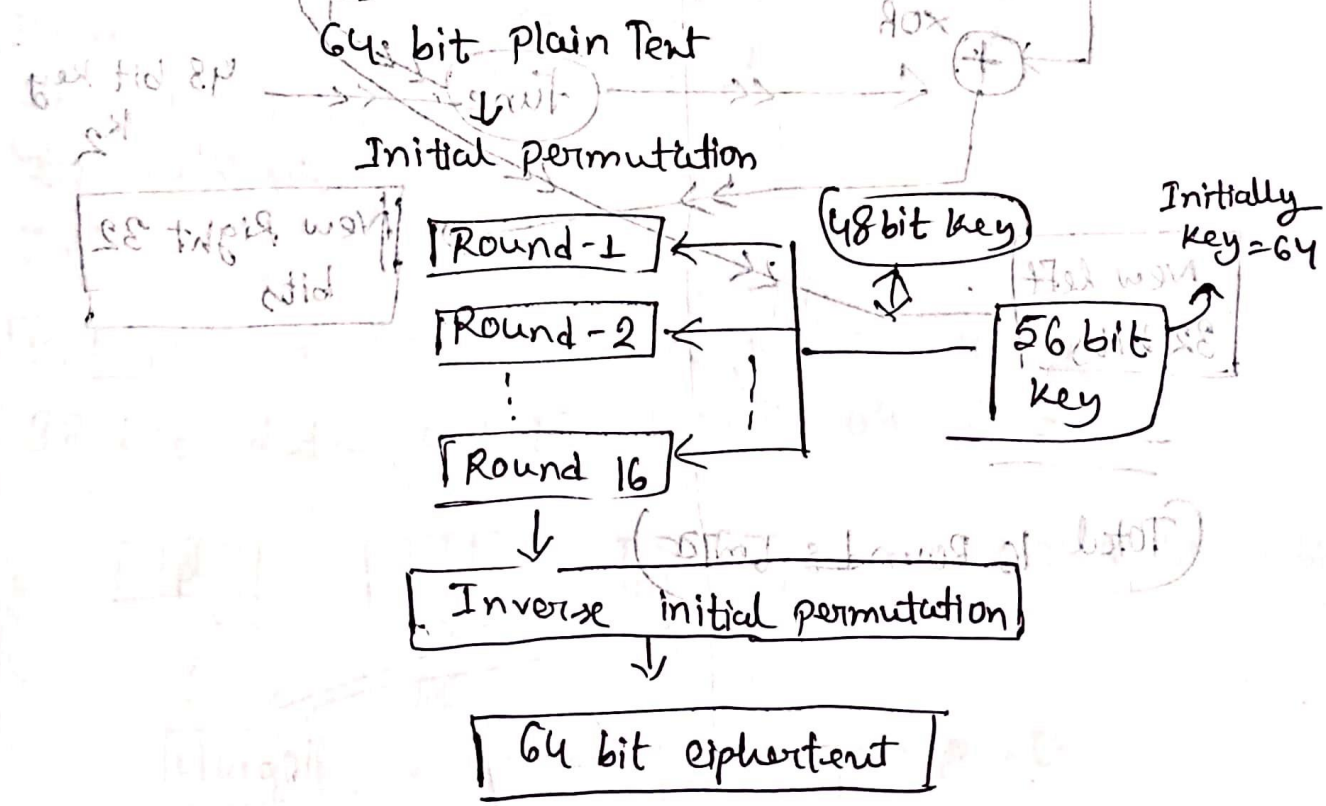
① Initial permutation.

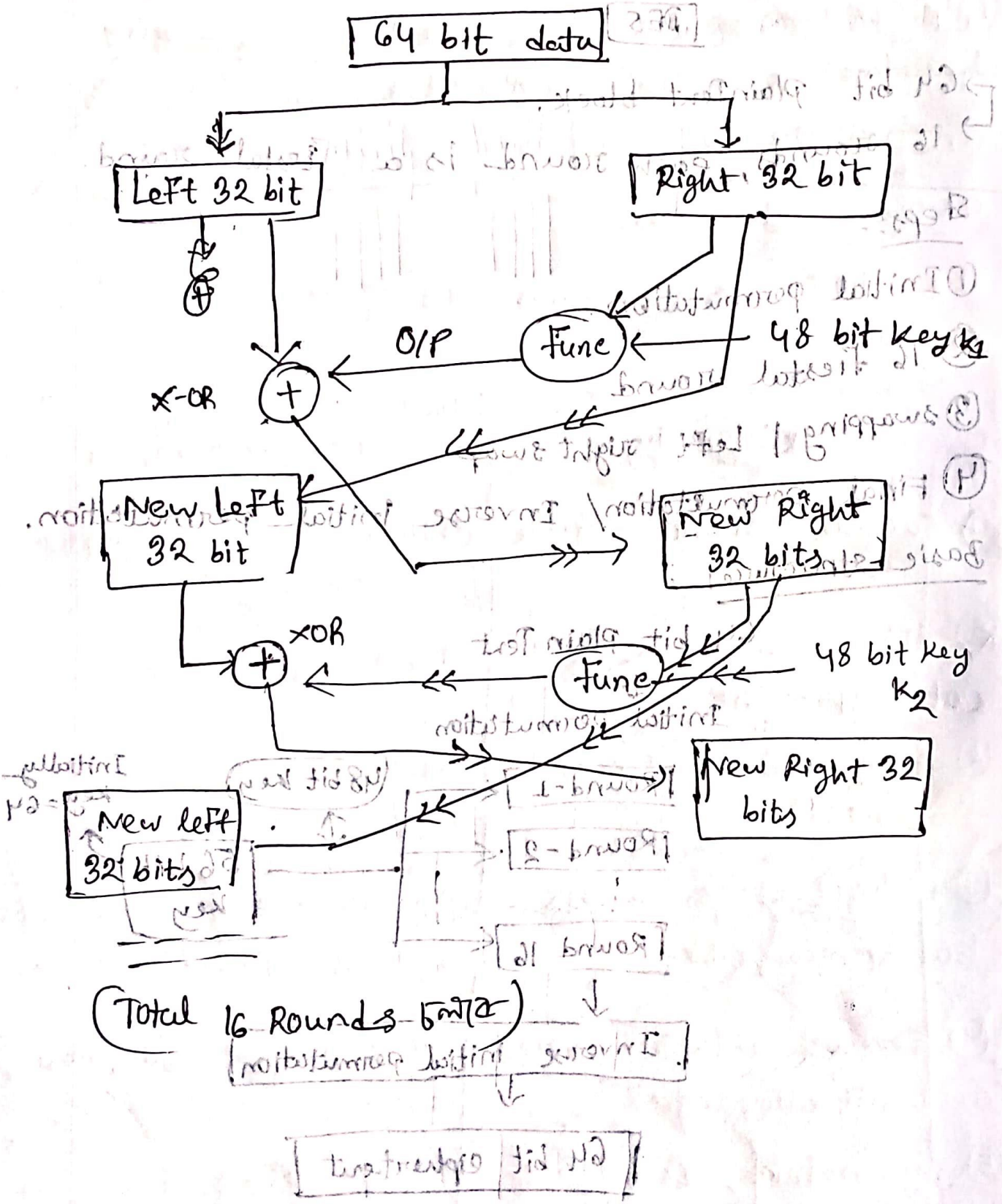
② 16 Feistal round

③ swapping | Left right swap

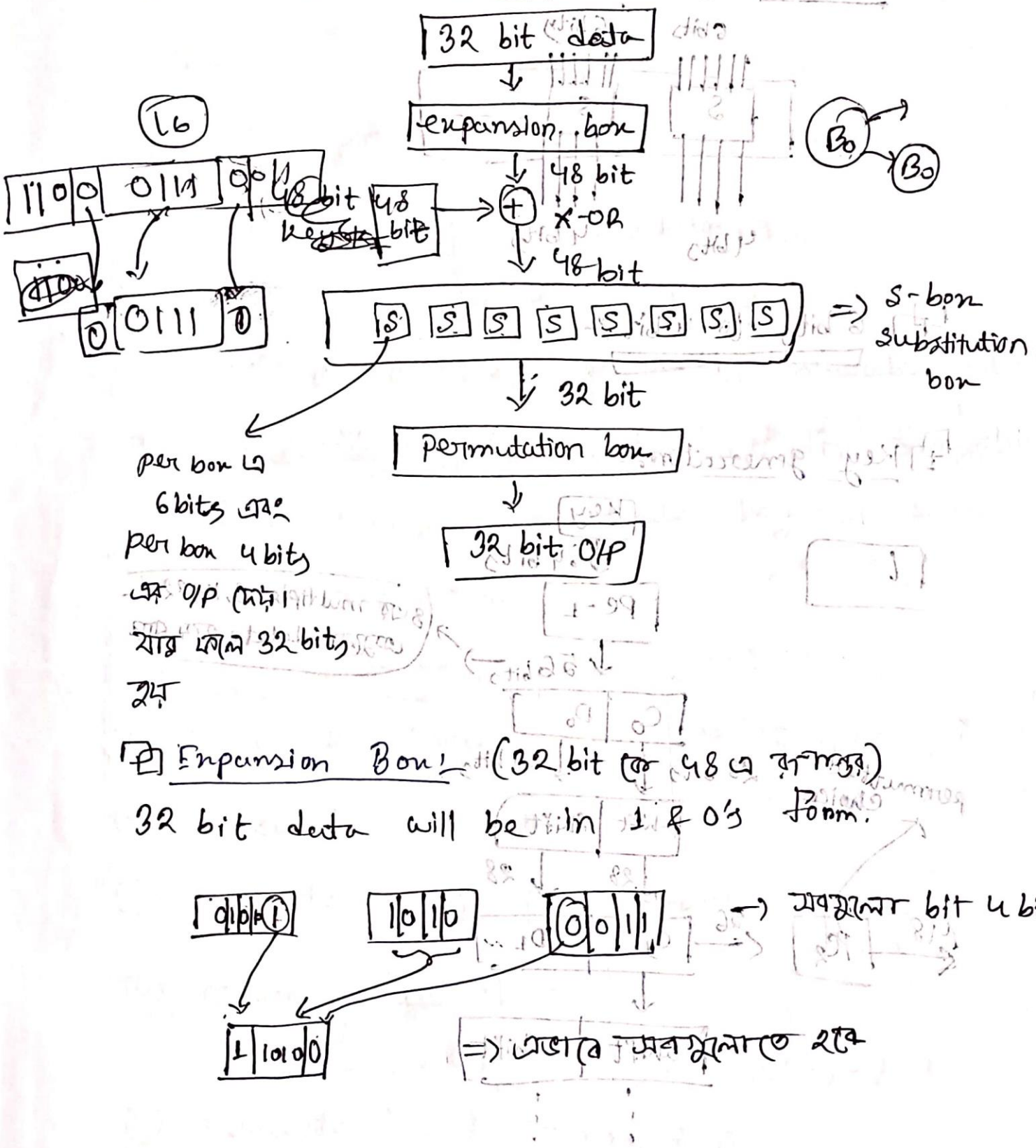
④ Final permutation/ Inverse Initial permutation.

**Basic structure:-**

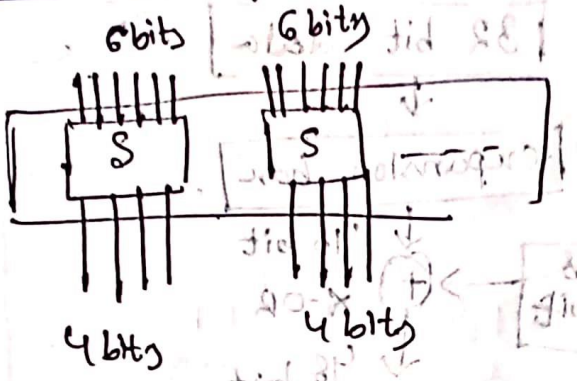



64 bit data
Left 32 bit
Right 32 bit
O/P
Func
48 bit key $k_1$
X-OR
New Left 32 bit
New Right 32 bits
XOR
Func
48 bit key $k_2$
New Right 32 bits
New left 32 bits
Total 16 Rounds

Func. (Function Definition) :-

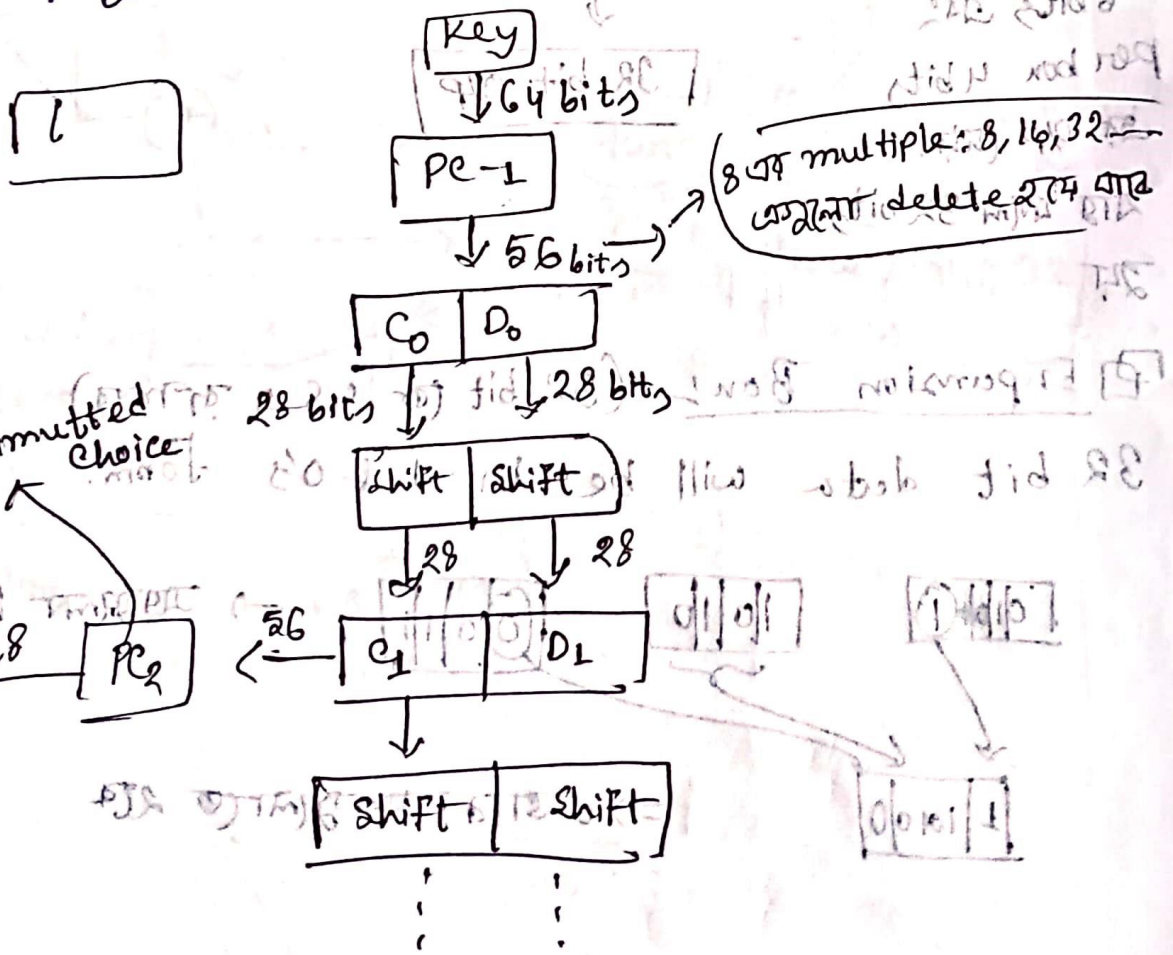


## S-box :- (48 bits → 32 bits, convert)




## 6 bits to 4 bit :-

## Key generation :-



11110000

~~1011~~ 0.

## RSA Algorithm:- Rivest-Shamir-Adleman

An asymmetric cryptographic algorithm.

Public Key → Known to all users in N/w

Private Key → Kept secret, not shareable at all.

If Public Key of user-A is used for encryption, we have to use the private key of same user for decryption.

### 1] Key Generation:-

(1) Select 2 large prime p & q

(2) Calculate; $n = p * q$

(3) Calculate $\phi(n) = (p-1) * (q-1)$ [euler Totient fn]

(4) Choose value of e

$1 < e < \phi(n)$ & $\gcd(\phi(n), e) = 1$

(5) Calculate $d = e^{-1} \bmod \phi(n)$

$ed \equiv 1 \bmod \phi(n)$

(6) public key = {e, n}

(7) private key = {d, n}

Question:

$p = 3, q = 11, e = 7$

$n = p * q = 3 * 11 = 33$

$\phi(n) = (p-1) * (q-1) = 2 * 10 = 20$

so, let $e = 7$ as $1 < 7 < 20$ & $\gcd(7, 20) = 1$

Now,

$d = e^{-1} \bmod \phi(n)$

$de = 1 \bmod \phi(n)$

$de \bmod \phi(n) = 1$

$7 * d = 1 \bmod \phi(n)$

$(7 * d) \bmod 20 = 1 \quad (\because d = 3)$

Since, $e = 7, d = 3$

Public key = $\{e, n\} = \{7, 33\}$

private key = $\{d, n\} = \{3, 33\}$

## Encryption (RSA)

$C = M^e \bmod n \quad [M = 31]$ — M < n (question থেকে)

$C = 31^7 \bmod 33$

$= 4$

[e, n public key using in Encryption]

## Decryption:-

$M = C^d \bmod n$ [d, n private key using in decryption.]

$= 4^3 \bmod 33 = 31$

---

## [Euler's Totient Function]

=> Represented using phi as $\varphi(n)$ & may also be called Euler's phi Function.

$f^n$ is defined as the number of the integers.

$\varphi(5) = \{1, 2, 3, 4\} = 4$ (values that are giving gcd = 1)

$\varphi(6) = \{1, 5\} = 2$

[gcd 1 থাকলেই Euler's Totient]

When n is prime, $\varphi(n) = n - 1$

$\varphi(5) = 4$

$\varphi(25) = 24$

If, $\varphi(a*b) = \varphi(a) * \varphi(b)$ [a & b should be coprime gcd=1]

$\varphi(15) = \varphi(3) * \varphi(5) = 2 * 4 = 8$

## Diffie Hellman

→ Not encryption algo

→ used to exchange key between sender & receiver.

Algorithm:

① Consider prime number : 'q'

② Select $\alpha$ such that it must be the primitive root of q & $\alpha < q$

(Primitive root check...

$a^1 \bmod q$

$a^2 \bmod q$

$a^3 \bmod q$ ---- $a^{q-1} \bmod q$

For mod = $(A-A) \div (B \times B)$

Alice, Bob — prime, $q = 17 \rightarrow (n)$

root, $= 5 \rightarrow (a)$

Alice, Secret, $x_a = 4$ (sender)

Bob, $x_b = 6$ (receiver)

So, public key,

Alice, $y_a = (a)^{x_a} \cdot \text{mod } n$

$= (5)^4 \cdot \text{mod } 17$

$= 13$

Bob $y_b = (a)^{x_b} \cdot \text{mod } n$

$= (5)^6 \cdot \text{mod } 17$

$= 2$

Now, secret key,

Alice, secret key $= (y_b)^{x_a} \cdot \text{mod } n$

$= (2)^4 \text{ mod } 17$

$= 16$

Bob, secret key $= (y_a)^{x_b} \cdot \text{mod } n$

$= (13)^6 \text{ mod } 17 = 16$

## RSA algorithm

encryption = $C = P^e \bmod n$ (e → public key)

C ↓ cipher, P ↓ plain

Decryption :- $P = C^d \bmod n$ (d → private key)

public key = $\{e, n\}$

private key = $\{d, n\}$

### Math-

$P = 17,\ q = 11,\ e = 7,\ M = 88$

$n = 17 \times 11 = 187$

$\phi(n) = (17-1) \times (11-1) = 160$

we know,

$d = e^{-1} \bmod \phi(n)$

$\Rightarrow d \cdot e \bmod \phi(n) = 1$

$\Rightarrow d \cdot 7 \bmod (160) = 1$

$\Rightarrow 23 \cdot 7 \bmod (160) = 1$

$\therefore d = 23$

∴ Encryption, $C = M^e \bmod (n)$

$= (88)^7 \bmod (187)$

$= 11$

$88^1 \bmod 187 = 88 \bmod 187$

$88^2 \bmod 187 = 77 \bmod 187$

$88^4 \bmod 187 = 77^2 = 132 \bmod 187$

$= (88 \times 77 \times 132) = 89432 \bmod 187$

$= 11$

$\therefore C = 11.$

∴ Decryption $= C^d \bmod (n)$

$= (11)^{23} \bmod 187$

$11^1 \bmod 187 = 11$

$11^2 \bmod 187 = 121.$

$11^4 \bmod 184 = 55$

$11^8 \bmod 187 = 71.$

$(11 \times 121 \times 71) \bmod 187 = 88$

## (3b) Euler's Totient:-

Euler's Function $\phi(n)$, counts the number of positive integers up to $n$ that are relatively prime to $n$.

**Example:-**

$n = 9$

So, the integers less than 9 are: 1, 2, 3, 4, 5, 6, 7, 8

The numbers that are coprime to 9 are: 1, 2, 4, 5, 7, 8

∴ Therefore, $\phi(9) = 6$

**General Formula:-**

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$$

**Example:-** $n = 12$

Prime factorization $= 2^2 \times 3$

$$\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$$

$$= 12 \times \frac{1}{2} \times \frac{2}{3} = 4$$

## Concept of Network penetration?

A process used to evaluate the security of a computer network by simulating an attack.

### Key concepts:-

(1) Gathering info about target network to identify potential entry.

(2) Using tools to scan the network.

(3) Developing custom exploits to breach network defenses.

(4) Once access is gained, the focus shift to maintaining access, gathering info.

(5) Documenting findings, providing detailed reports to stakeholders.

### penetration Testing:-

(1) planning:- Define scope & goal
- Collect (domain names, mail servers etc) to understand how target works.

(2) Scanning:-
- Inspect the code
- Inspect the the application

(3) Gaining access

(4) Maintain Access

(5) Analysis & Reporting

(6) Clean-up

Network penetration testing is a critical component of a organization's cybersecurity strategy. It involves a systematic approach to identifying, exploting & documenting within a network to improve its security defenses.

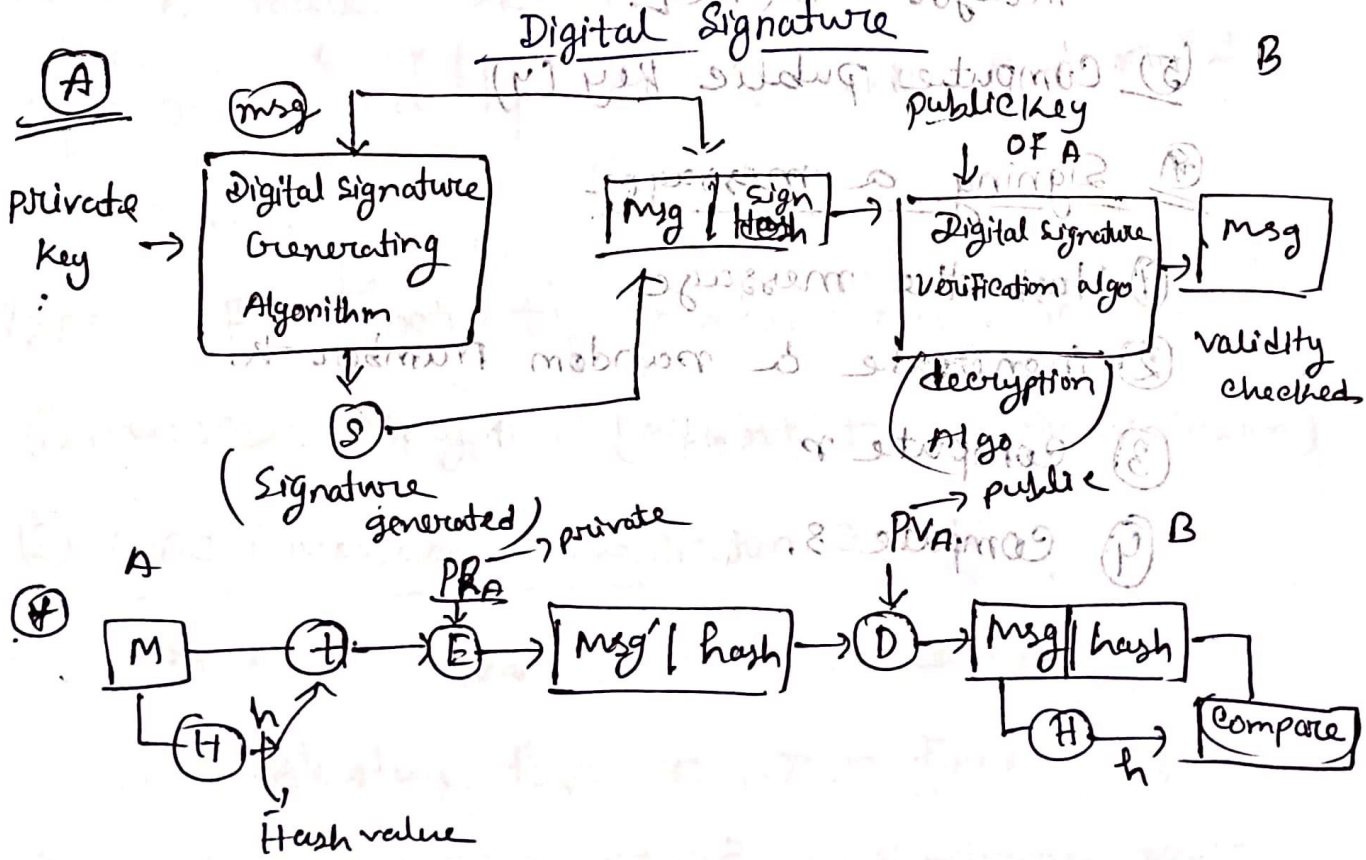



Fig:- Concept of D.Signature

→ Must use same info unique to the sender to prevent the denial.

→ It must be easy to produce digital signature

→ Easy to verify & recognize signature.

* **Key generation:-**

(1) Choose a prime number P.

(2) Choose a prime number q.

(3) Choose $g$ such that $g = h^{(p-1)/q}$

(4) Choose private key (x):- A randomly chosen integer $0 < x < q$

(5) Compute public key (y)

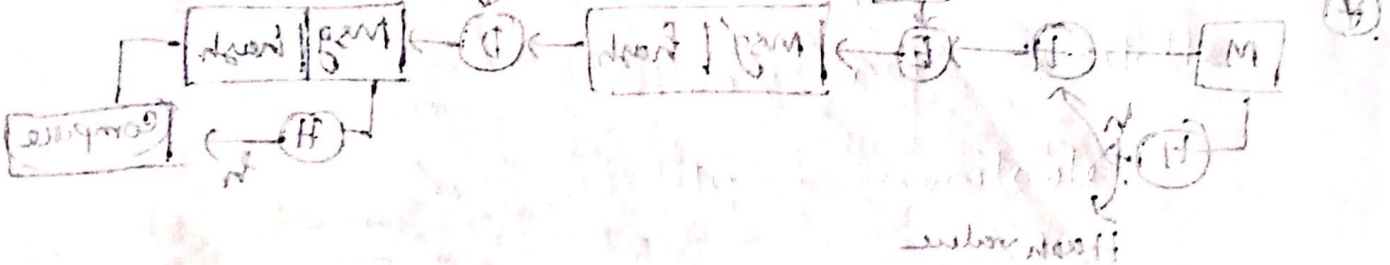
* **Signing a message:-**

(1) Hash the message

(2) Generate a random number - k.

(3) Compute r

(4) Compute s.



Confidentiality:- Refers to protecting the information from being accessed by unauthorized parties.

Data Integrity:- Data modification.

Authentication:- verify the user's identity.

## Authentication function:

Authenticator must be there to authenticate the message.

→ A value which is ~~sent~~ used to authenticate message & a function is which authenticate a message.

Types of function to produce Authentication:

① Message Encryption (ciphertext as Authenticator)

② MAC (Message Authenticator code):-

C(M, K) = Fixed length code (MAC)

যেকোন message নিয়ে তা থেকে Fixed length এ Convert করে। আর এটাকেই authentication verify বলে।

(iii) Hash Function:-

$H(M) \xrightarrow{msg}$ = Fixed length code (Hash code 'h')

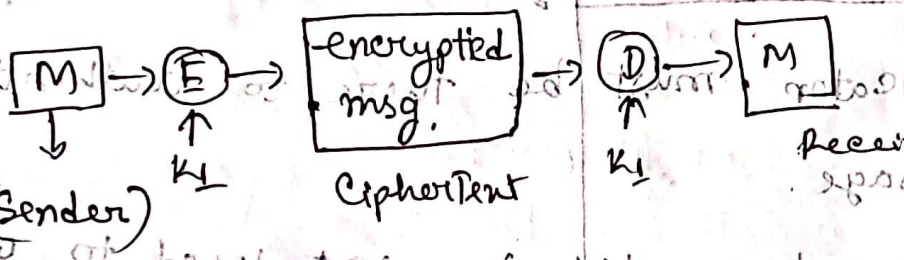
↓

Independent of key

Digram:

Message Encryption:-

① ciphertext is an authenticator.



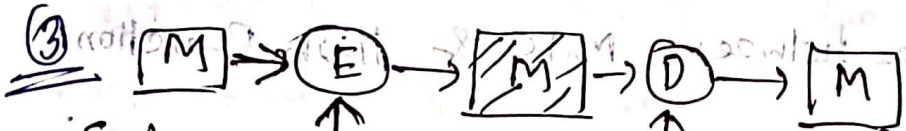

⇒ key $K_1$ is shared between sender & receiver only. [Both key same = Asymmetric]

② Symmetric :- [Different key]


→ Here Authentication is not available

↳ But Confidentiality is available.

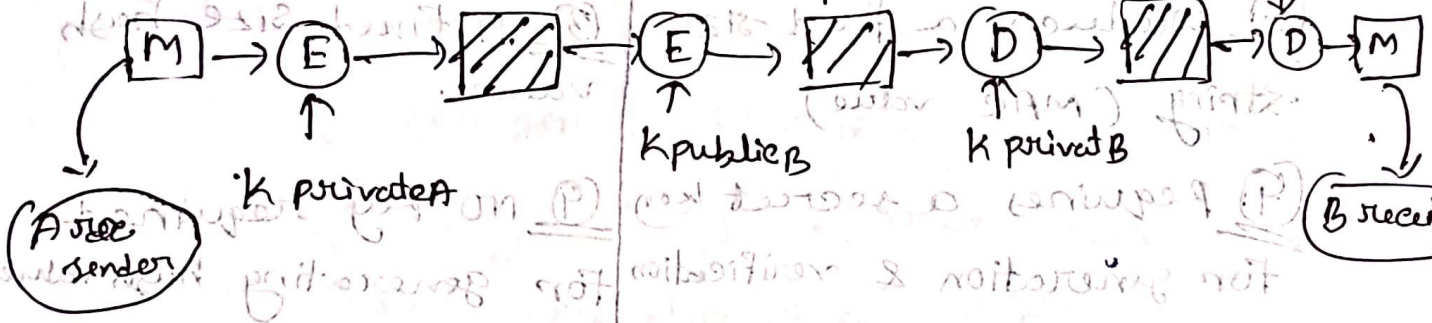
③




→ Authentication available

→ Confidentiality not available.

④ To get both Authentication & Confidentiality:-



5(b) Difference between MAC & Hash Function

| MAC (Message Authentication Code) | Hash Function |
|---|---|
| (1) provides data integrity & authencity. | (1) provides data integrity only. |
| (2) Takes a message & a secret key as input. | (2) Takes only a message as input. |
| (3) produces a fixed size string (MAC value) | (3) A fixed size hash value. |
| (4) Requires a secret key for generation & verification | (4) NO key required for generating hash values. |
| (5) Used for authentication to ensure message authenticity & integrity. | (5) Used for data integrity verification |

Security of Hash Functions :-

(1) preimage Resistance :-

→ Computationally infeasible to find any input x, such that $H(x) = h$, where h is a given hash value.

(2) Second preimage resistance :

$$H(x_1) = H(x_2)$$

This helps to prevent an attacker from finding

a different message that has the same hash value as a given message.

(b) Collision Resistance:-

Ensures that two different messages can't produce the same hash value.

Security OF MAC:-

(i) Confidentiality of the key:-

↳ Key management practices are critical, including using strong, random keys & protecting them from unauthorized access.

(ii) Resistance to forgery:-

↳ A secure MAC should make it computationaly infeasible for an attacker to generate a valid MAC for a message without knowing the secret key.

(iii) Replay Attack prevention:- An attacker reuses a valid message & its MAC deceive the receiver.

(iv) Algorithm Security:- The underlying cryptographic algorithm be secure against known attacks.

# MAC (From vd)

→ Will use a secret key

→ Generate a small fixed size of data
↳ compressed MAC
called MAC.

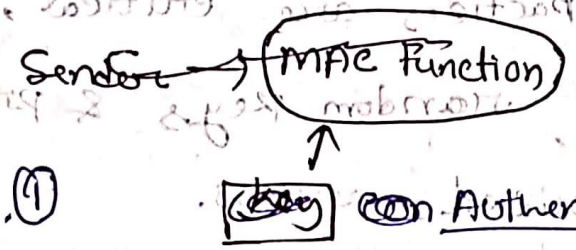
→ Then will append with the message.

→ Sender, receiver will have a secret key.

(i)

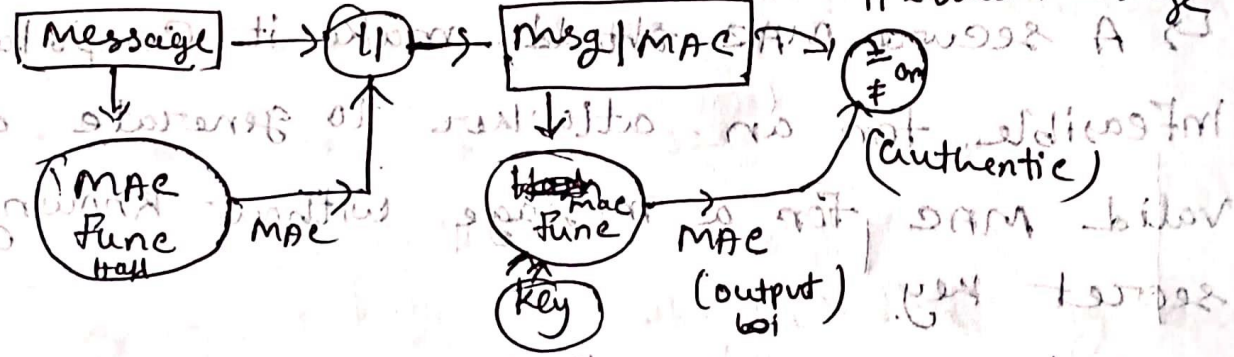
A → B

MAC = C (K, M)
↳ Key (common)
↳ message



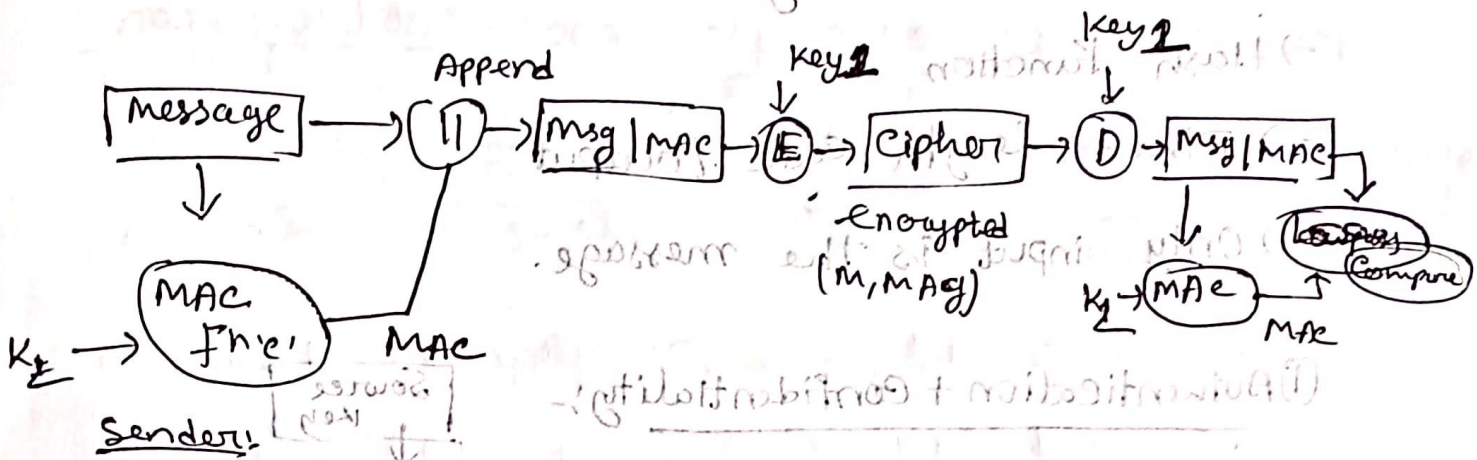

(ii) Authentication :-

Sender




(iii) ⇒ Here, Hash func added to message new message creates. Then again MAC Func is used with key. Again an output is generated which is MAC. if equal they are authentic if not then not authentic.

## ② Authentication & Confidentiality:




**Sender:**

⇒ Apply message + key 1 in encryption algorithm & will get output.

⇒ This O/P + key 2 given to MAC function

→ Now the Authentication text to cipher Text

**Receiver:**

⇒ We will give it as input to Decryption algorithm using key-1 & output message.

# Hash from (Rd)

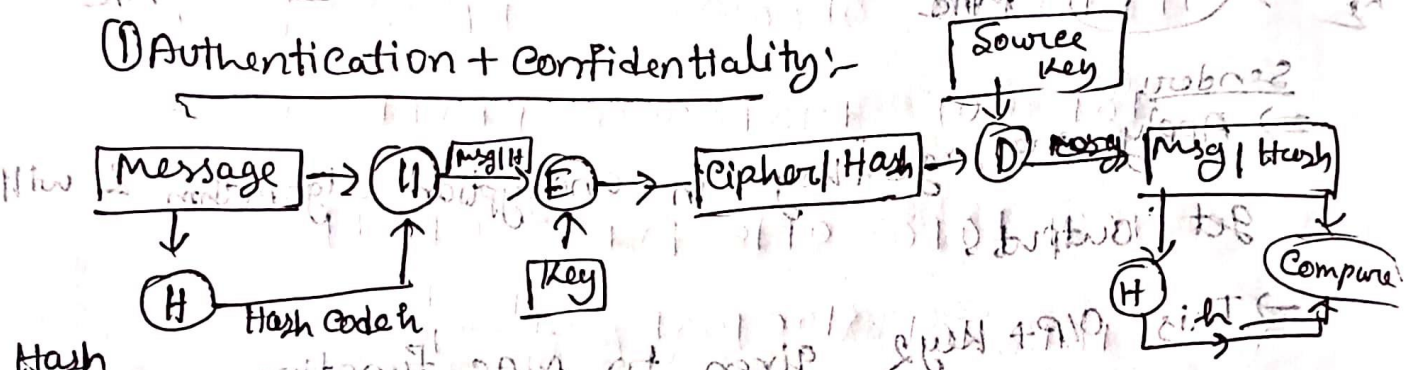
⇒ Does not use a key like MAC

→ Hash function

→ Fixed length code / output

→ Only input is the message.

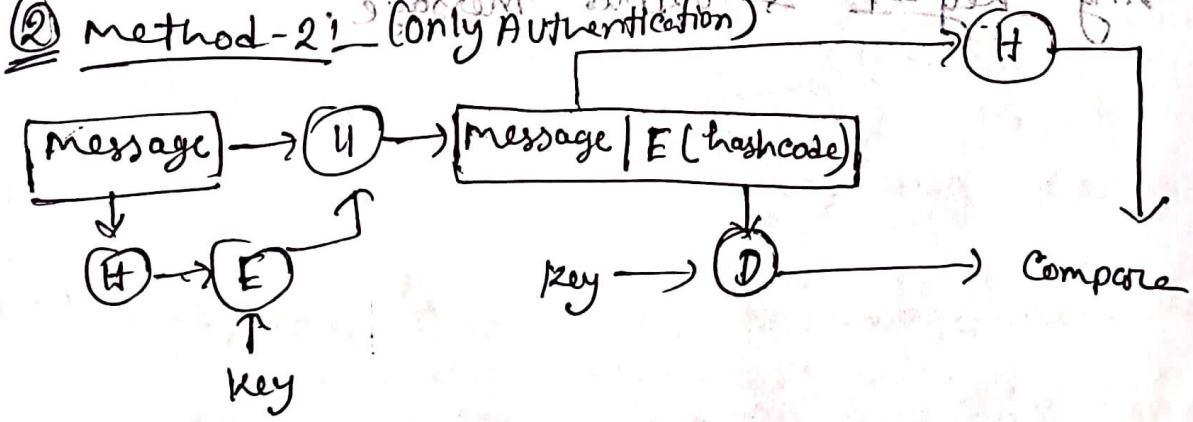
① Authentication + Confidentiality:-




Authentication:- If both hashcodes equal

Confidentiality:- message was encrypted before sending.

② Method-2:- (only Authentication)




→ processing time low

→ Same key used 2 times

# DES

Method 3

1, 2, 9, 16 = 1 shift
बाकि = 2 shift

Binary Notation :- K = 0000 0001 0010 0011 0100 0101
1-8 9-16 17-24

0110 0111 1000 1001 1010 1011 0100 1101 1110 1111
25-32 33-40 41-48 49-56 57-64

Now, we will apply 56 bit PC-1.

$C_0$ = 0000 0001 0010 0011 0100 0101 0110 0111
1-8 9-16 17-24 25-32

$D_0$ = 1000 1001 1010 1011 0100 1101 1110 1111
33-

K' = 1011000 1010100 1100110 0001110 0000000 0000000 0000000 0000000

1, 2, 9, 16 = 1 shift
बाकि = 2 shift

$C_0$ = 1011000 0110011 0010101 0100000

$D_0$ = 1010101 0110011 0011110 0000000

$C_1$ = 0110000 1100110 0101010 1000001
1-7 8-14 15-21 22-28

$D_1$ = 0101010 1100110 0111100 0000011 } $K_1$
29-35 36-42 43-49 50-56

$C_2$ = 1100001 1001100 1010101 0000010
1-7 8-14 15-21 22-28

$D_2$ = 1010101 1001100 1111000 0000010 } $K_2$
29-35 36-42 43-49 50-56

$C_3 = \underbrace{0000110}_{1-7}\ \underbrace{0110010}_{8-14}\ \underbrace{1010100}_{15-21}\ \underbrace{0001011}_{22-28}\ \Big\}\ k_3$

$D_3 = \underbrace{1010110}_{29-35}\ \underbrace{0110011}_{36-42}\ \underbrace{1100000}_{43-49}\ \underbrace{0001010}_{50-56}$

Now we will apply PC-2,

$k_1 = 00000011\ 00000010\ 01100111$

$10011011\ 01001001\ 10100101$

$k_2 = 01101000\ 10100110\ 01011001$

$10011011\ 01001001\ 10100101$

$k_3 = 01000101\ 11010100\ 00001010$

$10110100\ 00101000\ 11010010$

∴ $k_1, k_2, k_3$ are ~~opt~~ Obtained

## RSA Math:

$P=17,\quad q=11,\quad e=7, M=88$

$n = p*q = 17*11 = 187$

$\phi(n) = (P-1) \times (q-1) = 16 \times 10 = 160$

we know,

$d = e^{-1} \bmod \phi(n)$

$\therefore d \times e \bmod \phi(n) = 1$

$\therefore d \times 7 \bmod (160) = 1$

$\therefore (23 \times 7) \bmod (160) = 1$

$\therefore d = 23$

Now, encryption, $= c = m^e \bmod (n)$

$= (88)^7 \bmod 187$

$88^4 = 132$

$88^4 \bmod 187 = 132$

$88^3 \bmod 187 = 44$

$132 \times 44 = 5808 \bmod 187 = 11$

$\therefore$ decryption, $= c^d \bmod n$

$= (11)^{23} \bmod (187)$

$(11)^8 \times (11)^8 \times (11)^7 =$

$(11)^2 = 33 \bmod 187$

$(11)^7 = 88 \bmod 187$

$\therefore (33 \times 33 \times 88) \bmod 187$

$= 88$

Ans

## Diffie-Hellman math:

(i) primitive root of 11:-

$(2)^1 \bmod 11 = 2$

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

$(2)^3 \bmod 11 = 8$

$(2)^4 \bmod 11 = 5$

$(2)^5 \bmod 11 = 10$

$(2)^6 \bmod 11 = 9$

$(2)^7 \bmod 11 = 7$

$(2)^8 \bmod 11 = 3$

$(2)^9 \bmod 11 = 6$

$(2)^{10} \bmod 11 = 1$

$2^8 = 256$

$256 \times 2 = 512$

$512 \times 2 = 1024$

(ii) Here, A has public key, $y_A = 9$

So, A's private key $x_A = ?$

We know, $y_A = a^{x_A} \bmod q$

$y_A = (2)^{x_A} \bmod (11)$

$\Rightarrow 9 = (2)^{x_A} \bmod (11) = 2^6 \bmod 11$

$\therefore x_A = 6$