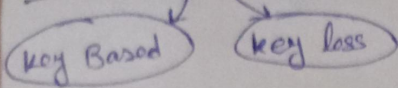


## Cryptography and Network Security



- Security
- Types of Security
  - 1) No Security
  - 2) ID & Password
  - 3) Obscurity
  - 4) Security through encryption

## Security Services/Principle of Security

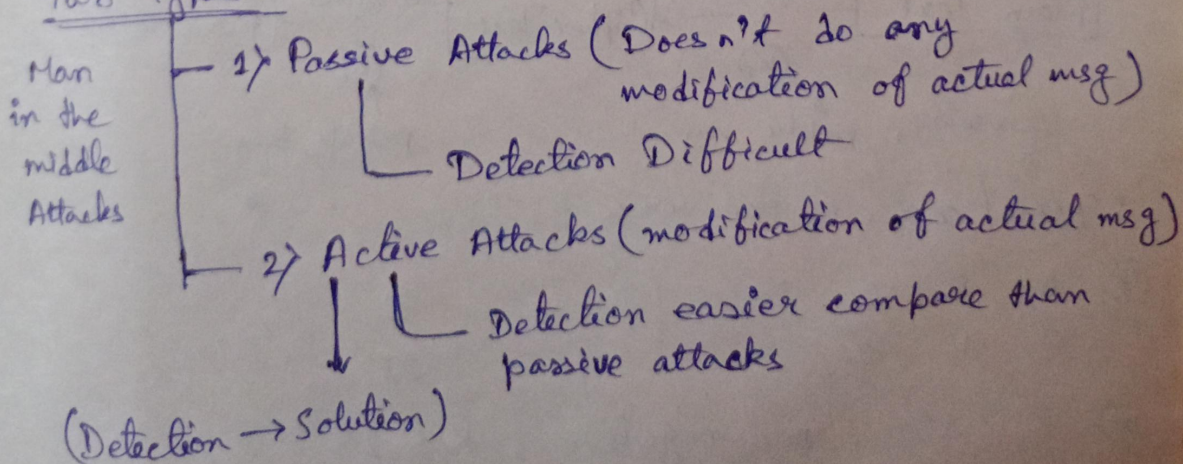
- i) Non-Repudiation  
(False Identification or you can't denied anything)
- ii) Authentication
- iii) Access Control
  - Role Management (User Specific)
  - Rule Management (Resource)

C I A → Confidentiality Integrity Availability

## Various types of security :-

### Attack

#### Two Types :-





# Cryptography

The art/science of achieving security through encryption

method to convert plain text to cipher text

[Easily readable & Understandable] [Non-Meaningful Text]

## Key

① Symmetric key cryptography

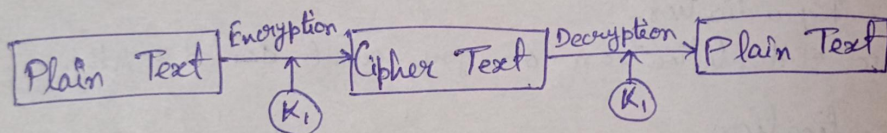
(Private key cryptography)

① Symmetric key

② Asymmetric key cryptography

(public key cryptography)

[used → i public key  
ii private key]

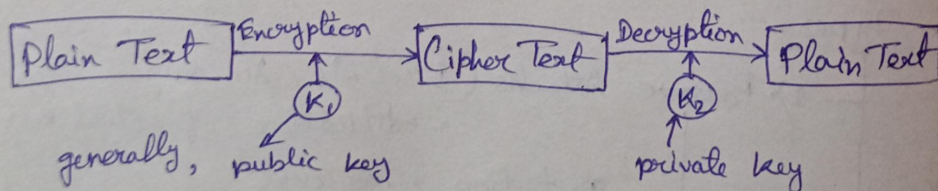


• one of algorithm

① Data Encryption Standard (DES) / DEA → Algorithm

② Asymmetric : (public)

(public key + private key)



generally, public key

private key

• special case → vice-versa

⊛ A B C D . . . . . Z  
0 1 2 3 . . . . . 25

⊛  $K \geq 1$ , non-negative,  $K \leq 25$   
 $1 \leq K \leq 25$  for ceaser cipher

Ex: HELLO, key = 4

$$e(H) = E(H, 4) = (H + 4) \bmod 26 = (7 + 4) \bmod 26 \\ = 11 \bmod 26 \\ = 11 \\ \Rightarrow L$$

E  $\rightarrow$  I  
L  $\rightarrow$  P  
L  $\rightarrow$  P  
O  $\rightarrow$  S

Cryptography Algorithm is divided into 2 parts

Substitution  
+4 / +const

Transposition (changing position of character)  
Key based      Key less

\* Hash Code:  $\rightarrow$  Do not use any key  
 $\searrow$  Uses Hash fn

Message Digest:

Fixed length for var.

MD5

\* 1<sup>st</sup> Algo. ever proposed

Caesar Cipher  $\rightarrow$  Mono alphabetic Cipher

C	B	A	S	E	R
+3 ↓	+3 ↓	+3 ↓	+3 ↓	+3 ↓	+3 ↓
F	H	D	N	H	U

Poly

H	B	Y	T	H	E	R	E
+	+	+	+	+	+	+	+
J	G		X	A	Y		

Example<sup>1</sup>:

Meet me at Two PM, Key = 4

+4 ↓	+4 ↓	+4 ↓	+4 ↓	+4 ↓	+4 ↓
------	------	------	------	------	------

\* Cyclic after Z

W	X	Y	Z
+4 ↓	+4 ↓	+4 ↓	+4 ↓
A	B	C	D

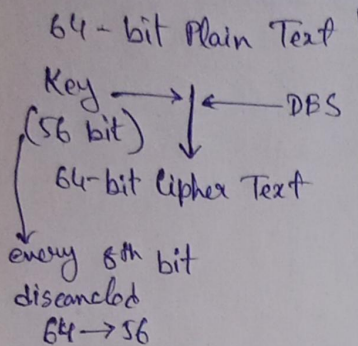
Formula:  $\rightarrow$  Encryption  
 $C = E(P, K) = (P + K) \bmod 26$   
 $\nwarrow$  Cipher

$\rightarrow$  no. of Alphabet

$$P = D(C, K) = (C - K) \bmod 26$$



Data Encryption Standard (DES) :



Steps

1. Key Transformation  
[56 bit → 48 bit Key]  
(left circular shift)

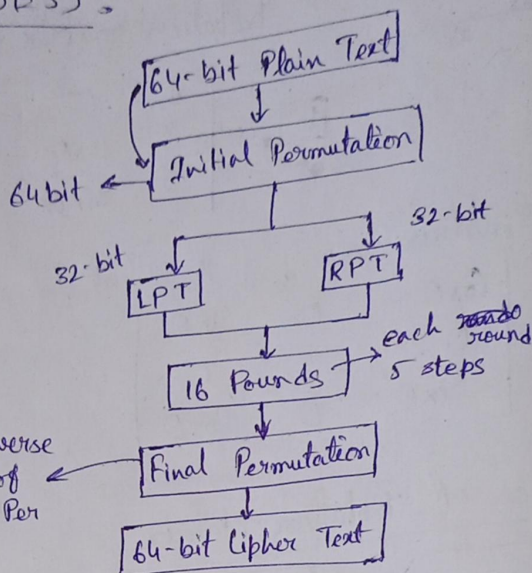
2. Expansion Permutation [32 bit → 48 bit]

3. S-box

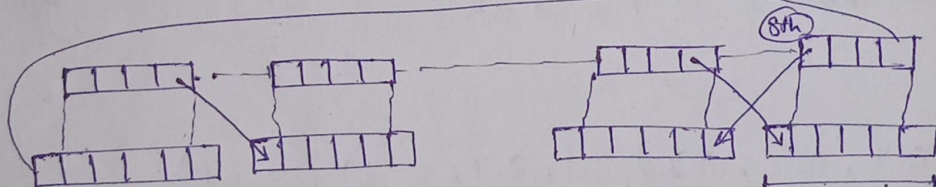
4. P-box

5. XOR and Swap

performed only on RPT



②



③ Substitution Box:

XOR operation of 48 bit (for 1) / and 48 bit (for 2)

Then 48 bit result in S-box.

Final output 32 bit from S-box

8 S-box, 64-bit, matrix/array

	0000	0001	0010	0011	0101	1111
00						
01						
10						
11						

16 Col.  
4 rows

values (0-15) → bit, 1111

col. number

10 → row number

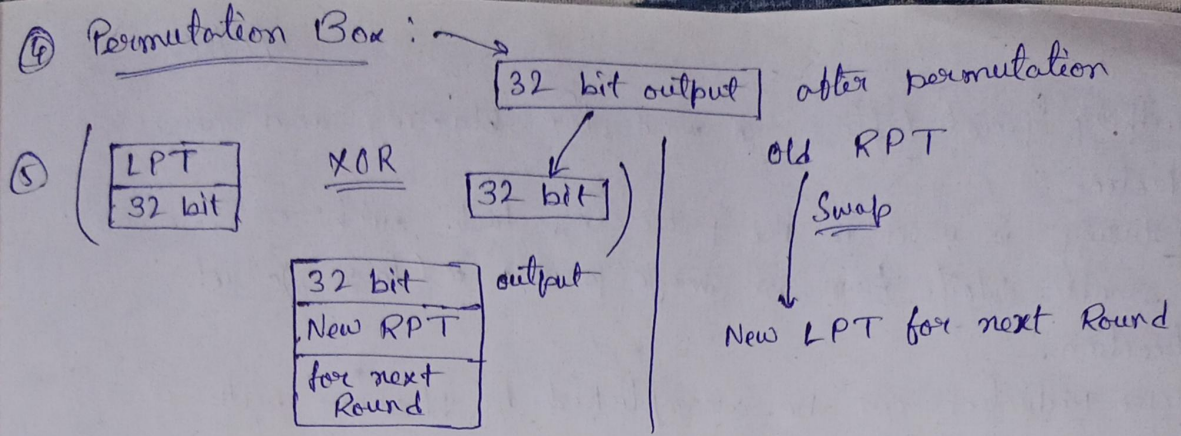
110110110

11111111

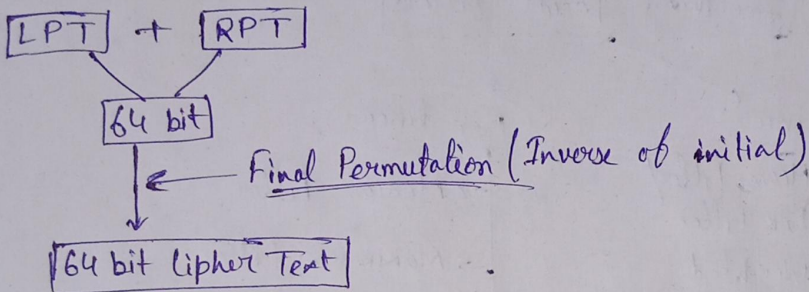
4 bit × 8 S-box

32 bit  
correct  
output





## After 16 rounds



## ## Analysis of DES:

### 1. Avalanche Effect:

A small change in plain text or key should create a significant change in Cipher Text.

### 2. Completeness Effect:

Each bit of the Cipher Text needs to depend on many bits of the plain Text.

## ## Weakness / Disadvantage of DES

(i) Parallel Processing in  $< 2$  min -

(ii) Plain Text  $\xrightarrow{\text{Enc.}}$  Cipher Text  $\xrightarrow{\text{Enc. Again}}$  Plain Text

4 weak keys. All 0's, All 1's, Half 0's, Half 1's

(iii) 6 sets - weak keys

(iv) 48 possible weak keys

(v) 2 diff. plain Text  $\rightarrow$  Same Cipher

(vi) 2 diff. keys  $\rightarrow$  same Cipher Text

# Cryptography

7/2/2025

## ① Diffie-Hellman Key Exchange Algorithm:

1.  $n, g \rightarrow$  prime numbers
2. Alice,  $x$ ,  $A = g^x \bmod n$
3. Alice send  $A$  to Bob.
4. Bob,  $y$ ,  $B = g^y \bmod n$ .
5. Bob sends  $B$  to Alice.

Large  
Prime Number

Alice,  
Bob



6. Alice  $\rightarrow K_1 = B^x \bmod n$ ,  
 7. Bob  $\rightarrow K_2 = A^y \bmod n$ .

Example:

1.  $n=7, q=11$

2. Alice  $\rightarrow A = \frac{7^3}{2} \bmod 7$   
 $= 2$

3. Alice  $\rightarrow 2 \rightarrow$  Bob

4. Bob  $\rightarrow B = \frac{7^6}{4} \bmod 11 = 4$

5. Bob  $\rightarrow 4 \rightarrow$  Alice

6.  $K_1 = 4^3 \bmod 11 = 9$

7.  $K_2 = 2^6 \bmod 11 = 9$

let,

$x=3, y=6$

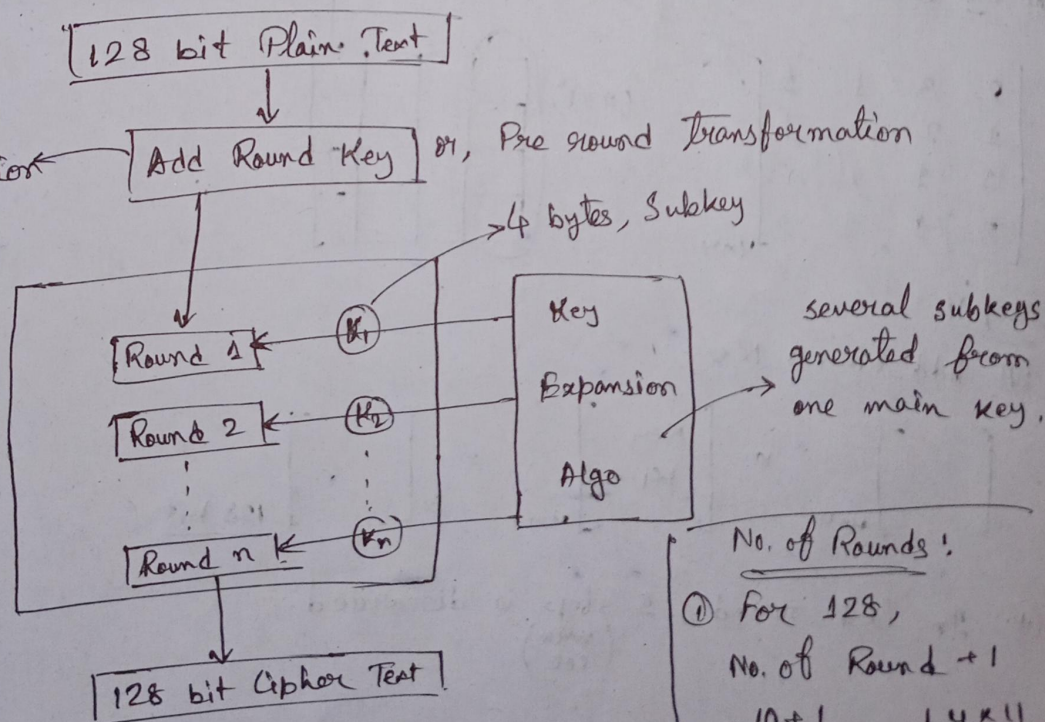
(\*) Advanced Encryption Standard (AES):

2000  
Rijndael  
pool

128 bit, plain Text

128 bits Cipher Text

Rounds	Length of Key	
10	128 bits	$\rightarrow$ AES-128
12	192 bits	$\rightarrow$ AES-192
14	256 bits	$\rightarrow$ AES-256



No. of Rounds:

- ① For 128,  
 No. of Round + 1  
 $= 10 + 1$   
 $= 11$  subkeys  
 [0 to 10]
- 4 x 11  
 44 bytes  
 subkeys



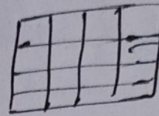
## Steps:

1. Substitution Bytes.
2. Shift Rows.
3. Mix Columns
4. Add Round Key

4 words

(Hexadecimal values)

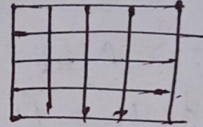
Converts To



Rows

Columns

Static Matrix



## Step 1

ABS  $\rightarrow$  S-box

16x16

## Step 2

Shift Rows

	1	2	3D	51
1	0	1	F	C
2	7	8	A	B
3	A	F	D	8

Left Shift

1	2	3D	51
1	F	C	0
A	B	7	8
8	A	F	D

0 shift

1 shift

2 bit left shift

3 bit left shift

i/p

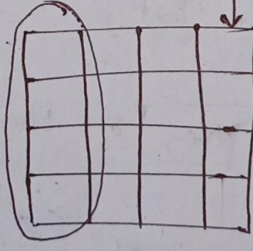
## Mix Columns:

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

(4x4)

(4x1)

Static Matrix



## Step 4

Add Round Key

$$\begin{bmatrix} \quad \end{bmatrix}_{4 \times 4} \otimes \begin{bmatrix} \text{Key} \\ K_1 \end{bmatrix}_{4 \times 1} = \begin{bmatrix} \quad \end{bmatrix}_{128 \text{ bit}}$$

In last round, 1 step is discarded.  
(mix col)