# Cryptography

7/01/2025

Cryptography and Network Security

Key Based    Key less

- 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 (Resources)

CIA → Confidentiality Integrity Availability

Various Types of security :-

Attack

Two Types :-

Man in the middle Attacks

1) Passive Attacks (Doesn't do any modification of actual msg)
Detection Difficult

2) Active Attacks (modification of actual msg)
Detection easier compare than passive attacks

(Detection → Solution)

## Cryptography :-

The art / science of achieving security through encryption

method to convert plain text to cipher text

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

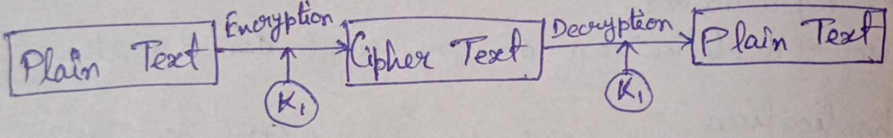
Key

① Symmetric key cryptography (Private key cryptography)

② Asymmetric key cryptography (public key cryptography)

[used → (i) public key (ii) private key]

① Symmetric key

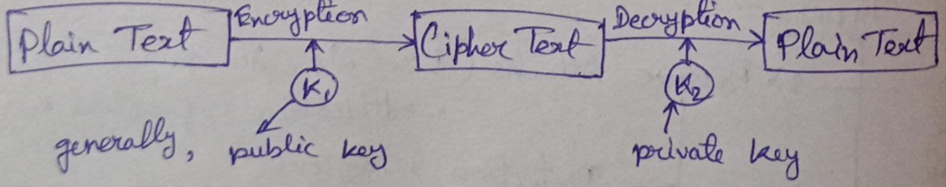


- One of algorithm

(i) Data Encryption Standard (DES) / DEA → Algorithm

② Assymmetric : (public)

(public key + private key)



- spacial 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 → I
L → P
L → P
O → S

Cryptography Algorithm is divided into 2 parts

- Substitution
  +4 / + const
- Transposition (changing position of character)
  - Key based
  - Key less

Hash Code: → Do not use any key
→ Uses Hash fn

Message Digest:
Fixed length for var.

MD5

1st Algo. ever proposed

Ceaser Cipher → Mono alphabetic Cipher

$$\begin{tikzcd}
C \arrow[d, "+3"'] & B \arrow[d, "+3"'] & A \arrow[d, "+3"'] & S \arrow[d, "+3"'] & E \arrow[d, "+3"'] & R \arrow[d, "+3"'] \\
F & H & D & N & H & U
\end{tikzcd}$$

Poly

H B Y      T H E R E

I G      X A Y

Example:

Meet me at Two PM, key = 4

+4 ↓↓↓↓
+4 +4 +4 +4

Cyclic after Z

$$\begin{tikzcd}
W \arrow[d, "+4"'] & X \arrow[d, "+4"'] & Y \arrow[d, "+4"'] & Z \arrow[d, "+4"'] \\
A & B & C & D
\end{tikzcd}$$

Formula: Encryption

$C = E(P, K) = (P+K) \bmod 26$

Cipher

no. of Alphabet

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

Crypto

31/1/2025

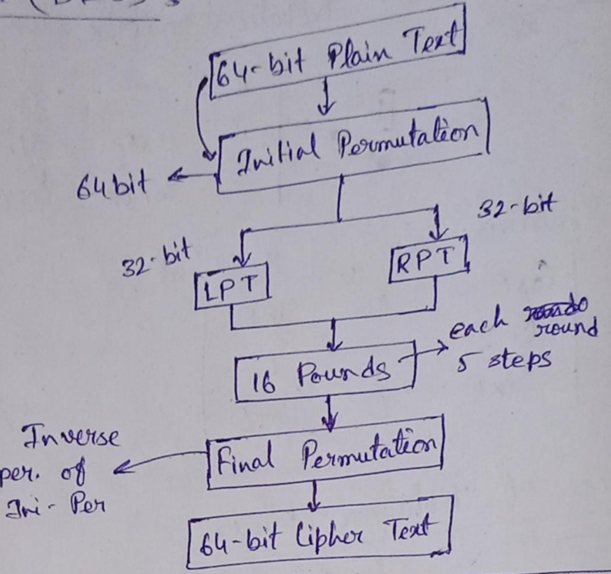
Sem-6

## Data Encryption Standard (DES):

64-bit Plain Text

Key → | ← DES
(56 bit)
↓
64-bit Cipher Text

every 8th bit discarded
64 → 56

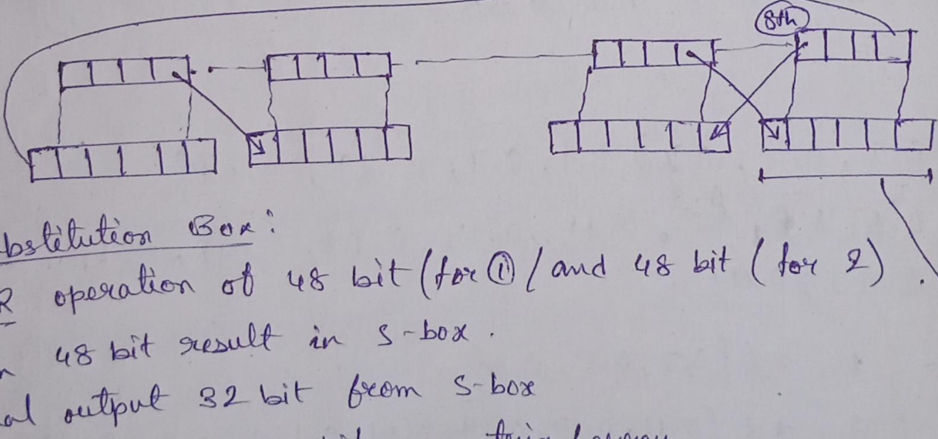


Steps

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

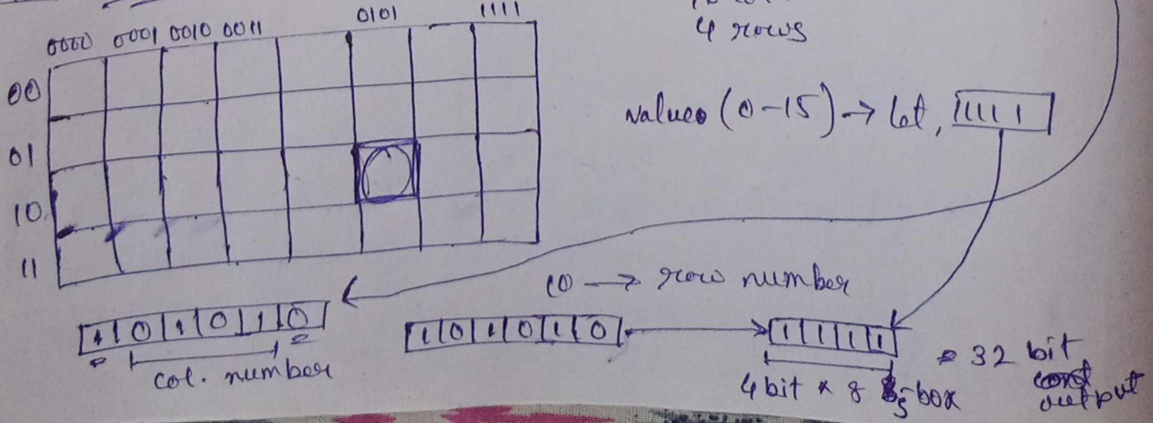
XOR operation of 48 bit (for ①) and 48 bit (for 2).

Then 48 bit result in S-box.

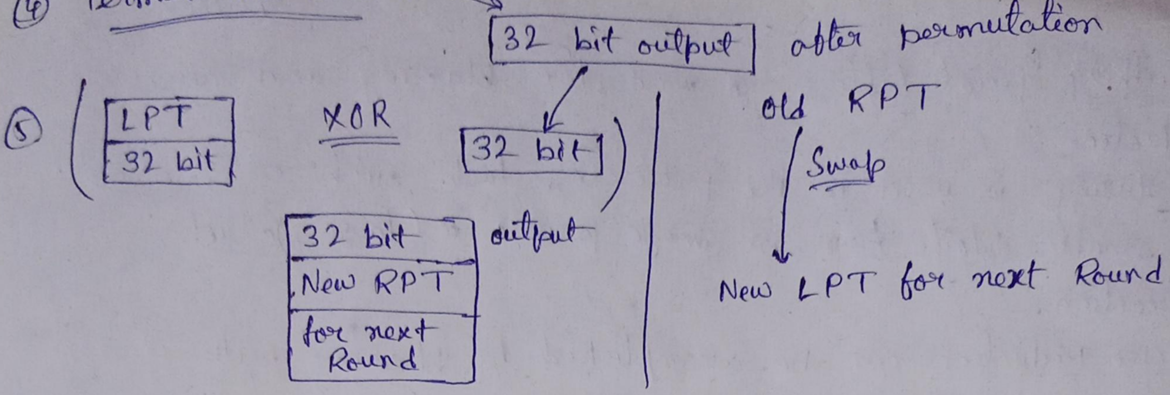
Final output 32 bit from S-box

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

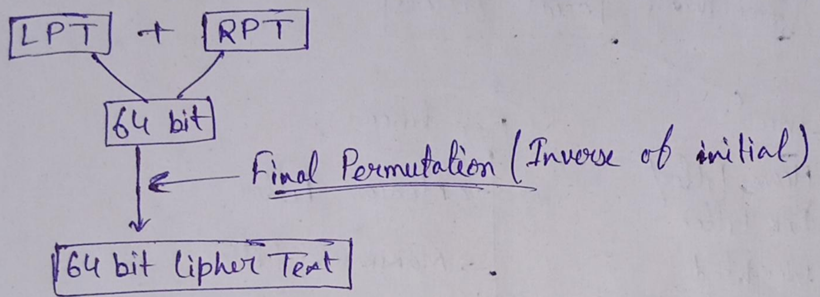
16 Col.
4 rows



④ Permutation Box :



## After 16 pounds



## 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.

## Weekness / Disadvantage of DES

(i) Parallel Processing in < 2 min –

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

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

(iii) 6 sems — week keys

(iv) 48 possible week keys

(v) 2 diff. plain Text ⟶ Same Cipher

(vi) 2 diff. keys ⟶ same Cipher Text