# 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 :-

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)

Man in the middle Attacks

## Cryptography :—

The art / science of achieving security through encryption

method to convert plain text to cipher text

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

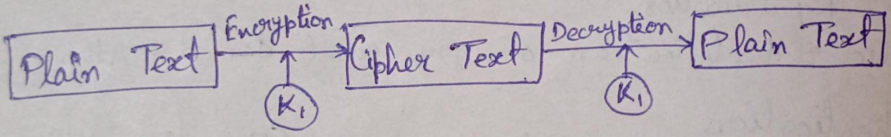
### Key

① Symmetric key cryptography (Private key cryptography)

② Asymmetric key cryptography (public key cryptography)

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

① Symmetric key

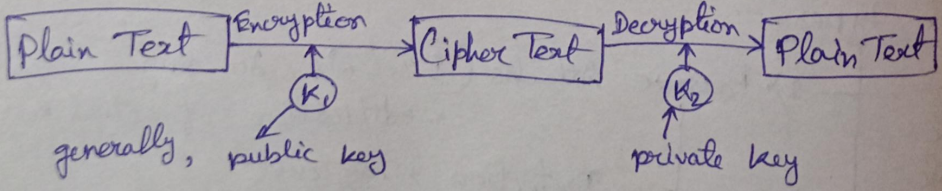



- One of algorithm

(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

| C | B | A | S | E | R |
|---|---|---|---|---|---|
| +3 ↓ | +3 ↓ | +3 ↓ | +3 ↓ | +3 ↓ | +3 ↓ |
| F | H | D | V | H | U |

Poly

H E Y  THERE
+ + +  + + + +
J G  X A Y

Example:

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: → Encryption

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

C → Cipher
26 → no. of Alphabet

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

Crypto

Sem - 6

31/1/2025

# Data Encryption Standard (DES):

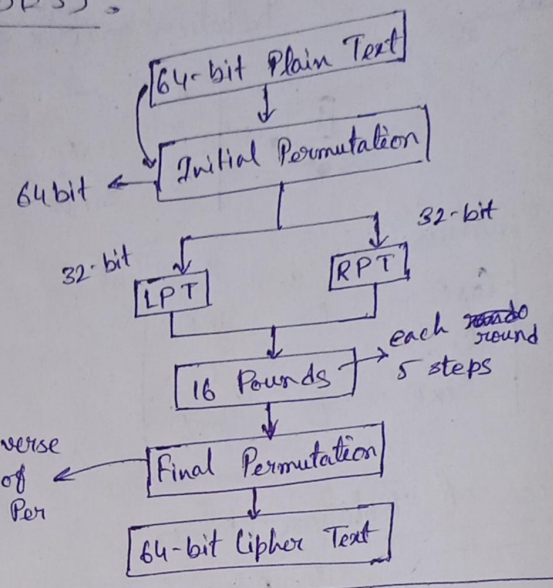
64-bit Plain Text

Key (56 bit) → DES

64-bit Cipher Text

every 8th bit discarded

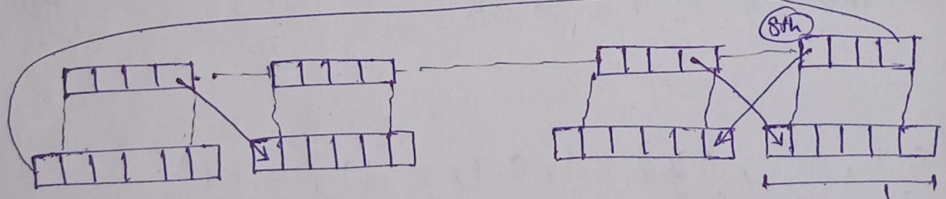
64 → 56




## 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 

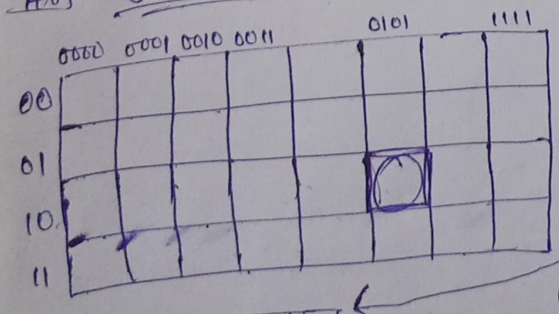

③ Substitution Box:

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

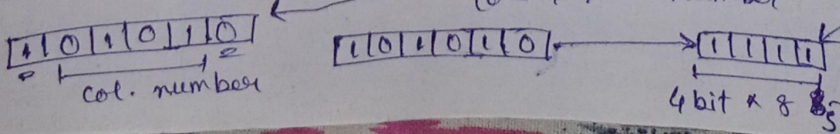
8 S-box, 64-bit, matrix / array




16 Col.

4 rows

values (0-15) → 4 bit, 1111



④ Permutation Box :→ 32 bit output after permutation

⑤ ( LPT 32 bit ) XOR ( 32 bit ) → 32 bit output for next Round

Old RPT → Swap → New LPT for next Round

After 16 pounds

LPT + RPT → 64 bit ← Final Permutation (Inverse of initial) → 64 bit Cipher Text

## 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 semi — weak keys

(iv) 48 possible weak keys

(v) 2 diff. plain Text → Same Cipher

(vi) 2 diff. keys → same Cipher Text

Cryptography

7/2/2025

## (*) 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 → $K_1 = B^x \bmod n$.

7. Bob → $K_2 = A^y \bmod n$.

Example:

1. $n = 7$, $g = 11$ | let, $x = 3$, $y = 6$
2. Alice → $A = 7^3 \bmod 7$ $= 2$
3. Alice → 2 → Bob
4. Bob → $B = 7^6 \bmod 11 = 4$
5. Bob → 4 → Alice
6. $K_1 = 4^3 \bmod 11 = 9$
7. $K_2 = 2^6 \bmod 11 = 9$ ✓

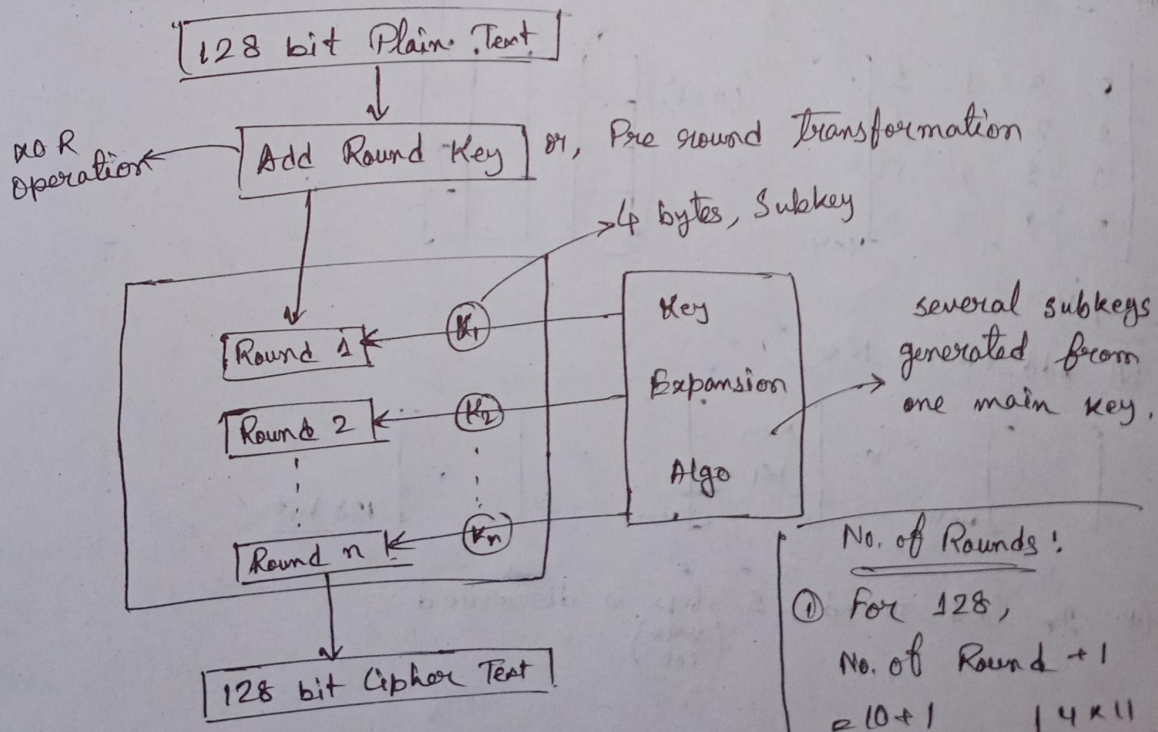
(+) Advanced Encryption Standard (AES):

2000
Rijndael
2001

128 bit, plain Text → 128 bits Cipher Text

| Rounds | Length of Key | |
|---|---|---|
| 10 | 128 bits | AES-128 |
| 12 | 192 bits | AES-192 |
| 14 | 256 bits | AES-256 |

(++)




No. of Rounds:

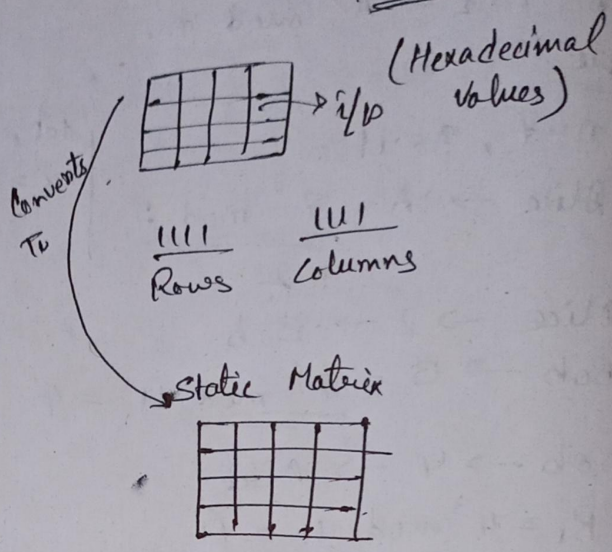
① For 128,
No. of Round + 1
= 10 + 1
= 11 subkeys
[0 to 10]

4 × 11
44 bytes subkeys

## Steps:

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

4 words




### Step 1

ABS ⟶ S-box

16×16

### Step 2 Shift Rows

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

i/p

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

4×1

(4×4) States Matrix

### Mix Columns:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}_{4\times4} \times \begin{bmatrix} & \\ & \\ & \\ & \end{bmatrix}_{4\times4} \rightarrow (4\times1)$$

### Step 4

### Add Round Key

$$\begin{bmatrix} \quad \end{bmatrix}_{4\times4} \times \begin{bmatrix} \text{Key} \\ \text{K1} \end{bmatrix}_{4\times1} = \begin{bmatrix} \quad \end{bmatrix}_{128\text{ bit}}$$

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

# Cryptography

Date: 14/2/2025

1) Encrypt the following plain text using ceaser cipher:

Plain Text: ~~All the Best~~ ALL THE BEST

Key: 4

2) Encrypt the plain text "HOW ARE YOU" using key "NCBTQZARG" by the substitution technique called Vernam Cipher.

3) Transform the below mentioned plaintext into cipher text using the key "COLLEGE" by using play fair cipher.

Plain Text: STUDENTS ARE PLAYING FOOTBALL

## Answers

1) Encryption:

E(A) + K = 4 ⟶ E

E(L) + K = 4 ⟶ P

E(T) + K = 4 ⟶ X

E(H) + K = 4 ⟶ L

E(E) + K ⟶ I

E(B) + K ⟶ F

E(S) + K ⟶ W

∴ Cipher Text = EPP XLI FIWX

2) A → D.

| | | |
|---|---|---|
| 7 14 22 | 0 17 4 | 24 14 20 |
| H O W | A R E | Y O U |
| N C B | T Q Z | A R G |
| 13 2 1 | 19 16 25 | 0 17 6 |
| 20 16 23 | 19 33 29 | 24 31 26 |
| U Q X | T H D | Y F A |

33%26=7 29%26=3 31%26=5 26%26=0

3)

COLLEGE

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

STUDENTS ARE PLAYING FOOTBALL

CT: TU SH ET UT BQ G N CD VN PE BB RB BD D2 LD XL