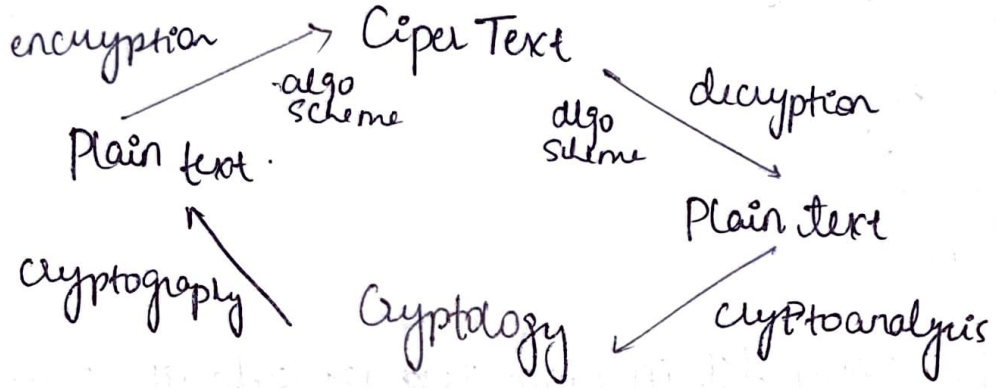
Unit I: Classical Encryption techniques. Symmetric cipher model.

- **Plain text**: It is the original message sent by the user.
- **Cipher text**: It is a coded message

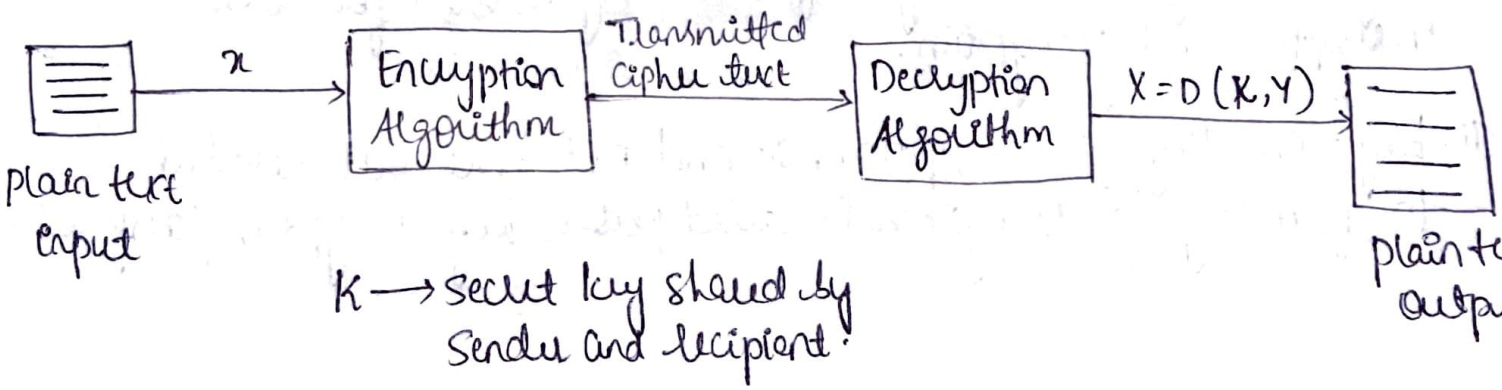
Method/process of converting plain text to cipher text is Encryption and vice-versa is decryption, ie restoring the plain text from cipher text
Area that includes studying and understanding algorithm and schemes of encryption is cryptography and of decryption is cryptanalysis.

Cryptology : cryptography + cryptoanalysis

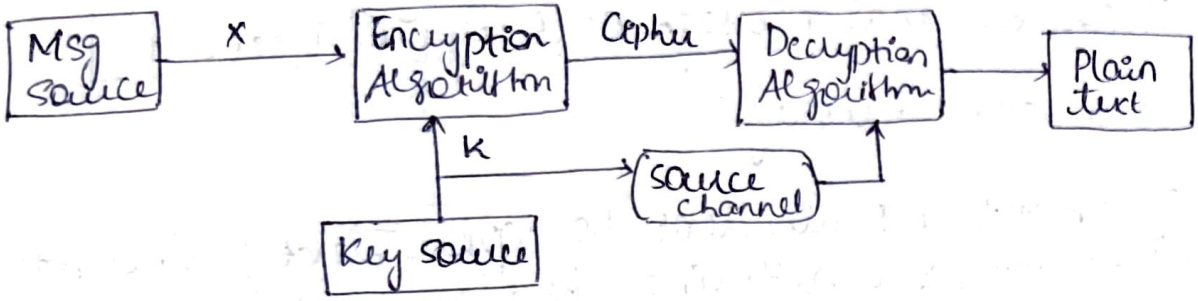


- **Symmetric cipher model**

There are five components
1. plain text
2. Ciphe text
3. Encryption Algorithm
4. Decryption algorithm
5. Key / Secret key / Symmetric key



- Essential elements of symmetric encryption scheme



$X = [X_1, X_2, X_3, X_n]$ plain text can be a word or an sentence.
Key Source: generates key K and send it through secure channel.

- Characteristic of cryptography

① Type of operation:
There are two types
- Substitution
- Transposition

- Substitution : For every bit in plain text we subscribe some other value or letter.
  Eg: abc ⟶ xyz

- Transposition: No new values is substituted, the letters are interchanged or position of letter is changed.
  Eg: abc → bca or cba

② The number of keys used secret key algorithm/connection

(i) Key algo/symmetric algo: If same key is used for both encryption and decryption.

(ii) Key: one key for encryption, second not same but related to first key for decryption is called public key encryption/asymmetric

③ The way in which plain text is processed, two types

(i) Block cipher: plain text is divided into block of some bits and each block is converted into cipher text.

(ii) Stream cipher: plain text is processed bitwise

- How do we attack cryptography system? 2 ways.

① Deduce the key

② Directly deduce plain text

- Types of attacks

① Cryptanalysis [5 types]

(i) Cipher text only

(ii) Known plain text: attacker knows algorithm, cipher text.
- attacker knows algorithm, cipher text, plain text - cipher text pair.

(iii) Chosen plain text: attacker knows algo, cipher text, a pair of plain text and cipher text from set of PT CT pair

(iv) Chosen cipher text
(v) Chosen text
} not used in real world nowadays.

- Unconditionally secure system
- Computationally secure system.

- Substitution techniques

① Caesar Cipher: Given the plain text, every bit is substituted with next alphabet. Next is determined by key

Eg: abc k = 3

cipher text ⟶ def

a - z ⟶ 1 - 26

$Y = E(k, x)$

$Y = (x+k) \bmod 26$

to get plain text back

$X = (Y-k) \bmod 26$

Cipher text for HI HOW ARE YOU for $k = 3$

H → 8

$Y = (8+3) \bmod 26$

$= 11 \bmod 26$

$= 11$

$= K$

I → 9

$Y = (9+3) \bmod 26$

$= (12) \bmod 26$

$= 12$

$= L$

O → 15

$Y = (15+3) \bmod 26$

$= 18 \bmod 26$

$= 18$

$= R$

W → 263

$Y = (23+3) \bmod 26$

$= 26 \bmod 26$

$= 0$

$= Z$

A → 1

$Y = (1+3) \bmod 26$

$= 4 \bmod 26$

$= 4$

$= D$

R → 18

$Y = (18+3) \bmod 26$

$= 21 \bmod 26$

$= 21$

$= U$

E → 5

$Y = (5+3) \bmod 26$

$= 8 \bmod 26$

$= 8$

$= H$

Y → 25

$Y = (25+3) \bmod 26$

$= 28 \bmod 26$

$= 2$

$= B$

HI HOW ARE YOU ⟶ KL KRZDVHBRX.

② Monoalphabetic Cipher : Some random alphabet is substituted to letter, some particular letter is substituted to particular letter.

③ Play fair Cipher (Rules for encryption)

- Draw a 5×5 matrix and construct the matrix by filling the letters of a keyword (eliminating the duplicates) from left to right and from top to bottom
- Fill the remaining boxes of the matrix with the remaining letters of english alphabets in the order.
- The letters i and j count as a single letter.
- Plain text is divided in block of two bits and if it is not possible then add X at the end.
- Repeating plain-text letters are in the same pair, are separated with the filler letter such as X.

  Eg: HELLO
  ↳ HE LX LO

- If two letters fall in the same row of the matrix then they are separated / replaced by the letter to its right.
- If both letters fall in the same column then each letter is replaced by the letter beneath it.
- If both the letters fall on different row and different column then the letters are replaced by the letters that lies in its own row and the column occupied by the other plain text.

• Example 1 : key → SECURITY
PT → COMPUTER.

PT COMPUTER

CT : UNNLEACS

- Example 2 : key → OCCURRENCE
  CT → ZCHENVU2

CT : ZCHENVU2
PT : WELCOMEX.

(4) Hill Cipher

- Key is in the form of matrix, either 2x2 or 3x3
- Plain text is divided as a matrix, for 2x2 (—)1x2 and for 3x3 (—)1x3.
- $P_m \longrightarrow C_m \Rightarrow \quad C = P \cdot k \bmod 26$
  $P = Ck^{-1} \bmod 26.$
- $k^{-1} = \frac{1}{|k|} Adj(k)$

- Example (1)

PT : HELP Key : $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Encryption

P_1 = HE [7 4]

$C_1 = P_1 k \bmod 26$

$= [7\ 4] \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$= [21+8 \quad 21+20]$

$= [29 \quad 41] \bmod 26$

$= [3 \quad 15]$

DP

P_2 = LP [11 15]

$C_2 = P_2 k \bmod 26$

$= [11\ 15] \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$= [33+30 \quad 33+75] \bmod 26$

$= [63 \quad 108] \bmod 26$

$= [11 \quad 4]$

LE

Decryption

$P = CK^{-1} \bmod 26$

$K^{-1} = \frac{1}{|K|} Adj(K)$

$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$|K| = [15 \quad -6] = 9$

$Adj(K) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$

{ Trial and error method:
$9x = 1 \bmod 26$
Remainder should be 1 }

$ax = b \bmod n$

$9x = 1 \bmod 26.$

q	n	a	r	t_1	t_2	t
2	26	9	8	0	1	-2
1	9	8	1	1	-2	3
8	8	1	0	-2	3	-26
	1	0		3	-26	

$t = t_1 - (t_2 \times 2)$

$K^{-1} = (3) \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$ add 26 to negative values.

$K^{-1} = 3 \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \bmod 26.$

$K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

$P = CK^{-1} \bmod 26$

$C_1 = [3 \quad 15]$

$P_1 = C_1 K^{-1} \bmod 26$

$= [3 \; 15] \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \bmod 26.$

$= [45 + 300 \quad 51 + 135] \bmod 26$

$= [345 \quad 186] \bmod 26 \quad = [7 \quad 4]$ HE.

$C_2 = [11 \quad 4]$

$P_2 = C_2 K^{-1} \bmod 26$

$= [11 \quad 4] \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \bmod 26$

$= [165+80 \quad 187+36] \bmod 26$

$= [245 \quad 223] \bmod 26$

$= [11 \quad 15]$

$= LP$

- Example ②

$Key = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$ PT = SCHOOL

Encryption

$P_1 = SC \quad [18 \quad 2]$

$C_1 = P_1 K \bmod 26$

$= [18 \quad 2] \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} \bmod 26$

$= [90+34 \quad 144+6] \bmod 26$

$= [124 \quad 150] \bmod 26$

$= [20 \quad 20]$

U U.

$P_2 = HO \quad [7 \quad 14]$

$C_2 = P_2 K \bmod 26$

$C_2 = [7 \quad 14] \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$

$= [35+238 \quad 56+42]$

$= [273 \quad 98] \bmod 26$

$= [13 \quad 20]$

N U

$P_3 = OH \quad [14 \quad 11]$

$C_3 = P_3 K \bmod 26 = [14 \quad 11] \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} \bmod 26$

$= [70+187 \quad 112+33] \bmod 26$

$= [257 \quad 145] \bmod 26$

$= [23 \quad 15]$

X P.

CT : UUNUXP.

Decryption

$P = CK^{-1} \bmod 26$

$K^{-1} = \frac{1}{|K|} Adj(K)$

$|K| = [15 - 136]$

$|a| = -121$

$|K| = 9$

$Adj(K) = \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix}$

$\frac{1}{|K|} = 3$

$K^{-1} = \begin{bmatrix} 9 & 54 \\ 27 & 15 \end{bmatrix} \bmod 26$

$K^{-1} = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix}.$

q	r	a	s	t_1	t_2	t
2	26	9	8	0	1	-2
1	9	8	1	1	-2	3
8	8	1	0	-7	3	-26
	1	0		[3]	-2	

$K^{-1} = \frac{1}{|K|} Adj(K)$

$K^{-1} = 3 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} = 3 \begin{bmatrix} 3 & 18 \\ 9 & 5 \end{bmatrix}$

$P_1 = C_1 K^{-1} \bmod 26$

$= (20\ 20) \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} \bmod 26$

$= (200\ \ 340) \bmod 26$

$= (18\ \ 2)$

SC

$P_2 = C_2 K^{-1} \bmod 26$

$= (13\ 20) \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \bmod 26$

$= (137\ \ 326) \bmod 26$

$= [7\ \ 14]$

HO

$P_3 = C_3 K^{-1} \bmod 26$

$= [23\ \ 15] \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \bmod 26$

$= [222\ \ 271] \bmod 26$

$= [14\ \ 11]$

OL

- **3x3 Encryption**

1) $K = \begin{bmatrix} 17 & 7 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ P = Pay more money

$P_1 = (15 \quad 0 \quad 24)$

$C_1 = P_1 K \bmod 26$

$(15 \quad 0 \quad 24) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26.$

$= [303 \quad 303 \quad 531] \bmod 26$

$= [17 \quad 17 \quad 11)$

R R L

$P_2 = MOR = [12 \quad 14 \quad 17]$

$C_1 = P_2 K \bmod 26$

$= [12 \quad 14 \quad 17] \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$

$= [532 \quad 490 \quad 677] \bmod 26$

$= [12 \quad 22 \quad 1]$

M W B.

$P_3 = EMO = [4 \quad 12 \quad 14]$

$C_3 = P_3 K \bmod 26$

$$= [4 \quad 12 \quad 14] \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$$= [348 \quad 312 \quad 538]$$

$$= 10 \quad 0 \quad 18$$
$$\text{IC} \quad A \quad S$$

$P_4 = NEY = (13 \quad 4 \quad 24)$

$C_4 = P_4 K \bmod 26$

$$= [13 \quad 4 \quad 24] \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$$= [353 \quad 341 \quad 605] \bmod 26$$

$$= 15 \quad 3 \quad 7$$
$$P \quad H \quad H.$$

Pay More Money $\rightarrow$ RRL MWBK ASPDH

Decryption

$|K| = 17(300) - 939 \bmod 26$

$= 23.$

$\frac{1}{|K|} = 23x = 1 \bmod 26 = 17.$

$$\text{Cofactor}(k) = \begin{bmatrix} +300 & -357 & +6 \\ -313 & +313 & -0 \\ +267 & -252 & +51 \end{bmatrix}$$

$$Adj(k) = \begin{bmatrix} 300 & -313 & +267 \\ -357 & 313 & -252 \\ +6 & 0 & -51 \end{bmatrix}$$

$$Adj(k) = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$k^{-1} = 17 \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix}$$

$$k^{-1} = \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$C_1 = RRL\ [17\ 17\ 11]$

$P_1 = Ck^{-1} \bmod 26$

$$= [17\ 17\ 11] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$$= [587\ 442\ 544] \bmod 26$$

$$= [15\ 0\ 24]$$

PAY

$C_2 = MWB\ [12\ 22\ 1]$

$= MWB = [12\ 22\ 1) \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$

$C = [10\ 0\ 18] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$

$= [472\ 90\ 456] \bmod 26$

$= [4\ 12\ 14]$

E M O

$C_4 = PDH = [15\ 3\ 7]$

$= [15\ 3\ 7] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 19 \end{bmatrix} \bmod 26$

$= [273\ 186\ 362] \bmod 26$

$= [13\ 4\ 24]$

N E Y.

RRLMWBKASPDH → PAY MORE MONEY.

⑤ Polyalphabetic cipher

① Vigenere cipher - Here the length of keyword must be less than or equal to length of the plain text.

- Keyword (n), plain text (m):
  - $n \leq m$ is accepted
  - $n \geq m$ is not accepted.

- Whenever the length of keyword is less than the plain text then it is made equal by repeating the keyword.

- Example ①

Key → deceptive
plain text → we are discovered save yourself.

DECEPTIVEDECEPTIVEDECEPTIVE
WEAREDISCOVEREDSAVEYOURSELF

D → 3
W → 22
25 [Z]

E → 4
E → 4
8 [I]

C → 2
A → 0
2 [C]

E → 4
R → 17
21 [V]

P → 15
E → 4
19 [T]

T → 19
D → 3
22 [W]

I → 8
I → 8
16 [Q]

V → 21
S → 18
39 mod 26
13 [N]

E → 4
C → 2
6 [G]

D → 3
O → 14
17 [R]

E → 4
V → 21
25 [Z]

C → 2
E → 4
6 [G]

E → 4
R → 17
21 [V]

P → 15
E → 4
19 [T]

T → 19
D → 3
22 [W]

I → 8
S → 18
26 → [A]

V → 21
A → 0
21 [V]

E → 4
V → 21
25 [Z]

D → 3
E → 4
7 [H]

E → 4
Y → 24
28 → 2 [C]

C → 2
O → 14
16 [Q]

E → 4
U → 20
24 [Y]

P → 15
R → 17
6 [G]

T → 19
S → 18
11 [L]

I → 8
E → 4
12 [M]

V → 21
L → 11
6 [G]

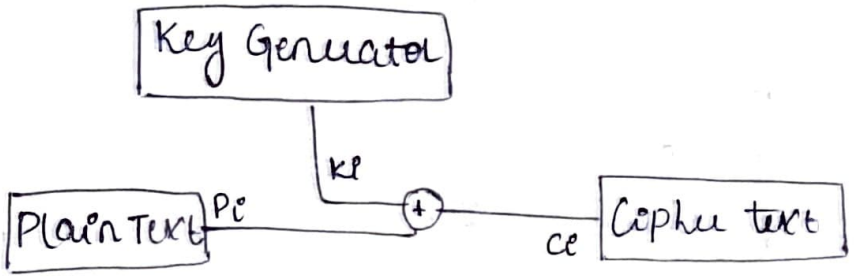
E → 4
F → 5
9 [J]

ZICVTWQNGR ZG VTW A VZ HCQYGLMGJ

- Auto key system We append the plain text till the key would becomes equal to the plain text.

② Vernam Cipher

- It deals with binary data [plain text]
- Keyword is randomly generated.



- One time pad : extension of Vernam cipher to provide more security.
- A key is generated and is used to encrypt a single message and it is then discarded. Same key is not used again.
- In practical it is not used because generation of key is difficult.

- ~~Transposition~~

- Transposition technique [Columnar cipher]

① Rail Fence cipher

Step 1 : Write two letters in diagonal form.
Step 2 : To get the cipher, read it row wise.

Example ① PT → meet me in the evening

Step 1 : m e e t m e i n t h e e v e n i n g

Step 2 : memetevnnetenheeeg.

② Single Encryption

Step 1 : Write the key in a row
Step 2 : Fill the letters of PT with some number of the columns as the keyword.
Step 3 : If there are any blank space then fill them with the last alphabets (X Y Z).
Step 4 : To get the cipher text we consider columns wrt to key value. lowest number first.

- Example Key → 4 3 1 2 5 6 7
  PT → attack postponed until two am.

Key →	4	3	1	2	5	6	7
	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.

CT → ttnaaptmtsuoaodwcoix knlypetz.

② Double transposition

- Here CT obtained from the single encryption/transposition is used as plain text.

key →	4	3	1	2	5	6	7
	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	c	t	z

CT → nscyauoptwltmdnaoicpaxttokz

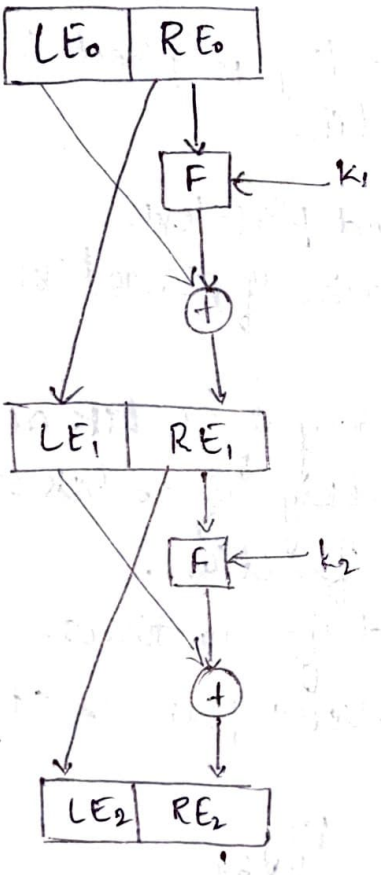
• Feistel Cipher

- Uses concepts of block cipher
- It has plain text of n bits and key of k bits.
- Makes use of both substitution and transposition techniques repeatedly.
- Two key features

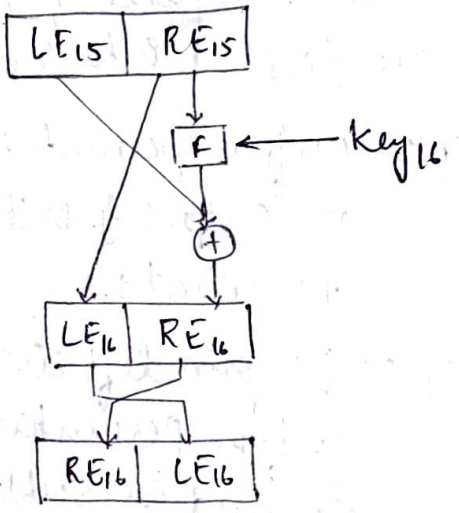
① Confusion: } A cipher text should be
② Defusion: } so strong that the cryptanalyst should not be able to deduce the key.

Substitution technique: Confusion, Transposition technique: Defusion.

Logic: Encryption



for n = 16.



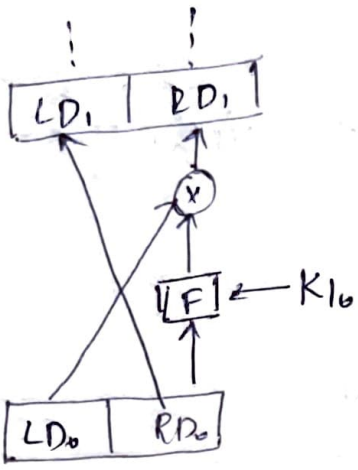
Step1: divide the PT into 2 halves
Step2: add round function to right part.
Step3: add key to the round function
Step4: XOR the output with left part and place it as the next right.

Encryption is top down approach.

F: round function

The encryption has to be carried out for n rounds.
Generally we take n = 16.

Decryption



after 16 rounds left and right parts are swapped.

$LD_0 = RE_{16}$

$RD_0 = LE_{16}$.

- This is bottom up approach.

Step 1: Round function is added to right part then key 16 (last key is) is attached.

Step 2: Resulting output is XOR with left part and is placed as right.

- **Data Encryption Standard (DES)**

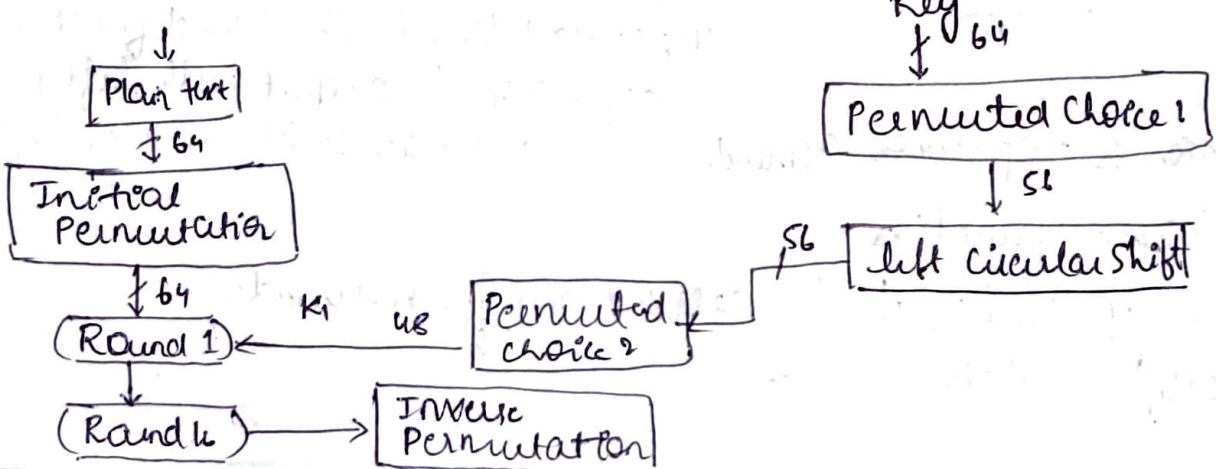
- Here the length/size of plain text and key is fixed ie 64 bits.
- Keys are divided into subkeys of 48 bit.

Step 1: perform permutation for key and plain text.
The output of initial permutation of plain text is given to round 1.

Step 2: Perform left circular shift to key of 56 bits and again perform permutation to get subkey of 48 bits which will be used as subkey to round function.

Step 3: The above steps are performed for 16 times.

Step 4: After 16th round perform inverse permutation to get the cipher text.



- Design principles

① Number of rounds : More the number of rounds, more secure the system will be, but it is time consuming.
Standard no of rounds : 16

② Design of function F:
→ SAC : Strict avalanche criteria
→ BIC : bit independent criteria

③ Scheduling of subkey