Unit - I

☆ Key terms:-

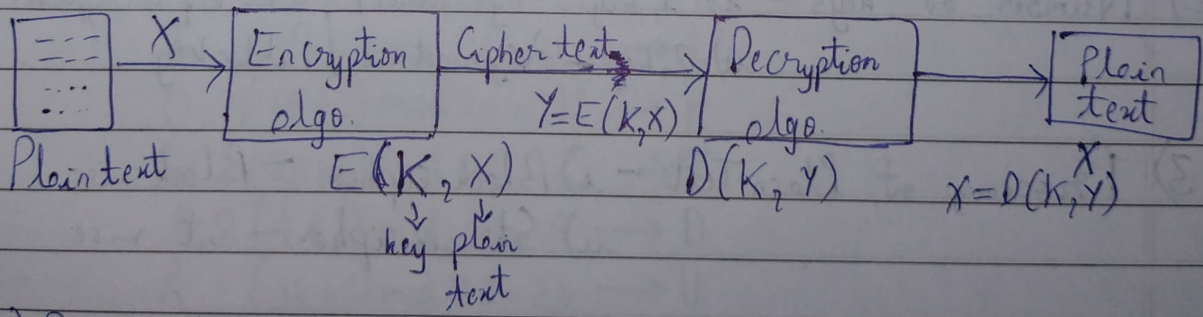
1) Plain text – Original message.
2) Ciphered text – Converted " (Coded message).
3) Encryption – Converting plain text to cipher text.
4) Decryption – Converting cipher text to plain text.
5) Cryptography } together Cryptology
6) Cryptanalysis }

☆ Cipher Models:-

1) Symmetric – Use same key for enc./decr.
2) Asymmetric – " diff. " for enc. & decr.

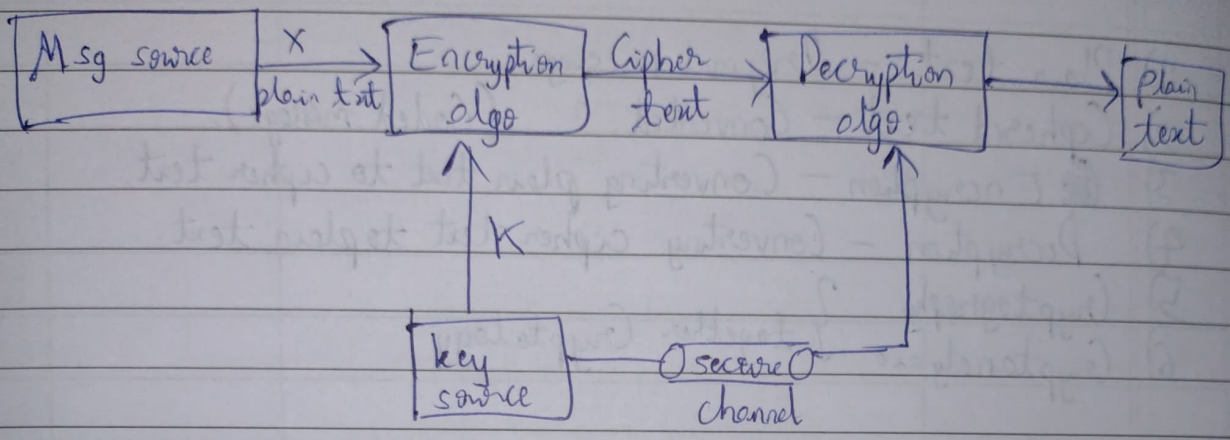
☆ Symmetric Cipher Model:-

Has 5 key components.



1) Plain text
2) Cipher text
3) Encryption algo.
4) Decryption algo.
5) Key / symmetric key / secret key

For the secure comm. to actually take place:
1) Use strong algo.
2) Sending key through secure channel.



☆ Characteristics Of Cryptographic System:-

1) Type Of Operation — i) Substitution } To convert plain to cipher
ii) Transposition

i) Substitute original message characters with diff. characters. Ex: abc → xyz
ii) No new chars used, just change order. Ex: abc → bac or bca

2) Number of keys — i) 1 key — Symmetric / Secret key encryption.
ii) 2 keys — Asymmetric / Public key "

3) Processing of Plain Text — i) Block cipher — Block wise
ii) Stream cipher — Bit wise

☆ Attacking the system:-

1) Cryptanalysis — Attacker knows about encryption algo.
2) Brute Force attack — Trial & error.

There are 5 types in Cryptanalysis:
i) Cipher text only — Attacker knows only cipher text.
ii) Known plain text — Attacker knows algo + cipher + plain & cipher text pairs.

iii) Chosen plain text – Attacker knows algo. + Cipher + select one pair of known cipher text – plain text pairs & deduce key
iv) Chosen cipher text.
v) Chosen text.

☆ Substitution Techniques:-

1) Caesar Cipher – Every bit substituted by next k^{th} letter.

Ex: abc
↓↓↓ k=3
def

P.T. C.T.
X Y

$Y = E(K, X)$
$Y = (X + K) \bmod 26$
$X = (Y - K) \bmod 26$

Ex: HI HOW ARE YOU
8 9 8 15 23 1 18 5 25 15 21 with k=3, show mathematical calc. for HI.

→ For H: $(8+3) \bmod 26 = 11 \rightarrow K$
I: $(9+3) \bmod 26 = 12 \rightarrow L$
O: $(15+3) \bmod 26 = 18 \rightarrow R$
W: $(23+3) \bmod 26 = 0 \rightarrow Z$
A: $(1+3) \bmod 26 = 4 \rightarrow D$
R: $(18+3) \bmod 26 = 21 \rightarrow U$
E: $(5+3) \bmod 26 = 8 \rightarrow H$
Y: $(25+3) \bmod 26 = 2 \rightarrow B$
U: $(21+3) \bmod 26 = 24 \rightarrow X$

Encoded message: KL KRZ DUH BRX

2) Monoalphabetic Cipher:-

[S] P.T. a b c d ... z
C.T. s v x e .... [R]

abc ⟶ svx

26! keys.

3) Play Fair Cipher:-

Rules for encryption:

1) Draw a 5X5 matrix & construct the matrix by filling the letters of the keyword (omitting duplicates) from left to right & from top to bottom.
2) Fill the remaining boxes of the matrix with the remaining letters of the english alphabet in order. Letters I & J count as a single letter (I/J).
3) Plain text is divided into blocks of 2 bits & if its not possible, add X at the end.
4) Repeating plain text letters that are in same pair are separated with a filler letter such as X. Ex. HELLO is HE LX LO
5) If 2 letters fall in same row of matrix, then they're replaced by the letter to its right.
6) If the 2 letters fall in same column of matrix, then each letter is replaced by the letter beneath it.
7) If both letters fall in different row & different column, then the letters are replaced by the letter that lies in its own row & the column occupied by the other plain text letter.

Rules for decryption:-

1) For same row, replace with left letter.
2) " " col, " " above "
3) Diff. row, diff. col. rule same as encryption.

Ex: i) Key : SECURITY
P.T. : COMPUTER

→

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

CO MP UT ER
UN NL EA CS

C.T. : UNNLEACS

ii) Key : OCCURRENCE
P.T. : ZCHENVUZ

→

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

ZC HE NV UZ
WE LC OM EX

P.T. : WELCOMEX or WELCOME

4) Hill Cipher :-

Key is in the form of a square matrix (2X2 or 3X3).
P.T. is divided in the form of matrix, depends on key.

$C = P \cdot K \bmod 26$

Numbering starts at 0 (A→0, Z→25)

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

Ex:

1) $P = HELP$

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

i) Encryption:

$C = P \cdot K \bmod 26$

$P_1 = [H \quad E] = [7 \quad 4]$

$P_2 = [L \quad P] = [11 \quad 15]$

$C_1 = P_1 \cdot K \bmod 26$

$$= [7 \quad 4] \times \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \bmod 26$$

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

$= [3 \quad 15]$

$= [D \quad P]$

$C_1 = DP$

$C_2 = P_2 \cdot K \bmod 26$

$$= [11 \quad 15] \times \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \bmod 26$$

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

$= [11 \quad 4]$

$= [L \quad E]$

$C_2 = LE$

$\therefore$ C.T. $= DPLE$

ii) Decryption:

$P = C \cdot K^{-2} \bmod 26$

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

$|K| = 9$

$adj(K) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$ $\quad \therefore \frac{1}{|K|} = 3$ $\quad (9 \times x = 1 \bmod 26)$ ↘ $1/|K|$

$\therefore K^{-1} = \begin{bmatrix} 5/9 & -3/9 \\ -2/9 & 3/9 \end{bmatrix} \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix}$

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

$K^{-1} = 3 \times \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = 3 \times \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} = \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \bmod 26$

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

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

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

$= [345 \quad 186] \bmod 26$

$= [7 \quad 4]$

$= [H \quad E]$

$P_1 = HE$

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

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

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

$= [11 \quad 15]$

$= [L \quad P]$

$P_2 = LP$ $\quad \therefore P.T. = HELP$

2) $K = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$

P.T. = SCHOOL

→ $P_1 = SC$, $P_2 = HO$, $P_3 = OL$ | $P_1 = [18 \quad 2]$, $P_2 = [7 \quad 14]$, $P_3 = [14 \quad 11]$

$C_1 = P_1 K \bmod 26$

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

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

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

$= [20 \quad 20]$

$= [U \quad U]$

$C_1 = UU$

$C_2 = P_2 K \bmod 26$

$= [7 \quad 14] \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} \bmod 26$

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

$= [13 \quad 20]$

$C_2 = NU$

$C_3 = P_3 K \bmod 26$

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

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

$= [23 \quad 15]$

$C_3 = XP$

$C = UUNUXP$

$|K| = -121 \bmod 26 = \underline{9}$

q	a	b	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	

$\therefore 9^{-1} \bmod 26 = \underline{3}$

$\therefore (\det K)^{-1} = \underline{3}$

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

$$\therefore K^{-1} = (\det K)^{-1} \cdot \text{adj}(K)$$

$$= 3 \cdot \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & -24 \\ -51 & 15 \end{bmatrix} \bmod 26$$

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

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

$= [20 \quad 20] \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \bmod 26 = [200 \quad 340] \bmod 26 = [18 \quad 2]$

$P_1 = \underline{SC}$

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

$= [13 \quad 20] \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \bmod 26 = [137 \quad 326] \bmod 26 = [7 \quad 14]$

$P_2 = \underline{HO}$

$P_3 = C_3 \cdot K^{-1} \bmod 26 = [23 \quad 15] \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \bmod 26 = [222 \quad 271] \bmod 26 = [14 \quad 11]$

$P_3 = \underline{OL}$ $\qquad P = P_1 P_2 P_3 = \underline{SCHOOL}$

$= [14 \quad 11]$

3X3 encryption:-

1) $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$, P = paymoremoney

→ P_1 = pay = $[15 \quad 0 \quad 24]$

$C_1 = P_1 \cdot K \bmod 26$

$= [15 \quad 0 \quad 24] \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$

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

$= [17 \quad 17 \quad 11]$

$C_1 = \underline{RRL}$

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

$C_2 = P_2 \cdot K \bmod 26$

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

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

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

$C_2 = \underline{MWB}$

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

$C_3 = P_3 \cdot K \bmod 26$

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

$= [348 \quad 312 \quad 538] \bmod 26$

$= [10 \quad 0 \quad 18]$

$C_3 = \underline{KAS}$

$P_4 = \text{key} = [13 \quad 4 \quad 24]$

$C_4 = P_4 \cdot K \bmod 26$

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

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

$$= [15 \quad 3 \quad 7]$$

$C_4 = \underline{\underline{PDH}}$

$C = RRLMWBKASPDH$

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

$|K| = -939 \bmod 26 = \underline{\underline{23}}$

q	a	b	r	t_1	t_2	t ($t = t_1 - qt_2$)
1	26	23	3	0	1	−1
7	23	3	2	1	−1	8
1	3	2	1	−1	8	−9
2	2	1	0	8	−9	26
	1	0		−9	26	

$-9 + 26 = \underline{\underline{17}}$

$(\det K)^{-1} = \underline{\underline{17}}$

Matrix of cofactors of $K = \begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & -0 \\ 267 & -252 & -51 \end{bmatrix}$

$$\text{adj}(K) = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} = \begin{bmatrix} 300 & 25 & 267 \\ 7 & 313 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$\text{adj}(K) \bmod 26 = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$\therefore K^{-1} = 17 \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix} \bmod 26$$

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

Decryption:

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

$$= [17 \ 17 \ 11] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26 = [587 \ 442 \ 544] \bmod 26$$

$$= [15 \ 0 \ 24] = \text{pay}$$

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

$$= [12 \ 22 \ 7] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26 = [402 \ 482 \ 329] \bmod 26$$

$$= [12 \ 14 \ 17] = \text{mor}$$

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

$$= [10 \ 0 \ 18] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26 = [472 \ 90 \ 456] \bmod 26$$

$$= [4 \ 12 \ 14] = \text{emo}$$

$P_4 = C_4 \cdot K^{-1} \bmod 26$

$$= [15 \ 3 \ 7] \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26 = [273 \ 186 \ 362] \bmod 26$$

$$= [13 \ 4 \ 24] = \text{ney}$$

$P = \text{paymoremoney}$

☆ Polyalphabetic Cipher:-

1) Vigenere Cipher:-

→ keyword (length n)
→ plain text (" m)

Condition $n \leq m$.

Example:-
i) key → deceptive
P.T. → we are discovered save yourself. (discard spaces)
→ len(P.T.) = 27
len(key) = 9
key → deceptivedeceptivedeceptive
P.T. → wearediscoveredsaveyourself

deceptive → 3 4 2 4 15 19 8 21 4
we → 22 4
are → 0 17 4
discovered → 3 8 18 2 14 21 4 17 4 3
save → 18 0 21 4
yourself → 24 14 20 17 18 4 11 5

Cipher text :-
we → zi
are → ecvt
discovered → wqngrzgvtw
save → svzh
yourself → cqyglngj

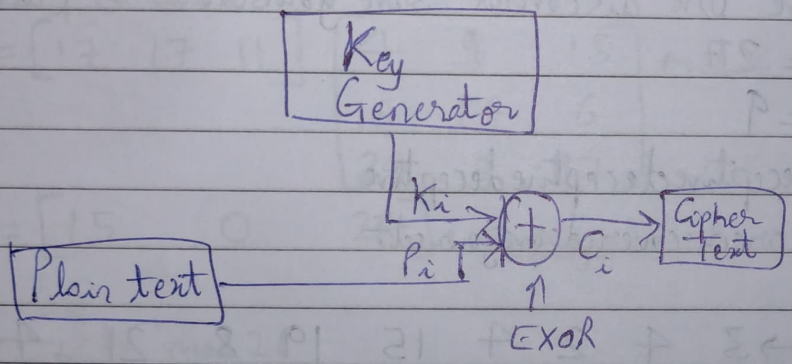
* Autokey system :- (Part of vigenere)

Don't repeat key to equalize length.
Instead attach plain text.

Ex: for previous example, key = deceptivewearediscoveredsav

2) Vernam Cipher :-

→ P.T. in the form of binary data.
→ key is randomly generated.



* One timepad :-

Discard key K_i after encrypting P_i.

* Transposition Techniques (also called Columnar Cipher) :-

1) Rail Fence Cipher :-

Ex: P.T → meet me in the evening
No key.

m e m i t e v n n
e t e n h e e i g

⇓

C.T. → memitevnnetenheeig

* Single encryption & Double encryption:-

Ex:

P.T. → attack postponed until two am

Key → 4 3 1 2 5 6 7

Soln.

Key → 4 3 1 2 5 6 7

P.T. → a t t a c k p

o s t p o n e ⇒ C.T. → ttnaaptmtsuoaodw

d u n t i l t coixknlypetz

w o a m x y z

fillers to complete row

Col.1 Col.2

C.T. is obtained columnwise

Above ex. is single transposition.

Double transposition:-

Take C.T. of First transposition as P.T. in second transposition, use same key.

Ex:

key → 4 3 1 2 5 6 7

P.T. → t t n a a p t

m t s o u a o ⇒ C.T. → nscyaaoptttwltmdn

d w c o i x k aauiepaxttokz

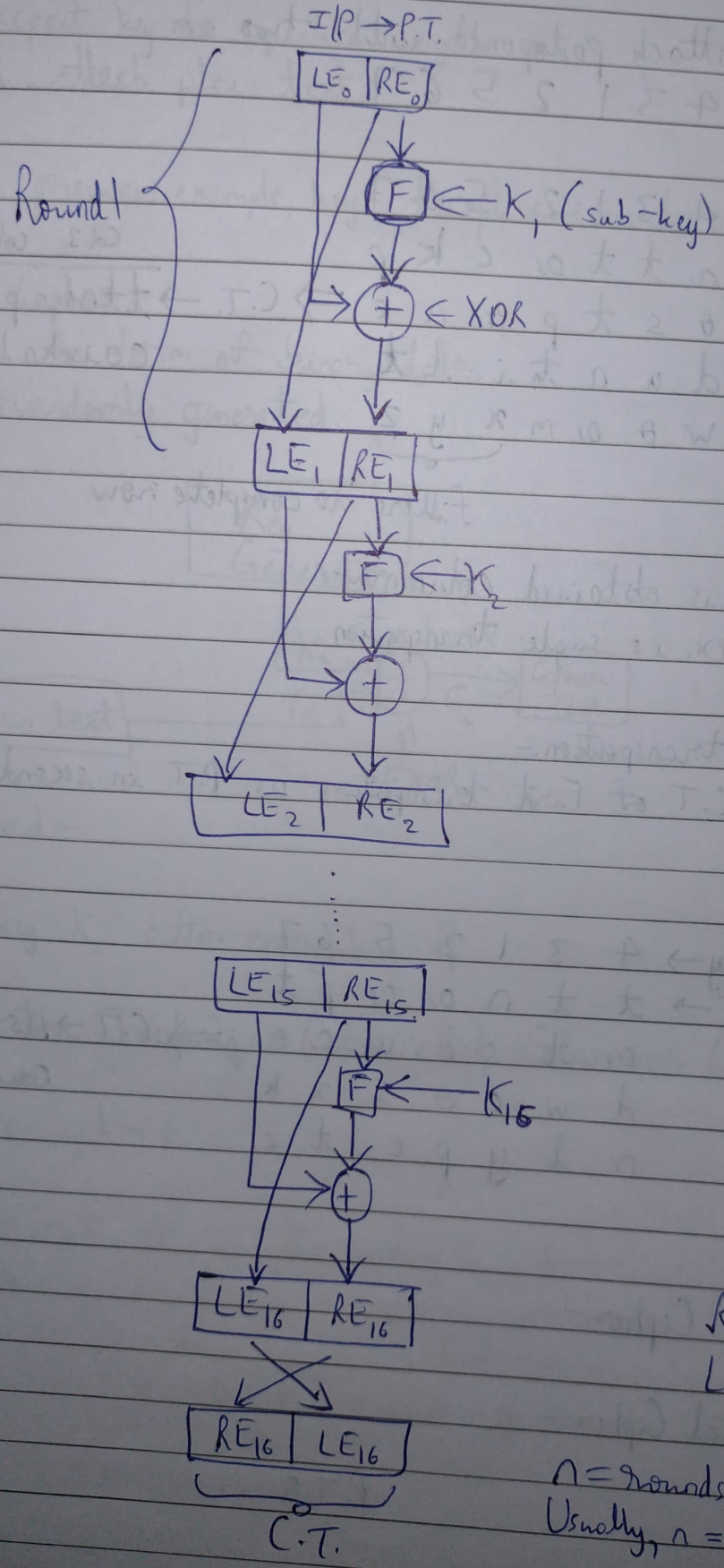
n l y p e t z

* Block Cipher:-

* Feistal Cipher:-

P.T.O.

K → key
F → Round fn.



RE - Right of encryption.
LE - left " "

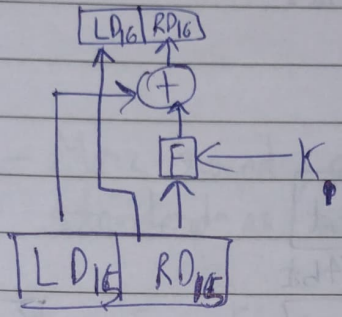
n = rounds
Usually, n = 16

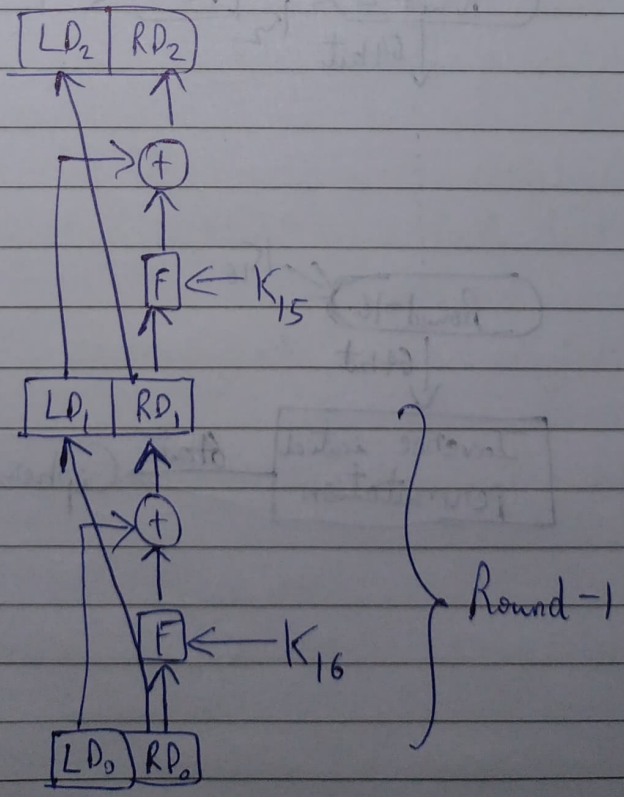
Encryption (Top down approach)
Decryption (Bottom up approach)

RD – right of decryption
LD – left " "

$LD_0 = RE_{16}$, $RD_0 = LE_{16}$

P.T. = $RD_{16} | LD_{16}$



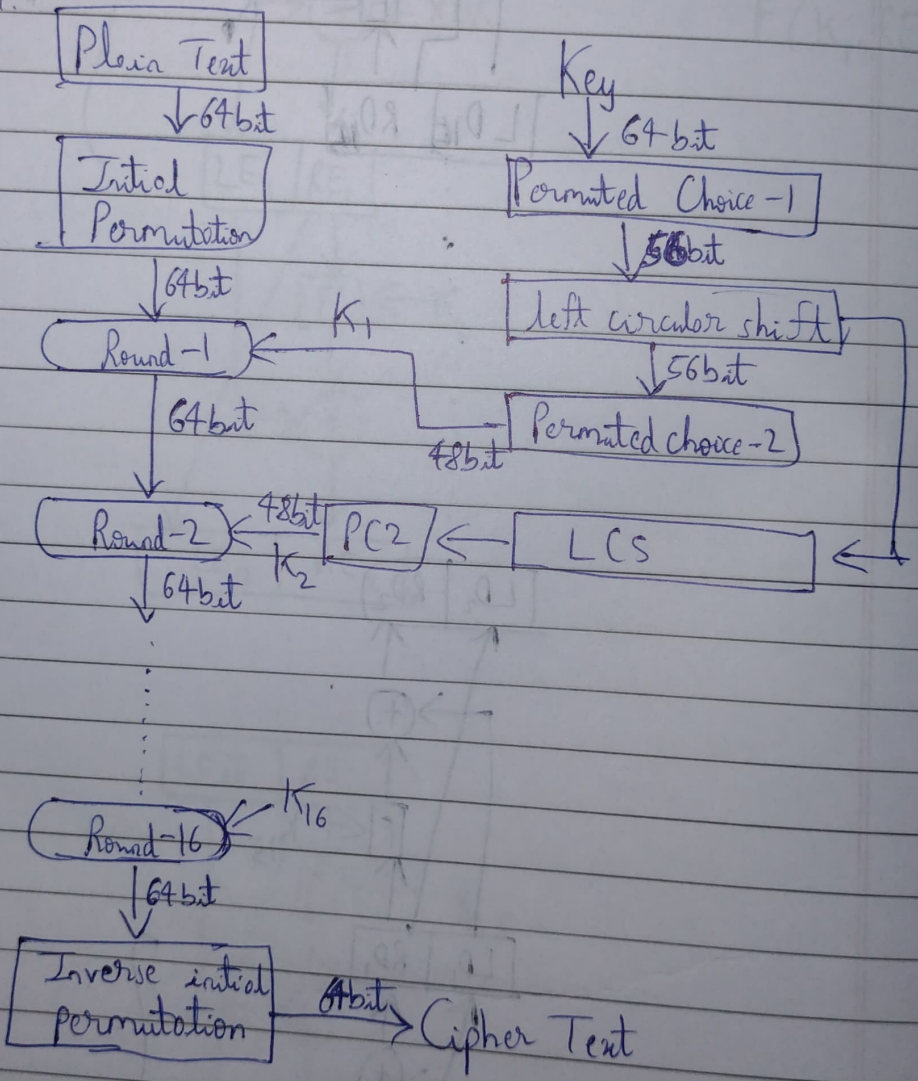


☆ Data Encryption Standard (DES):-

→ P.T. → 64bits (fixed length)
→ key → 64bits
→ subkeys used → 48bits

* Encryption:-

I/P → P.T.



✳ Decryption:-

Reverse from round 16 with key 16 to round 1 with key 1 & then inverse permutation.

✡ Design Principles:-

1) No. of rounds – More rounds, stronger C.T., but more time consuming
standard no. of rounds = 16

2) Design of function F – Should be non-linear in nature & should have strong Avalanche effect.
⟹ SAC (strict avalanche criteria).
⟹ BIC (bit independent criteria).

3) Sub-key (Key scheduling algorithm)