Date / / Saathi

① ② ③ Single
④ ⑤ Multi

SUBSTUTION. TECH

① CAESER CIPHER. (P)

② MONO ALPHABETIC CIPHER. (P).

③ POLYALPHABETIC CIPHER:
- (i) VERMAN
- (ii) VIGINER (P) → Normal and Auto Key

④ PLAYFAIR CIPHER (P)

\+ ⑤ HILL CIPHER (P)

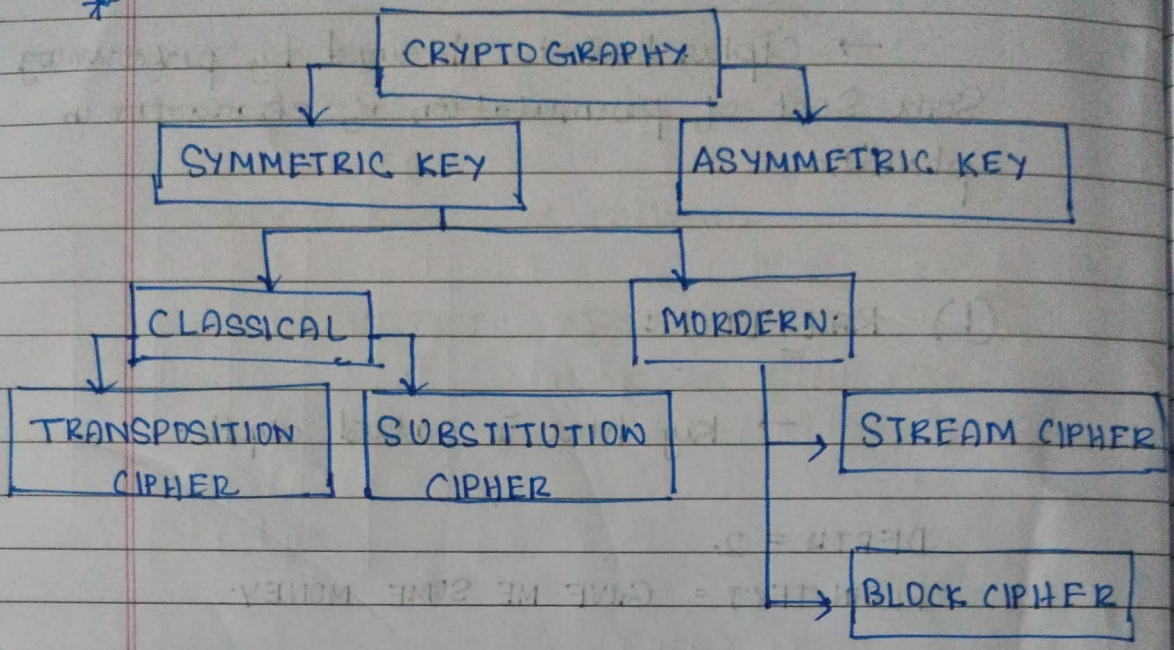
\+ ⑧ ONE TIME PAD ← K

TRANSPOSITION. TECH

① RAIL FENCE (P)

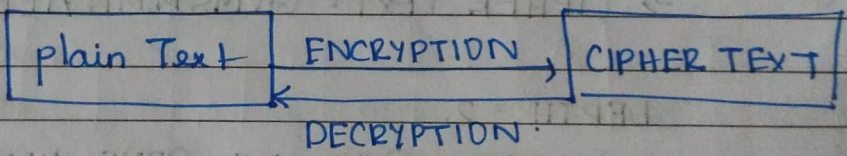
② ROW COLUMN (P).

CRYPTOGRAPHY



* plain Text ⇒ Original message.

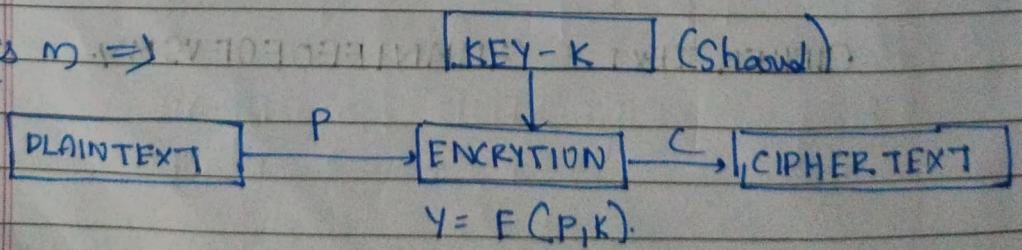
* cipher Text ⇒ coded / modified / encrypted message.

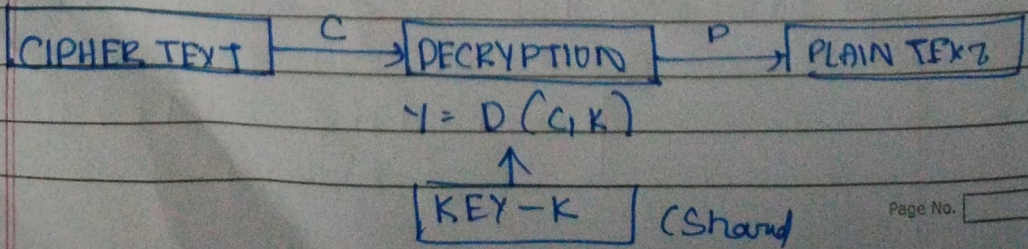


⇒ SYMMETRIC CIPHER MODEL / SYMMETRIC CRYPTOG.

→ Both Sender and Reciver Share a Secret Key.

Mechanism ⇒





Date ___/___/_____

Saathi

* TRANPOSITION TECHNIQUE:

→ Ciphur text is obtained by performing Some Sort of permutation of character in plaintext.

(i) RAILFENCE:

→ Key here is called depth.

DEPTH = 2.
PLAIN TEXT = GIVE ME SOME MONEY.

G V M S M M N Y
I E E O E O E

⇒ CIPHER TEXT = GVMSMMNYIEEOEOE.

DEPTH = 2.
PLAINTEXT = GIVE ME SOME MONEY.

G M M N
I E E O E O E
V S M Y

CIPHER TEXT = GMMNIEEOEOEVSMY.

(ii) ROW-COLUMN:

→ plain text written row by row
→ & Read column by column.

KEY ⇒ order of column.

Eg: PLAINTEXT: ~~[illegible]~~
GIVE ME SOME MONEY AS SOON AS POSSIBLE

1	2	3	4	5
G	I	V	E	M
E	S	O	M	E
M	O	N	E	Y
A	S	S	O	O
N	A	S	P	O
S	S	I	B	L
E	A	B	C	D

KEY: 4 3 1 2 5

⇒ CIPHER TEXT: EMEOPBCVONSSIB GEMANSF ISOSASAMEYOOLD.

→ This cipher text can again be fedded into the above matrix an. can be encrypted again ⇒ increase complexity

Date ___/___/_____

Saathi

Main types of Symmetric Encryption are

① Substitution Cipher } Classic Methods
② Transposition Cipher.

* SUBSTUTION TECHNIQUE:

→ Letters of plaintext are replaced by some other Letters.

↓
Substitute by ciphertext value

(i) CAESER CIPHER:

→ Shifts character in a plaintext by K. character

i.e

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

M	N	O	P	Q	R	S	T	U	V	W	X
12	13	14	15	16	17	18	19	20	21	22	23

Y	Z
24	25

Eg: AFTER K=3 ⇒ DIWHU
K=1 ⇒ BGUFS

⇒ Encryption Function: = ~~C(P,K) = (P+K) mod 26~~

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

Page No. ____

Date __/__/____

→ Shifting back by K characters will give the plaintext

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

→ Only 25 possible key values (1 - 25)
i.e Key Space is very small So easy to Brute Force.

(ii) MONO ALPHABETIC CIPHER:

→ increases the key space dramatically when compared to ceaser cipher (25 to 26!).

→ achieved by using permutation of characters (A - Z)

↓

N! Permutations for N char's

i.e

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

Eg: AFTER ⇒ DIXHV

⇒ can be cracked by analysing the frequency of characters in cipher text (by comparing to Standard Character frequency)

Date __/__/____

(iii) PLAYFAIR CIPHER:

→ multi-letter encryption cipher.
→ uses a 5×5 matrix of letter constructed using a key word

KEY = "MONARCHY"

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

→ 1st Fill key, Repeat letter should be Skipped, the fill remaining with A-Z. again repeats should be Skipped.

Encryption Steps: (group letter as pair).

① if repeating letter in plaintext Separate them with 'x' ⇒ i.e both same in pair

Eg: BALLOON ⇒ BALXLOON
BA LX LO ON.

② if Both letters in a pair are in same row/col each letter will be replaced by next character in cyclic manner

Eg: OR ⇒ NM , MN ⇒ OA (Same row)
OF ⇒ HP , GW ⇒ QN (Same col)

③ otherwise replace by same row and column of other letter.
Eg: EW ⇒ GV , FX ⇒ IV / JV.

Page No.

→ The pair of letters in the plain text is called **digrams**

→ Used during World War I and II

Eg: KEY = "TONYSTARK"

PLAINTEXT = "ENCRYPTION"

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

EN CR YP TI ON

FO AK BX AU NY

⇒ **CIPHER TEXT = "FOAKBX AUNY"**

(IV) HILL CIPHER:

→ Also a multi letter cipher.

→ Key used here will be a Square matrix of Size M×M.

Eg: ATTACK = plain text, K = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

⇒ Take M characters from plain text.

Date __/__/____

Saathi

ATT = [0, 19, 19]

$$\Rightarrow \begin{bmatrix} 0 & 19 & 19 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \text{ mod } 26$$

$$\Rightarrow \begin{bmatrix} 0\times17 + 19\times21 + 19\times2, & 0\times17 + 19\times18 + 19\times2, & 0\times5 + 19\times21 + 19\times19 \end{bmatrix}$$

$$\begin{bmatrix} 437 & 380 & 760 \end{bmatrix} \text{ mod } 26$$

$$\Rightarrow \begin{bmatrix} 21 & 16 & 6 \end{bmatrix} \Rightarrow \boxed{ATT = VQG}$$

ACK = [0 2 10]

$$\Rightarrow \begin{bmatrix} 0 & 2 & 10 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 0\times17 + 2\times21 + 10\times2, & 0\times17 + 2\times18 + 10\times2, & 0\times5 + 2\times21 + 10\times19 \end{bmatrix}$$

$$= \begin{bmatrix} 62 & 56 & 232 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 10 & 4 & 24 \end{bmatrix} \Rightarrow \boxed{ACK = KEY}$$

$$\Rightarrow \boxed{\text{CIPHER TEXT} = VQGKEY}$$

⇒ Decryption is done by computing inverse of K

[LEARN THIS]

Page No.

⇒ If key matrix is N×N then we can encrypt N characters at a time

$$[C_1\ C_2\ C_3] = [P_1\ P_2\ P_3] \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \% 26$$

$$\Rightarrow \boxed{C = PK \bmod 26}$$

→ Can use fillers character 'x' if ends not use Size

DECRIPTION ⇒ $C \times K^{-1} \bmod 26$

$$\boxed{K^{-1} = \frac{1}{|K|} \text{Adj } K.}$$ (matrix Inverse)

$$\Rightarrow \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$= 17(18\times19 - 2\times21) - 17(21\times19 - 2\times21) + 5(21\times2 - 2\times18)$

$= 5100 - 6069 + 30$

$= -939 \Longrightarrow -939 \bmod 26$

$= -3 \bmod 26 \Rightarrow 23$

$$\boxed{|K| = 23}$$

Date __/__/____

Saathi

① Find determinant of K.

$|K| = |K| \bmod 26$.

mod 26 for both Step

if $|K| < 0 \Rightarrow$ divide $|K|$ by 26 and write - Remainder
(and ≥ 26)
↳ else Just add

② Find adjoint.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \Rightarrow \begin{bmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 18\times19 - 2\times21 & 2\times5 - 17\times19 & 17\times21 - 18\times5 \\ 21\times2 - 19\times21 & 19\times17 - 5\times2 & 5\times21 - 21\times17 \\ 21\times2 - 2\times18 & 2\times17 - 17\times2 & 17\times18 - 21\times17 \end{bmatrix}$$

$$\begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \quad \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \bmod 26$$

$$\text{Adj } K = \begin{bmatrix} 14 & 25 & 7 \\ 19 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

Page No.

Saathi

Date ___/___/_____

$\Rightarrow |K| = 23$ ✓ $\quad ADJ(K) = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$ ✓

⇒ NUMBER THEORY NEEDED BADLY :(

(v). POLYALPHABETIC CIPHER (VIGINER CIPHER):

→ Single letter cipher.
→ uses several cipher principal

Eg:

KEY = "ATTACK"
PLAIN TEXT = "GIVE MONEY"

P.T	G	I	V	E	M	O	N	E	Y	
K	A	T	T	A	C	K	A	T	T	

Enc

P.T	6	8	21	4	12	14	13	4	24	
KEY	0	19	19	0	2	10	0	19	19	
C.T	6	1	14	4	14	24	13	22	17	

⇒ CIPHER TEXT = GIBOE ■OYNWR.

Dec.

C.T	6	1	14	4	14	24	13	22	17	
K	0	19	19	0	2	10	0	19	19	
P.T	6	8	21	4	12	14	13	4	24	

Page No. ____

→ Auto Key Systems : Having the Same Key repeated can be illuminable. So after 1st occurance of Key concat plain text of Sub

i.e KEY = ATTACK ⟶ ATTACK GIV

PLAINTEXT = GIVEMONEY

(vi) POLYALPHABETIC CIPHER (VERNAM CIPHER):

→ works using binary Bits
→ Key as long as plain text (Very long but Repeating after Some point)

$C_i = P_i \oplus K_i$

(XOR)

$P_i = C_i \oplus K_i$

(vii) ONE-TIME PAD CIPHER: