

⇒ *ਕੋਈ ਮਿਲੀਅਰ ਰੁਪਏ / ਕਾਨੂੰਨ ਦੇ ਵਿਖੇ ਵੀ ਸੁਣਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।*

\* Cryptography is a method of protecting information and communications using codes.

\* Cipher text:



Encrypted text

transformed from plain text,

plain text

Any readable data

\* Classical encryption technique —②

(i) Substitution, (ii) Transposition.

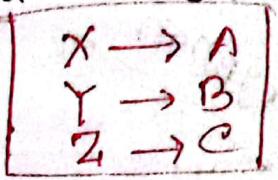
- Caesar
- Monoalphabetic
- Playfair
- Hill
- Polyalphabetic
- One-Time Pad

- Rail Fence
- Row column
- Transposition.

\* .

## 4108 (Cryptography)

01.  $\frac{1}{2}$  Caesar Cipher.  $\rightarrow$  3 places further down the alphabet

↳ This technique involves shifting the results letters of the alphabet by a fixed number of places. For example, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E'. 

↳ Used it for secure communication.

↳ The fixed number of position is called 'shift' or 'key'.

→ number of possible shift for the English alphabet is 26 limited (25 different shifts).

36  
37 mod 26  
11  
Encryption phase with shift n

$$E_n(x) = (x+n) \text{ mod } 26$$

— Decryption phase with shift n

$$D_n(x) = (x-n) \text{ mod } 26$$

↳ e.g. ciphertext.

Plaintext | Plain text  
↓  
Encrypted text  
↳ ciphertext  
 $P = \text{GEEKS}$   
 $E_n = (P+k) \text{ mod } 26$   
 $= (G+3) \text{ mod } 26$   
 $= 9 \text{ mod } 26$   
 $= 9$   
= J

02.  $\frac{1}{2}$  Monoalphabetic cipher

↳ It is a part of the substitution technique in which a single cipher alphabet is per message. (Mapping is done from plain alphabet to cipher alphabet).

↳ It converts plain text into cipher text and re-converts cipher text into plain text.

↳ Eliminates brute force technique.

## 03. Brute Force Attack cipher

→ A brute force attack is a cryptographic technique used to decipher encrypted data by exhaustively trying all possible keys until one is found.

Encryption

Shift 0 : amina

Shift 1 : bnjob

Shift 2 : cokpc

Shift 3 : dplqd

Shift 4 : eqmre

Shift 5 : frnsf

Shift 6 : gsotg

Shift 7 :

Decryption

Correct encryption - ①

Shift 1 ② decryption ③  
shift 0.

Shift 0 : bnjob

Shift 1 : amina ④ Target -  
Shift 2 : zlhmz Letter

gmlt - ⑤ )

&lt;p

## Monoalphabetic

Q W E R . . . . M  
A B C D - - - - Z,  
O 1 2 3 - - - - 25

Plaintext:

①

ABCD → plaintext



QWER → ciphertext.

②

A, B, C, D, - - - - Z.

key = ICE, plaintext = Amina

Amor

A B C D E F G H I J K L M N O P &  
I C E A B D F G H J K L M N O P Q  
R S T

Plain: Amina

Cipher: IMHNI

U V W X T

2

## Hill cipher

→ 2x2 or 3x3 matrix into cipher.

2x2  
matrix } Plaintext = hill  
key = sh

### Encryption

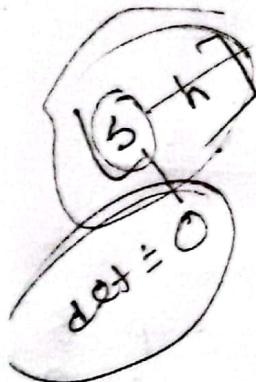
$$C = PK \bmod 26$$

$$= \begin{bmatrix} h & i \\ i & h \end{bmatrix} \begin{bmatrix} 3 & h \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 203 \\ 215 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 \\ 6 \end{bmatrix}$$

$$= \begin{bmatrix} g \end{bmatrix}$$



$2^3$

$\begin{matrix} 5 & 9 & 8 \\ 6 \end{matrix}$

$$\frac{203}{26}$$

$$= 7.807$$

$$\in 7.81$$

$$7.81 \times 26$$

$$= 21.06$$

### Decryption

$$\text{Plaintext} = C K^{-1} \bmod 26$$

Ciphertext  
Key

# Playfair

5x5

→ Repeat step  
2nd row

Encrypt

a	s	u	m	o	n
c	b	d	i/j	k	
f	g	h	r	t	
l	p	q	y	z	
v	w	x			

Input text = amina

key = sumona

P = amina  
am in ax

P = amina

am    in    ax  
C = es ko cv

P = amina

C = esko cv

Decrypt

Repeating  
am in ax

am in ax

C = esko cv  
am in ax

column wise read

es ko cv

m

l

o

ml  
e.g.: lo

Row wise read

es ko cv

Row 2

es ko cv

Row 3

es ko cv

Row 4

es ko cv

Row 5

es ko cv

Row 6

es ko cv

Row 7

es ko cv

Row 8

es ko cv

Row 9

es ko cv

Row 10

es ko cv

m

l

o

es ko cv

s → l  
p → r

## Poly-Alphabetic

Plaintext = sumon @  
key = amna

$$\text{Encrypt: } (P+K) \bmod 26$$

$$= 18 + 0 \bmod 26$$

$$= 18 \bmod 26$$

$$= 18$$

9

$$(20 + 12) \bmod 26$$

$$= 32 \bmod 26$$

$$= 6$$

$$= g$$

$$= -$$

Decryption  $\rightarrow$  sumon

0	1	2	3	4	5	6
a	b	c	d	e	f	g

$$\begin{aligned} 0 + 0 &\bmod 26 \\ &= 0 \\ &= a \end{aligned}$$

## Vernam cipher

a -	b	c	-	.	.	z
0	1	2	-	-	-	25

key's length = ~~not~~ plain text length.

- \* Bitwise x-or both the numbers
- \* Subtract the number from 26 if the number  $\geq 26$
- \* If it's not then leave it.

### Encrypt

Plaintext : O A K

key : S O N

$$\begin{array}{r} 26 \\ 12 \\ \hline 14 \end{array}$$

Plain $\rightarrow$	14	0	10
key $\rightarrow$	18	14	13
(P+K)	32	14	23
	6	14	23

$\rightarrow \geq 26 - 26 \text{ (NET)} (25 \text{ or } 26)$   
 $12 (28) 23 (27)$

Cipher : G O X

### Decryption

cipher $\rightarrow$	6	14	23
key $\rightarrow$	18	14	13
(@-K)	-12	0	10
	14	0	10

Negative value  
 $12 (25) 26 (25)$

plain  $\rightarrow$  OAK