Chapter 4th

Caesar cipher:

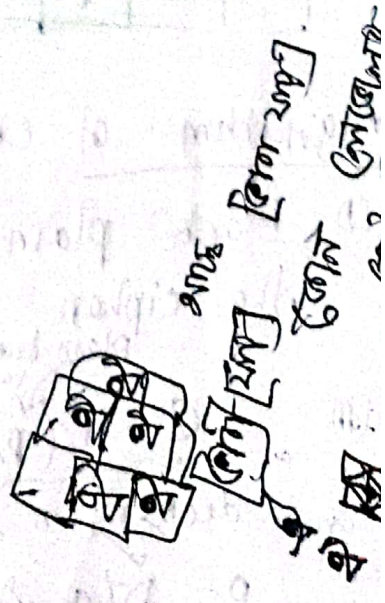
The earliest known and the simplest use of a substitution cipher was by only Julius cipher.

The Caesar cipher involves to replacing each letter of the alphabet with the letter standing three places further down the alphabet.

→ Classical encryption techniques has two different part:

(i) Substitution techniques
(ii) Transposition techniques.

Substitution technique	Transposition technique
Caesar cipher	
(i) Caesar cipher	(i) Rail Fence
(ii) Mono alphabatic	(ii) Raw Column.
(iii) Playfair cipher.	
(iv) Hill cipher	
(v) Poly alphabetic	
(vi) One time pad.	



letters are replaced by

Caesar cipher:

(i) Caesar cipher has follows as letters are replaced by other letter or symbol.

(ii) The earliest known and simplest method used be julius caesar. Julius

(iii) Replacing each plain text letter of the alphabet with the letter standing three places further down the alphabet.

Example: Example:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

C = F(P,K) mod 2

Algorithm of cipher text

(i) Each plain text letter 'P' is substitute by the cipher text letter 'C'.

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

(Plain text input; key information)

and decryption =>

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

For example:

My name IS nasan

Plain text: m y n a m e i s n a y a n

Ciper text: p b q d p h l v q d b d q

Ciper text algorithm

for, m,

$C = E(p+k) \bmod 26$

$= (12+3) \bmod 26$

$= 15 \bmod 26$

$= 15$

12 + 3

for, y.

$C = (p+k) \bmod 26$

$= (24+3) \bmod 26$

$= 27 \bmod 26$

$= 1$

mod 26

follow this algorithm and find out the Caesar ciper text for this plain text.

Plain text: my name IS nasan

ciphen text: pbqdphlvqdbdq.

Monoalphabetic cipher:

With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the keys can be achieved by allowing substitution techniques.

→ Now, The 'cipher' line can be any permutation of the 26 alphabetic characters.

A permutation of a finite set of elements 'S' is is an ordered sequences of all the elements of 'S' with element appearing exactly once.

For example,

$S = \{a, b, c\}$

Permutation, = 3!

= abc
= acb
= bac
= bca
= cab
= cba

Encryption →

$C_i = (P + k) \bmod 26$

$= (13 + 3) \bmod 26$

Naam

$(13 + 3) \bmod 26$

= 16 mod 26

= P

(4) Playfair cipher:

The best known multiple letter encryption cipher is the playfair which treats diagram in the plaintext as single units and translates these unit into ciphon text.

The playfair algorithm is based on 5×5 matrix of letters constructed using keywords

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

Rules for encryption using playfair:

(i) Digrams
(ii) Repeating letters - filler letter
(iii) Same column |↓| Wrap around
(iv) Same row → Warp around
(v) Rectangle |⇄| Swap

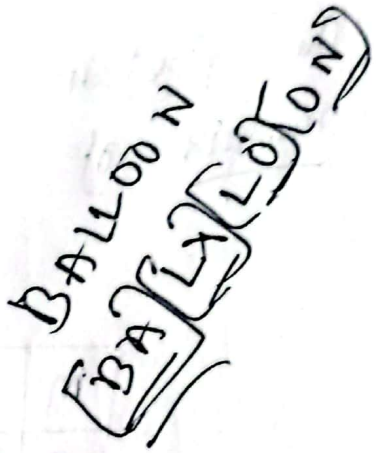
The playfair cipher is a great advance over simple monoalphabetic letter that lies its own kind ciphers.

For one things, whereas there are only 26 letters there are 26 * 26

Plain text : attack

Digram at ta ck

Plain text : balloon

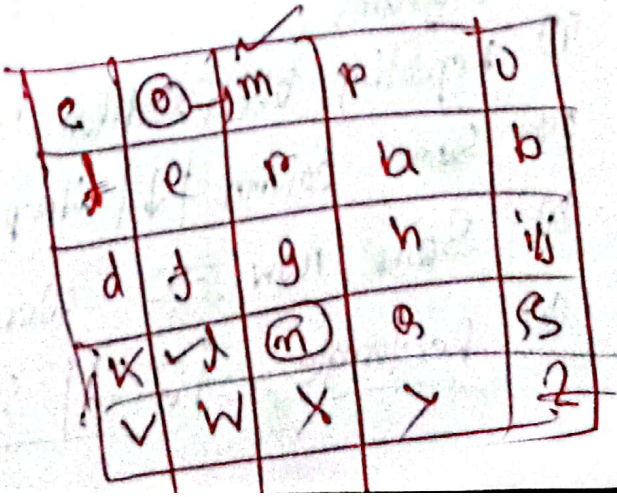


cipher → ba ll oo n

filler letter

→ ba lx lo on

Description of playfair



attack

at	ta	ck
RS	SR	DE

Plain: at ta ck

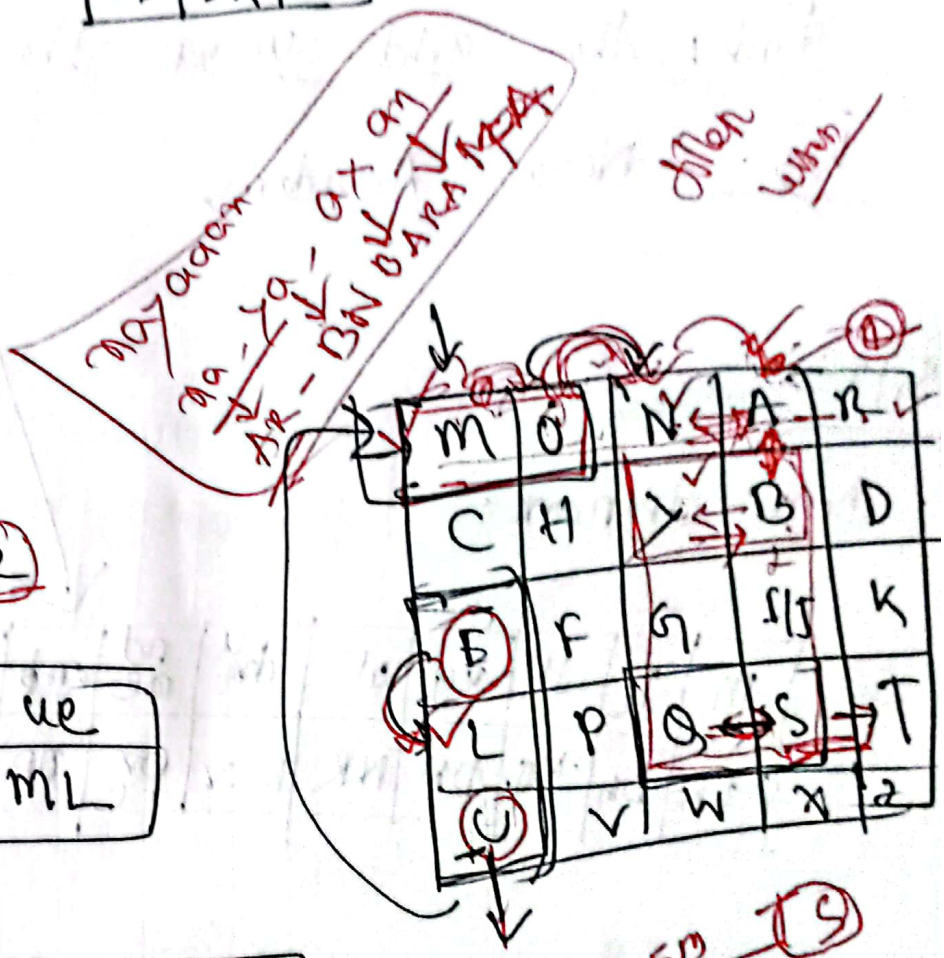
Cipher: RSSRDE

Example:

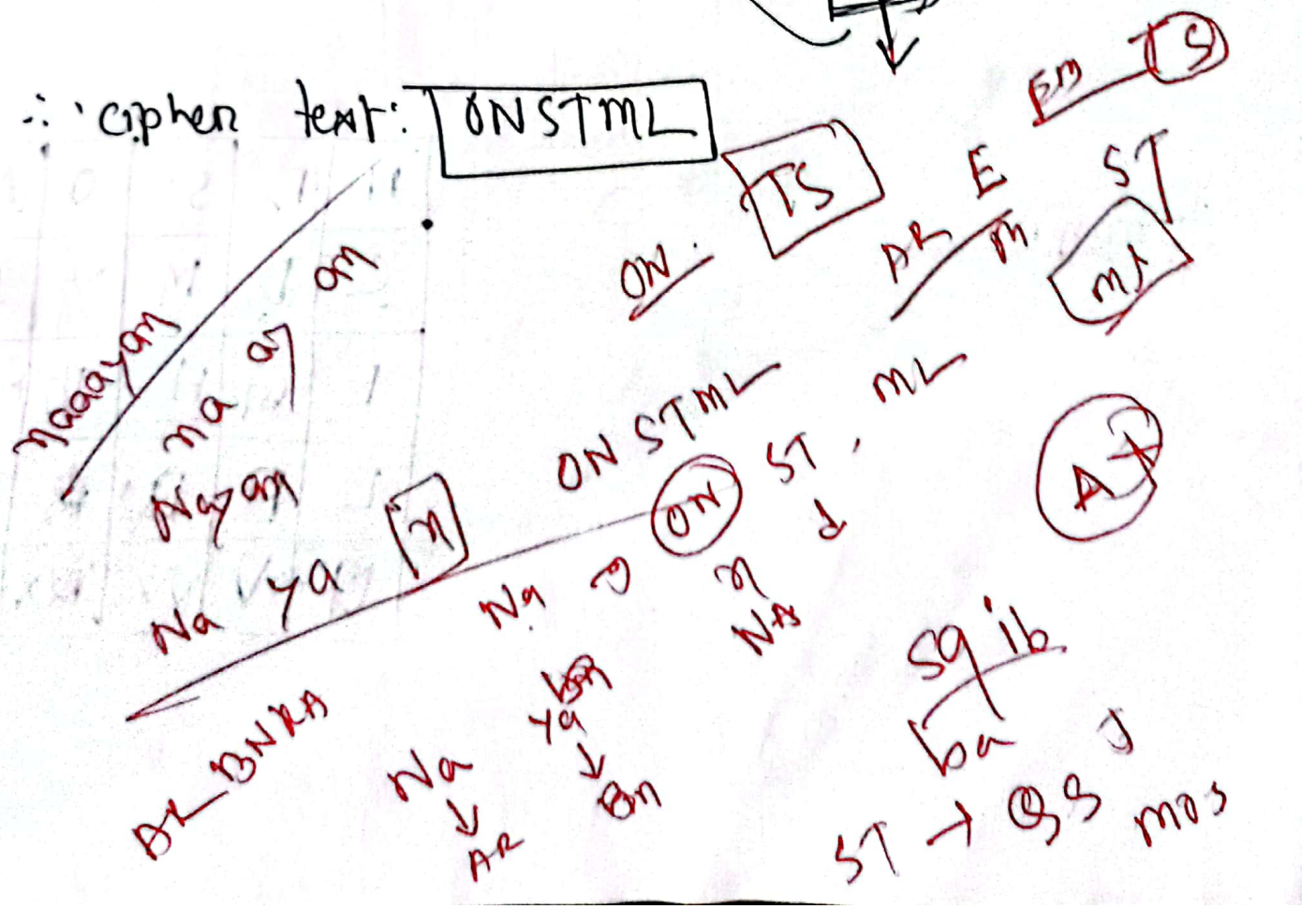
Mosque

mo sq ue

mo	sq	ue
ON	ST	ML



∴ Cipher text: ONSTML



Problem: Using Playfair cipher

→ Plain text:

Hide the gold under the carpet

Key: Neso Academy

Soln:

Now diagram:

Hi	de	th	eg	ol	dh	[illegible]	[illegible]	he	ca	rp	et
IK	DH	KG	DP	NR	[illegible]	[illegible]	OP	SG	NB	QT	MP

N	E	S	O	A
C	D	M	Y	B
F	G	H	[illegible]	K
L	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	Z

Encryption

Decryption

Hill cipher:

Another interesting multiletter cipher is the Hill cipher developed by mathematician Lester Hill in 1929.

↳ Linear algebra →

- matrix modulo 26
- Square matrix
- Determinant
- Multiplicative inverse

Hill Algorithm:

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

$$P = D(K, C) = CK^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$$

$$(C_1, C_2, C_3) = (P_1, P_2, P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$\therefore C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$

$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \text{ modulo } 26$$

$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \text{ modulo } 26.$$

Poly alphabetic cipher:

Encryption,

Sajeeb
iceice

$C = (P_i + K_i) \bmod 26$

dinar key value যে সমান হয় দিতে
হবে (মেলাতে) না হলে সমান না হলে—

যেমন,

Input : Sajeebb

key : Ice

Sajeeb → 18 0 9 4 4 1
iceice → 8 2 4 8 2 4

26 2 13 12 6 5

% 26

= 0

= A C N M G F

=> ACNMGF

তাহলে, key হবে : iceicei → প্রয়োজনে input এর সমান করবো

Decrypt:

$P_i = (C_i - K_i + 26) \bmod 26$

C_i = ciper text value

K_i = key value

Vernam cipher —

(i) used for encrypting alphabet.
(ii) Simple as a type of substitution cipher.

0 10 15
A B C D E F G H I J K L M N O P
Q R S T U V W X Y Z
17 20 25

Encryption:

Plain text: RAMSWARUPK
key : RANCHOBABA

plaintext	17	0	12	18	22	0	17	20	15	10
key →	17	0	13	2	7	14	1	0	1	0
$(P_i + K_i)$ →	34	0	25	20	29	14	18	20	16	10
mod 26 value →	8	0	25	20	3	14	18	20	16	10
cipher text →	I	A	Z	U	D	O	S	U	Q	K

answer → IAZUDOSUQK
26 mins

P → UMMAE

K → FIRST

20	8	12	0	4
5	8	17	18	19
25	20	29	18	23
25	20	3	18	23

L

Z U D S X

ZUDSX

UMMAE

FIRST

Decryption:

Cipher	Z	U	D	S	X	
Key	F	I	R	S	T	
Cipher K						

Dec

Cipher(c_i)	25	20	3	18	23
Key (k_i)	5	8	17	18	19
$c_i - k_i$	20	12	-14	0	4
	20	12	12	0	4
	U	M	M	A	E

Value minus 26

26 करना

[मतलब]

Hill Ciphen Decryption:

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

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

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

$= 15 - 6$

$= 9$

$\det(K) \cdot (\det(K))^{-1} = 1 = 27 \bmod 26$

$\Rightarrow [\det(K)]^{-1} = \frac{27}{9} \bmod 26$

$= 3 \bmod 26$

$= 3$

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

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

$K^{-1} = \frac{1}{9} \begin{bmatrix} 5 & -2 \\ -3 & 3 \end{bmatrix}$

$Adj = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$

$$\therefore K^{-1} = \left[(\det K)^{-1} \cdot \text{Adj}(K)\right] \bmod 26$$

$$= 3\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \bmod 26$$

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

Encrypt

Decrypt

For 3×3.

$$K = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\det(K) = a(ei - hf) - b(di - gf) + c(dh - eg)$$