তথ্য সুরক্ষিত রাখার / কোড করার প্রক্রিয়া
যেখানে সুইফলার সেই ফাংশন বলা হয়।

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

* Ciphen text.
  ↓
  Encrypted text transformed from plain text

plain text
↓
Any readable data

* Classical encryption technique — (2)
  (i) Substitution, (ii) Transposition.
  - Caesen
  - Monoalphabetic
  - playfair
  - Hill
  - Polyalphabetic
  - One-Time Pad
  - Rail Fence
  - Row column Transposition.

*.

4108 (Cryptography)

01. Caesar cipher → 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'.

X	A
Y	B
Z	C

↳ 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).

Plaintext

↓

encrypted text / ciphertext

→ plaintext

Encryption phase with shift n

$E_n(x) = (x+n) \bmod 26$

— Decryption phase with shift n

$D_n(x) = (x-n) \bmod 26$

↳ e.g. ciphertext.

P = HELLO

K = 3

CIPHER

$E_n = (P+K) \bmod 26$

$= (6+3) \bmod 26$

$= 9 \bmod 26$

$= 9$

= J

02. Monoalphabatic cipher

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

↳ In converts plain text into cipher text and re-convert ciphertext 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 find.

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

কোন encryption এর decryption কত shift 1 হলে shift 0.

Shift 0: bnjob
Shift 1: amina ← আগের letter গুলো হবে।
Shift 2: zlhmz

Monoalphabetic

Q	W	E	R	. . . . .	M
A	B	C	D	. . . . .	Z
0	1	2	3	. . . . .	25

Plaintext:

① ABCD → plaintext

↓

QWER → ciphertext.

② A, B, C, D, ... Z.

key = ICE , plaintext = Amina

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

Plain: Amina

Cipher: IMHNI

Hill cipher

→ 2×2 or 3×3 matrix ব্যবহার করে encrypt করা হয়।

2×2 matrix

plaintext = hill

key = sh

23

5.98
= 6

Encryption

$C = PK \bmod 26$

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

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

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

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

5 h

det ≠ 0

203/26 = 7.807

7.81

.81 × 26.

= 21.06

Decryption

ciphertext

key

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

Playfair

5 × 5

→ Repeat করা যাবে না

Encrypt

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

Plaintext = amina

key = sumona

P = amina

am in ax

P = a mina

am in ax

C = CS KO CV

P = amina

C = CSKOCV

Column wise নিচে যাব

s
m
l
o

ml

ci: lo

Row wise ডান দিকে যাব

s m o

ml

ci: lo

Decrypt

amina

am in ax

C = CSKOCV

amin ax

s m l

p q r

s → l

p → r

Eh Poly- Alphabatic

Plaintext = Sumon

key = amima

Enery: (P+K) mod 26

= (18+0) mod 26

= 18 mod 26

= 18

= S

(20+12) mod 26

= 32 mod 26

= 6

= G

0+0 mod 26

= 0

= A

Decryption → ডিক্রিপশন

Vernam cipher

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

keys length = plain text length.

* Bitwise X-OR both the number
* Subtract the number from 26 if the number ≥ 26
* If it's not then leave it.

Encrypt

Plaintext : O A K
key : S O N

26
12
14

Plain →	14	0	10
key →	18	14	13
(P+K)	32	14	23 → ≥26 হলে মোট থেকে 26 বিয়োগ করতে হবে।
	6	14	23

cipher : G O X

Decryption

cipher →	6	14	23
key →	18	14	13
(C-K)	-12	0	10 Negative value এ... যোগ 26 করতে হবে।
	14	0	10

plain → O A K