Semester : VI Subject : CSS Academic Year: 2023-2024

Caesar Cipher :-

It is also called as shift cipher / additive cipher.

Each letter in the plaintext is replaced by a letter corresponding to a no. of shifts in a alphabet.

Note → Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes called Caesar Ciphers.

He used a key of 3 for communications.

(eg) Plain Text → meet me | Zebra.
Cipher Text → PHHW PH | CHEUD.

How is the Cipher Text Generated?

Encryption :

$$C = E(k, P) = (P + K) \bmod 26$$ // Encryption.

P → plain text, k = key.

Decryption :

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

C → cipher text, k = key.

Note : If (C-K) is negative then add 26 to it.

The very first step is numerical value is assigned to each letter as follows :

Semester : 4 Subject : CSS. Academic Year: 20 - 20

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

If the cryptanalyst/attacker knows a cipher text, then he can apply brute-force technique, to find the plain text by using all the possible 25 keys. Since it is a part of symmetric encryption, same key is used for encryption and decryption. The key value lies between 1 and 25.

$$1 \leq K \leq 25$$

Example:
Convert the message → "HELLO" to cipher text using Caesar Cipher. Let key = 4.

$C(H) = (P+K) \bmod 26$
$= (7+4) \bmod 26 = 11 = L.$

$C(E) = (4+4) \bmod 26.$
$= (8) \bmod 26 = 8 = I$

$C(L) = (11+4) \bmod 26$
$= (15) \bmod 26 = 15 = P$

$C(O) = (14+4) \bmod 26$
$= (18) \bmod 26 = 18 = S$

∴ Cipher → LIPPS.

Decryption:

$P = (C-K) \bmod 26$.

$P(L) = (L-4) \bmod 26$

$= (11-4) \bmod 26 = 7 = H$.

$P(I) = (I-4) \bmod 26 = (8-4) \bmod 26 = 4 = E$

$P(P) = (15-4) \bmod 26 = 11 \bmod 26 = 11 = L$

$P(S) = (18-4) \bmod 26 = 14 \bmod 26 = 14 = O$

∴ Plain Text → HELLO

Example 2:-
Use the additive cipher with key = 15 to encrypt the message "hello".

Solution:-

Plain Text →

H	E	L	L	O
↓	↓	↓	↓	↓
7	4	11	11	14.

Encryption:-

$H \rightarrow (07+15) \bmod 26 = 22 \rightarrow W$

$E \rightarrow (04+15) \bmod 26 = 19 \rightarrow T$

$L \rightarrow (11+15) \bmod 26 = 00 \rightarrow A$.

$L \rightarrow (11+15) \bmod 26 = 00 \rightarrow A$

$O \rightarrow (14+15) \bmod 26 = 03 \rightarrow D$.

Cipher Text = WTAAD

Decryption:

Cipher Text : W T A A D

↓ ↓ ↓ ↓ ↓

22 19 00 00 03

W → (22 − 15) mod 26 = 7 → H

T → (19 − 15) mod 26 = 4 → E

A → (00 − 15) mod 26 = −15 = 11 → L

negative → add to 26

A → (00 − 15) mod 26 = 11 → L

D → (03 − 15) mod 26 = 14 → O

Plain Text → HELLO