Q.1 Explain additive cipher? Use additive cipher with key 2 to encrypt message "DEPARTMENT".

→

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

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

plaintext = D E P A R T M E N T

3	4	15	0	17	19	12	4	13	19

Key = 2

Encryption using additive cipher :→

Ciphertext = (plaintext + key) mod 26

① C = (3+2) mod 26

= 5 mod 26

= F

② C = (E+K) mod 26

= (4+2) mod 26

= 6 mod 26

= G

③ C = (P+K) mod 26

= (15+2) mod 26

= 17 mod 26

= R

④ C = (A+K) mod 26

= (0+2) mod 26

= 2 mod 26

= C

Teacher's Signature _____

⑤ $C = (R+K) \bmod 26$

$= (17+2) \bmod 26$

$= 19 \bmod 26$

$= 19 \sim T$

② $C = (m+k) \bmod 26$

$= (12+2) \bmod 26$

$= 14 \bmod 26$

$= 14$

$= O$

⑥ $C = (T+K) \bmod 26$

$= (19+2) \bmod 26$

$= 21 \bmod 26$

$= 21 \sim V$

⑧ $C = (N+K) \bmod 26$

$= (13+2) \bmod 26$

$= 15 \bmod 26$

$= 15 \sim P$

∴ Cipher Text = FIARLTVOLNPV

* Additive Cipher :-

① An additive cipher is a type of mono-alphabetic cipher that shifts the plaintext alphabets by a fixed amount to obtain the cipher alphabet.

② It is also referred as 'shift cipher' or 'caesar cipher'

③ As name suggests, addition modulus 2 operation is performed on plain text to obtain a cipher text.

④ $C = (P+K) \bmod 26$

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

where,

Teacher's Signature

P = plaintext / message

C = ciphertext

K = key

(5) It is not very secure. It can be broken by brute force attack.

(6) It means the message encrypted by this method can easily decrypted.

(7) It is the weak method of Cryptography.

(8) Advantages :→

1) Very easy to implement

2) Simplest method and only one key used in its entire process.

3) It requires only few computing resources.

(9) Disadvantages :→

1) It can be easily hacked.

2) It provide very little security.

3) By looking at the pattern of letters in it, the entire message can decrypted easily.

Question 2. Explain Substitution techniques. Using the key "COMPUTER" encrypt the message "TRANSFER" by using Vigenere cipher.

→ * Substitution technique →

(1) Substitution technique is a classical encryption technique where the characters present in the original message are replaced by other characters or numbers or by symbols.

(2) If the plain text is considered as the string of bits, then the substitution technique would replace bit patterns of plain text with the bit pattern of cipher text.

(3) Some substitution techniques are

a) Caesar Cipher.

b) Monoalphabetic Cipher

c) polyalphabetic cipher.

d) playfair Cipher

e) Hill Cipher

f) One-Time pad.

*

Key =	C	O	M	P	U	T	E	R
	2	14	12	15	20	19	4	17
plaintext =	T	R	A	N	S	F	E	R
	14	17	0	13	18	5	4	17

Teacher's Signature

Encryption:

① $C = (P+K) \bmod 26$
$= (2+19) \bmod 26$
$= 21 \bmod 26$
$= 21 \sim V$

② $C = (P+K) \bmod 26$
$= (14+17) \bmod 26$
$= 31 \bmod 26$
$= 5 \sim F$

③ $C = (P+K) \bmod 26$
$= 12 \bmod 26$
$= 12 \sim M$

④ $C = (P+K) \bmod 26$
$= (5+13) \bmod 26$
$= 28 \bmod 26$
$= 2 \sim C$

⑤ $C = (P+K) \bmod 26$
$= (20+18) \bmod 26$
$= 38 \bmod 26$
$= 12 \sim M$

⑥ $C = (P+K) \bmod 26$
$= (19+5) \bmod 26$
$= 24 \bmod 26$
$= 24 \sim Y$

⑦ $C = (P+K) \bmod 26$
$= 8 \bmod 26$
$= 8 \sim I$

⑧ $C = (P+K) \bmod 26$
$= (17+17) \bmod 26$
$= 34 \bmod 26$
$= 8 \sim I$

∴ Ciphertext = VFMCMYII

Teacher's Signature

V	F	M	C	M	Y	I	I
21	5	12	2	12	24	8	8

Date
Page

* Decryption:

① $p = (c-k) \bmod 26$
$= (21-19) \bmod 26$
$= 2 \bmod 26$
$= 2 \sim C$

② $p = (5-17) \bmod 26$
$= -12 \bmod 26$
$= 14 \sim O$

③ $p = (12-0) \bmod 26$
$= 12 \sim M$

④ $p = (2-13) \bmod 26$
$= -11 \bmod 26$
$= 15 \sim P$

⑤ $p = (12-18) \bmod 26$
$= -6 \bmod 26$
$= 20 \sim U$

⑥ $p = (24-5) \bmod 26$
$= 19 \bmod 26$
$= 19 \sim T$

⑦ $p = (8-4) \bmod 26$
$= 4 \sim E$

⑧ $p = (8-17) \bmod 26$
$= -9 \bmod 26$

∴ plain text = COMPUTER.

Teacher's Signature