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 = (P + K) mod 26
= (D + K) mod 26
= (3 + 2) mod 26
= 5 mod 26
= 5 ∼ F

② C = (E + K) mod 26
= (4 + 2) mod 26
= 6 mod 26
= 6 ∼ G

③ C = (P + K) mod 26
= (15 + 2) mod 26
= 17 mod 26
= 17 ∼ R

④ C = (A + K) mod 26
= (0 + 2) mod 26
= 2 mod 26
= 2 ∼ C

⑤ $C = (R+K) \bmod 26$
$= (17+2) \bmod 26$
$= 19 \bmod 26$
$= 19 \sim T$

⑦ $C = (M+K) \bmod 26$
$= (12+2) \bmod 26$
$= 14 \bmod 26$
$= 14$
$= O$

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 = FGRCTVOGPV.

* 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 refered 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 attacks.

(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 is 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 patterns of letter in it, the entire message can decrypted easily.

Teacher's Signature

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 the 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 pattern 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 $C = (P+K) \bmod 26$
$= (15+13) \bmod 26$
$= 28 \bmod 26$
$= 2 \sim C$

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 _____

Decryption :

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

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

③ $p = (12 - 12) \bmod 26$
$= 0 \bmod 26$
$= 0 \sim A$

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

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

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

⑦ $p = (8 - 4) \bmod 26$
$= 4 \bmod 26$
$= 4 \sim E$

⑧ $p = (8 - 17) \bmod 26$
$= 17 \sim R$

∴ plaintext = TRANSFER.

Teacher's Signature

Question 3. Explain the Substitution Techniques ? if the cipher is keyed by a word "COMPUTER" and plaintext is "please transfer one million dollars to my account six six two" obtain the cipher text by playfair substitution methods ?

→

* Substitution Techniques :→

(1) A Substitution cipher simply means that each letters in the plaintext is substituted with another letter to form the ciphertext.

(2) Substitution technique is a classical encryption approach where the characters represent in the initial message are restored by the other characters or number or by symbol.

(3) There are various types of substitution ciphers :
a) monoalphabetic cipher.
b) polyalphabetic cipher.

plaintext = PLEASE TRANSFER ONE MILLION DOLLARS TO MY ACCOUNT SIX SIX TWO.

Key = COMPUTER

Teacher's Signature

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

PL	EA	SE	TR	AN	SF	ER	ON	EM	IL	LI
OΦ	RB	LB	EA	RΦ	LI	RA	ML	RO	FS	SF

ON	DO	LX	EA	RS	TO	MY	AC	CO	UN	TS
ML	FC	NW	ΦE	BN	EC	PX	TP	OM	MS	BK

IX	SI	XT	WO
GZ	ZJ	VR	OE

Ciphertext : OΦRBLB EARΦLIRA MLR OFSSFML

FCNWΦEBN EC PX TPOMMSBK

KGZ ZJVR ROE

Q.4 One time pad :

plaintext = SUBJECT

key = abcd

→ plaintext = SUBJECT

key = abcdefg

adding e f g, because length of plaintext & key must be same in one time pad

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

plain text = S U B J E C T

18 20 1 9 4 2 19

key = a b c d e f g

0 1 2 3 4 5 6

Add: (plaintext + key)

18 21 3 12 8 7 25

Subtract: (subtract if no. is greater than 26)

18 21 3 12 8 7 25

Cipher text = S V D M I H Z

18 21 3 12 8 7 25

Teacher's Signature _____

Ques.5) Explain DES in detail.

→ (1) DES stands for Data Encryption Standard.

(2) The DES algorithm uses a key of 56 bit size.

(3) Using the key, the DES takes a block of 64 bit plain text as input and generates a block of 64 bit cipher text.

(4) General structure of DES is depicted in the following illustration:

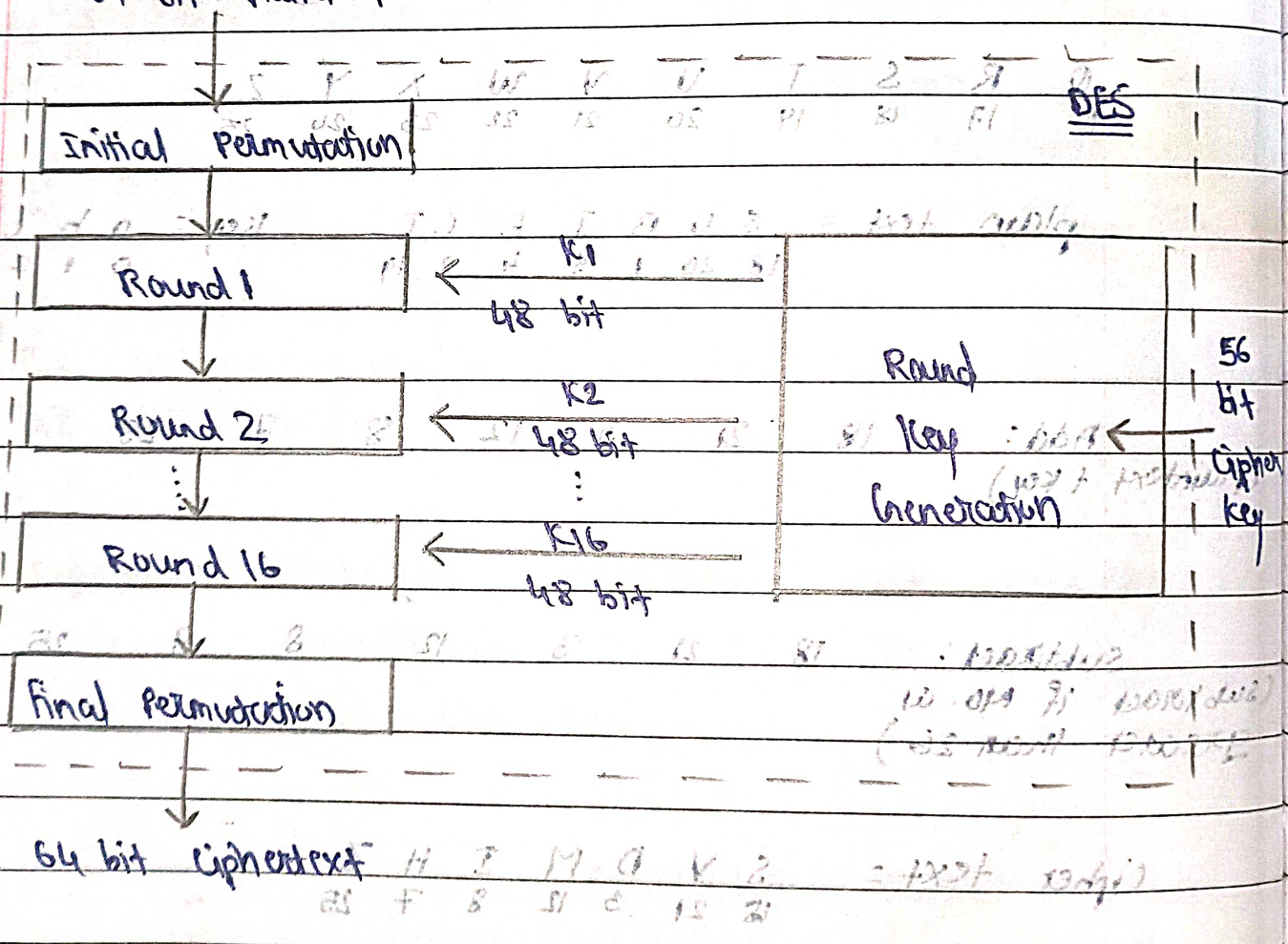

Fig: DES

Teacher's Signature _____

(5) DES is an implementation of Feistel cipher. It uses 16 round Feistel structure.

(6) Since DES is based on the Feistel cipher, all that is required to specify DES is -
- Round function
- Key Schedule
- Any additional processing - initial and final permutation

(7) The encryptor and the decryptor need to use the same key otherwise they will not be able to communicate together.

(8) The decryption process is the exact opposite of the encryption - It takes in a 64 bit block of ciphertext and produces the 64-bit block of plaintext using the same 48 bit key during encryption.

Q.6 Difference between :→

a) Private Vs Public key cryptography
b) Conventional Vs public key encryption
c) Symmetric Vs Asymmetric cryptography.

→

Private key Cryptography	Public key cryptography
(1) Private key is faster than the public key	(1) It is slower than private key.
(2) In this, the same key & algo. are used to encrypt and decrypt the message	(2) In this, two keys are used.
(3) private key is symmetrical because there is only one key that is called Secrete key	(3) public key is asymmetrical because there are two keys
(4) It is efficient technology	(4) It is an inefficient technology.
(5) It is used for large amount of text	(5) It is used for only short message.

Teacher's Signature