1. Given a cipher text, "**TTB JTB EAO MHE ENL OHY"**. Show all the mathematical calculations and works involved to derive the answers. Decrypt the cipher text using the Transposition cipher and a key: **453126**. Find the original message (plain text).

[5 Marks]

6	2	1	3	5	4
O	E	M	E	J	T
H	N	H	A	T	T
Y	L	E	O	B	B

1	2	3	4	5	6
M	E	E	T	J	O
H	N	A	T	T	H
E	L	O	B	B	Y

MEETJOHNATTHELOBBY
Decrpt: MEET JOHN AT THE LOBBY

2. Given a Plain text, "**CYBER FORENSIC IS FUN"**. Answer all the following question. Show all the mathematical calculations and works involved to derive the answers. Encrypt the plain text using Vigenere cipher and a key: **REPUBLIC.** Find the Encryption message (Cipher Text)

[8 Marks]

Answer:

C	Y	B	E	R	F	O	R	E	N	S	I	C	I	S	F	U	N	X	Y	Z	A	B	C
R	E	P	U	B	L	I	C	R	E	P	U	B	L	I	C	R	E	P	U	B	L	I	C

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Pi	Ki	$(Pi + Ki) mod 26$	Ci
2	17	$(2+17) mod\ 26 = 19 (2\ +\ 17)\ mod\ 26\ =\ (2+17) mod 26 = 19$	19
24	4	$(24+4) mod\ 26 = 2 (24\ +\ 4)\ mod\ 26\ =\ (24+4) mod 26 = 2$	2
1	15	$(1+15) mod\ 26 = 16 (1\ +\ 15)\ mod\ 26\ =\ (1+15) mod 26 = 16$	16
4	20	$(4+20) mod\ 26 = 24 (4\ +\ 20)\ mod\ 26\ =\ (4+20) mod 26 = 24$	24
17	1	$(17+1) mod\ 26 = 18 (17\ +\ 1)\ mod\ 26\ =\ (17+1) mod 26 = 18$	18
5	11	$(5+11) mod\ 26 = 16 (5\ +\ 11)\ mod\ 26\ =\ (5+11) mod 26 = 16$	16
14	8	$(14+8) mod\ 26 = 22 (14\ +\ 8)\ mod\ 26\ =\ (14+8) mod 26 = 22$	22
17	2	$(17+2) mod\ 26 = 19 (17\ +\ 2)\ mod\ 26\ =\ (17+2) mod 26 = 19$	19
4	17	$(4+17) mod\ 26 = 21 (4\ +\ 17)\ mod\ 26\ =\ (4+17) mod 26 = 21$	21
13	4	$(13+4) mod\ 26 = 17 (13\ +\ 4)\ mod\ 26\ =\ (13+4) mod 26 = 17$	17
18	15	$(18+15) mod\ 26 = 7 (18\ +\ 15) mod\ 26\ =\ (18+15) mod 26 = 7$	7
8	20	$(8+20) mod\ 26 = 2 (8\ +\ 20)\ mod\ 26\ = (8+20) mod 26 = 2$	2
2	1	$(2+1) mod\ 26 = 3 (2\ +\ 1)\ mod\ 26\ = (2+1) mod 26 = 3$	3
8	11	$(8+11) mod\ 26 = 19 (8\ +\ 11)\ mod\ 26\ =\ (8+11) mod 26 = 19$	19
18	8	$(18+8) mod\ 26 = 0 (18\ +\ 8)\ mod\ 26\ =\ (18+8) mod 26 = 0$	0
5	2	$(5+2) mod\ 26 = 7 (5\ +\ 2)\ mod\ 26\ =\ (5+2) mod 26 = 7$	7
20	17	$(20+17) mod\ 26 = 11 (20\ +\ 17)\ mod\ 26\ = (20+17) mod 26 = 11$	11
13	4	$(13+4) mod\ 26 = 17 (13\ +\ 4)\ mod\ 26\ =\ (13+4) mod 26 = 17$	17

$$Ci = (Pi + Ki) mod 26$$

TCQYSQWTVRHCDTAHLR

3. In order to deliver a key in safely condition, Diffie Hillman key exchange has been applied. In this algorithm, both sender, **Alice** and receiver, **Bob** has agreed on the values for 2 parameter which are p, prime number and g, root number (p = 17 and g = 13). Find the value for shared keys.

[7 Marks]

$$Let: p = 17;\ g = 13; X_A = 3;\ X_B = 5$$

$Y_A = g^{X_A} mod p$ $Y_A = 13^3 mod 17 = 4$	$Y_B = g^{X_B} mod p$ $Y_B = 13^5 mod 17 = 13$
$K_1 = Y_B^{X_A} mod\ p$ $K_1 = 13^3 mod 17 = 4$	$K_2 = Y_A^{X_B} mod\ p$ $K_2 = 4^5 mod 17 = 4$

$$K_1 = K_2 = 4$$

4. Given a plain text, **"SEE YOU AT THE LOBBY NOW"**. Encrypt the plain text using the monoalphabetic substitution cipher with the key obtained from **QUESTION 3**.

[7 Marks]

5. Given a cipher text, "WCGXEERORYLVYTAHOPP". Decrypt the cipher text using Rail Fence cipher with the key obtained from **QUESTION 3.**

[5 Marks]

$k = 4$

W						C						G						X
	E				E		R				O		R				Y	
		L		V				Y		T				A		H		
			O						P						P			

WELOVECRYPTOGRAPHYX

WE LOVE CRYPTOGRAPHY

6. Given a plain text "HIDDEN". Encrypt the message using RSA algorithm with **p=5**, **q=7** and public key **e=5**. Do the works for each alphabet.

[10 Marks]

$$n = p \times q = 5 \times 7 = 35$$

$$\phi(n) = (p-1)(q-1) = (5-1)(7-1) = (4)(6) = 24$$

$$d_{k=n} = \frac{[1 + k\phi(n)]}{e}$$

$$d_{k=0} = \frac{[1+0]}{5} = fraction$$

$$d_{k=1} = \frac{[1+24]}{5} = \frac{25}{5} = 5\ not\ a\ fraction\ \boldsymbol{STOP}$$

so, d=5

Use public key to encrypt the message usin g formula $C = M^e mod\ n$

P:	H	I	D	D	E	N

M:	7	8	3	3	4	13
$M^5 mod\ 35$: $M^d mod\ n$	7	8	33	33	9	13

Ciphertext=7, 8, 33, 33, 9, 13

Decrypt: $M^d mod\ n$