Assignment No. 2

Q. 1) Using the play fair to encrypt the following message "This is a columnar transposition" use key APPLE.

→ plaintext :- "This is a columnar transposition"
key :- APPLE

→ Step 1 :- Generate the key square (5 x 5).

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

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

- Step 2 :- The plaintext is split into pairs of two letters. If their is an odd number of letters, a z is added to the last letter.

→ Plaintext :- "This is a columnar transposition"
After split :- 'Th' 'is' 'is' 'ac' 'ol' 'um' 'na' 'rt' 'ra' 'ns' 'po' 'si' 'ti' 'on'

Step 3 :- Convert the plaintext into ciphertext According to rules.

Th → UG
is → MQ
Ac → CI / CJ
ol → MB
um → SO
na → IE / JE
rt → SU
ra → QP
ns → MT
po → BK
si → QM
ti → QN
on → IO / JO

∴ ciphertext :- UGMQCIMBSOJESUQPMTBKQMQNIO

Q.2) Using Hill cipher encrypt the message 'ESSENTIAL'. The key of encryption is 'ANOTHERBZ'

→ plaintext :- ESSENTIAL
key :- ANOTHERBZ

1) Step 1 :- create a matrix (3×3)

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

$$\text{key} :- \begin{bmatrix} A & N & O \\ T & H & E \\ R & B & Z \end{bmatrix} = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 7 & 4 \\ 17 & 1 & 25 \end{bmatrix}$$

2) The message 'ESSENTIAL' is written as vector.

$$\text{plaintext} \Rightarrow \text{ESSENTIAL} = \begin{bmatrix} E & S & S \\ E & N & T \\ I & A & L \end{bmatrix} \Rightarrow \begin{bmatrix} 4 & 18 & 18 \\ 4 & 13 & 19 \\ 8 & 0 & 11 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} E \\ E \\ I \end{bmatrix} \begin{bmatrix} S \\ N \\ A \end{bmatrix} \begin{bmatrix} S \\ T \\ L \end{bmatrix} \Rightarrow \begin{bmatrix} 4 \\ 4 \\ 8 \end{bmatrix} \begin{bmatrix} 18 \\ 13 \\ 0 \end{bmatrix} \begin{bmatrix} 18 \\ 19 \\ 11 \end{bmatrix}$$

- Step 3 :- The enciphered vector is given as

$$\begin{bmatrix} 0 & 13 & 14 \\ 19 & 7 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 4 \\ 4 \\ 8 \end{bmatrix} = \begin{bmatrix} 164 \\ 136 \\ 272 \end{bmatrix} = \begin{bmatrix} 8 \\ 6 \\ 12 \end{bmatrix} \pmod{26}$$

Which corresponds to ciphertext of IGM

$$\begin{bmatrix} 0 & 13 & 14 \\ 19 & 7 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 18 \\ 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 169 \\ 433 \\ 319 \end{bmatrix} \Rightarrow \begin{bmatrix} 13 \\ 17 \\ 7 \end{bmatrix} \pmod{26}$$

Which corresponds to ciphertext of 'NRH'

$$\begin{bmatrix} 0 & 13 & 14 \\ 19 & 7 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 18 \\ 19 \\ 11 \end{bmatrix} = \begin{bmatrix} 401 \\ 519 \\ 600 \end{bmatrix} \Rightarrow \begin{bmatrix} 11 \\ 1 \\ 2 \end{bmatrix} \pmod{26}$$

Which corresponds to ciphertext of 'LBC'

∴ Ciphertext of message 'ESSENTIAL' is 'JGMNRHLBC'

Q.3) Using polyalphabetic cipher to encryt the plain text 'SHE IS VERY HAPPY AND BEAUTIFUL GIRL" using Key "ANOTHER"

→ (By using Vigenere Cipher, we solve above problem;
plaintext :- 'SHE IS VERY HAPPY AND BEAUTIFUL GIRL'
KEY :- "ANOTHER"

→ Step 1 :-
'SHE IS VERY HAPPY AND BEAUTIFUL GIRL'
ANO TH ERAN OTHER ANO THERANOTH ERAN

To encrypt, pick a letter in the plaintext & its corresponding letter in the keyword, use the keyword letter & the plaintext letter as the row index & column index, respectively, & the entry at the row-column intersection is the letter in the ciphertext.

∴ Ciphertext :- SUSBZZVRLVTWTPAARULAELTVTNSKZRY

Q.4) Use the transposition cipher to encrypt the plain text 'WE ARE THE BEST" use the key 'HEAVEN'.

→ plain text :- 'WE ARE THE BEST'
Key :- 'HEAVEN'

~~1)~~ ~~Rail Fence Cipher~~.
By using Columnar transposition Technique. we solve the above Example.
plain text :- 'WE ARE THE BEST'
Key :- 'HEAVEN' length of keyword :- 6
~~Matrix :- 6×~~
order of Alphabets in HEAVEN :- ~~23164~~ 421635

H E A V E N
4 2 1 6 3 5
W E - A R E
~~T H E~~
- H E

H	E	A	V	E	N
4	2	1	6	3	5
W	E	-	A	R	E
-	T	H	E	-	B
E	S	T			

Ciphertext :- ~~HTETSRWE~~
-HTETSR_W_EEBAE

Another order of Alphabet in HEAVEN :- 431625

H	E	A	V	E	N
4	3	1	6	2	5
W	E	-	A	R	E
-	T	H	E	-	B
E	S	T			

Ciphertext :- -HTR_E§TS W_EEBAE