Assignment No. 2

(9.1) Using the play fair to encrypt the following message "This is a columnar transposition" use key

-> plaintext: "This is a columnar transposition"

-> Step 1: - Generate the key square (5x5).

1 11 11 14 1			1	10	7]	A	P	1	E	В
A	P	12		G	10 1	C	D	E	G	Ħ
13	ILT	N/A	M	N	1.89	IH	K	M	N	0
1	73	R	5	Т		9	R	5	T	U
1	V	W			a 1	V	W	X	Y	2

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 a columnar transposition" po si ti on

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

Th -> UG ns -> MT is → Mg . po → BK

AC -> CI/CJ Si -> OM

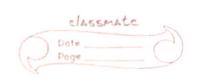
ol → MB ti → ON

um -) 50 0n -> 10/Jo

na -> IE/JE

x t → 50

7a -) OP



: ciphertext :- 1	UGMQCIMB50 IE SUOPM	TBKGM9NIO
-------------------	---------------------	-----------

0.2) 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 F F G H J J K L M N O P 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

9 R S T U V W X Y Z 16 17 18 19 20 21 22 23 24 29

A N 0 0 0 13 14 1 Key:- T H E = 19 7 4 17 1 25

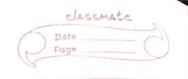
2) The message 'ESSENTIAL' is written as vector

 $\begin{array}{c|c} \Rightarrow & \begin{bmatrix} E \\ E \end{bmatrix} & \begin{bmatrix} S \\ N \end{bmatrix} & \begin{bmatrix} S \\ T \end{bmatrix} \Rightarrow \begin{bmatrix} 4 \\ 4 \end{bmatrix} & \begin{bmatrix} 18 \\ 13 \end{bmatrix} & \begin{bmatrix} 18 \\ 19 \end{bmatrix} \\ \downarrow & \downarrow & \end{bmatrix}$

Step 3:- The enciphered vector is given as

 $\begin{bmatrix}
0 & 13 & 147 & 47 & 164 \\
19 & 7 & 4 & 47 & 136 & = 6 \\
17 & 1 & 25 & 8 & 272
\end{bmatrix}$ $\begin{bmatrix}
10 & 13 & 147 & 47 & 164 \\
47 & = 136 & = 6 \\
272 & = 19
\end{bmatrix}$

Which corresponds to ciphertext of IGM



$$\begin{bmatrix} 0 & 13 & 14 \\ 19 & 7 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 18 \\ 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 169 \\ 433 \\ 319 \end{bmatrix} \Rightarrow \begin{bmatrix} 13 \\ 17 \\ 7 \end{bmatrix} \pmod{2c}$$

Which corresponds to ciphertext of NRH'

$$\begin{bmatrix}
0 & 13 & 14 \\
19 & 7 & 4
\end{bmatrix}
\begin{bmatrix}
19 & = \begin{bmatrix} 401 \\
519 \\
600 \end{bmatrix}
=)
\begin{bmatrix}
11 \\
25
\end{bmatrix}$$
(mod 26)

Which corresponds to ciphertext of 'LBC'

.. Ciphertext of message ESSENTIAL is JGMNRHLBC'

- (5.3) Using polyalphabetic cipherto encryt the plaintext "SHE IS VERY HAPPY AND BEAUTIFUL GIRL" using Key "ANOTHER"
 - -) (By using Vigenere (ipher. we solve above problem.)

 plaintext: SHE IS VERY HAPPY AND BEAUTIFUL GIRL'

 KEY: ANOTHER

-> Step 1:SHE IS VERY HAPPY AND BEAUTIFUL GIRL
AND THE ERAN OTHER AND THERANOTH ERAN

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

: Ciphertext :- SUSBZZVRLVTWTPAARULAELTVTNSKZRY

0.4)	Use the transposition cipher to encrypt the
	plain text 'WE ARE THE BEST" Use the Key 'HEAVEN'
->	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 - 6x

order of Alphabets in HEAVEN: - 23164 421635

HEAVEN	H	E	Α	V	E	N	
4 2 1/6 3 5	4	2	1	6	3	5	
WE - A RE	W	E		Α	R	E	
THE.		T	H	E		B	
- H E	E	5	T				-

Ciphertext :- HTETSRWE

-HTETSR-W-EEBAE

Another order of Alphabet in HEAVEN: 431625

HEAVEN: 431625

WE-ARE

THE-B

Ciphertext: - HTR_ESTSW_EEBAE