4- Hill cipher:

Hill cipher is a multiletter cipher . The encryption algorithm takes *m* successive plaintext letters and substitutes for them *m* ciphertext letters. The substitution is determined by *m* linear equations in which each character is assigned a numerical value (a = 0, b = 1 ... z = 25). For *m* = 3, the system can be described as follows:

$$c_1 = (k_{11_{p1}} + k_{12_{p2}} + k_{13_{p3}}) \bmod 26$$

$$c_2 = (k_{21_{p1}} + k_{22_{p2}} + k_{23_{p3}}) \bmod 26$$

$$c_3 = (k_{31_{p1}} + k_{32_{p2}} + k3_{3_{p3}}) \bmod 26$$

This can be expressed in term of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

Or

$$\mathbf{C} = \mathbf{KP} \bmod 26$$

C is cipher letter (3x1)

K is key (3x3).

P is plaintext letter (3x1).

In general terms, the Hill system can be expressed as follows:

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{KP} \bmod 26$$

$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{P}) = \mathbf{K}^{1}\mathbf{C} \bmod 26 = \mathbf{K}^{1}\mathbf{KP} = \mathbf{P}$$

Ex: plaintext = paymoremoney

and use the encryption key is

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Find the ciphertext?

Sol:

pay mor emo ney

first three letters p=15 , a=0 , y=24

this can be represented in vector as :

$$P=\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$$

Then;

$$C=K\,P \bmod 26= \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$$

11 = L , 13 = N , 18 = S

So , pay $\longrightarrow$ LNS .continuing in this fashion,

The ciphertext for the entire plaintext is LNSHDLEWMTRW.

Ex :

Decrypt the above ciphertext ?

Sol.

Decryption requires using the inverse of the matrix **K**. The inverse **K** of a matrix **K** is defined by the equation **KK**   = **K**   **K** = **I**,

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as follows:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

P= D(K,C)= K   . C mod 26

$$\begin{bmatrix} P1 \\ P2 \\ P3 \end{bmatrix} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 11 \\ 13 \\ 5 \end{bmatrix} \quad \text{mod26=} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \quad \begin{matrix} p \\ a \\ y \end{matrix}$$

H.W

The plaintext "**friday**" is encrypted using a 2 x 2 Hill cipher to yield the ciphertext **PQCFKU**, find the encrypted key?

Note: to find additive inverse modulo n of an integer we use the table below ,as example modulo 5

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The negative of integer x is the integer y ,such that

$$(x+y) \bmod n = 0$$

$$(x+y) \bmod 5 = 0$$

If x=2 ⟹ y=3 because (2+3)mod 5=0

If x=4 ⟹ y=1 because (4+1) mod 5=0

While the multiplicative inverse of an integer x is y such that

$$(x^* y) \bmod n = 1$$

Example of modulo 5 multiplicative invers of an integer x is

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(x*y) mod 5 =1

If x= 2 ⟹ y=3 because (2*3) mode 5=1

If x= 4 ⟹ y=4 because (4*4) mod 5=1

<u>Example</u> :

Find $\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$ for modulo 26 ?

<u>solution :</u>