***HILL CIPHER***

*Hill Cipher was developed by Lester Hill in 1929. It was the first Polygraphic cipher to operate on more than 3 symbols at once .*

* *Encryption – Each letter is represented by a number Modulo 6 ,*

*As follows ( A=0 , B=1 ,C=2 …. Z=25)*

*The Message to be encrypted is “HILL” which is equivalent to [H L] = [7 11]*

*[I L] [8 11]*

*The Letter is in the 7th Position so we replace h by 7 , I by 8 and l by 11 respectively*

* *Each Block of N letters is multiplied by an Invertible nxn matrix mod 26 .*

*Let us assume the Key K = BAAD which is equivalent to [B A]=[1 0]*

*[A D] [0 3]*

*The letter A is in the 0th position so replace A by 0 , B by 1,D by 3*

* *Now to Encrypt the data .*

*Each column of the message is Multiplied by the Key Separately*

1. *[1 0] [7]=[1\*7+0\*8]=[7 ] mod 26 = [H]*

*[0 3] [8] [0\*7+3\*8] [24] [Y]*

1. *[1 0][11]=[1\*11+0\*11]=[11]mod26 = [11] = [L]*

*[0 3][11] [0\*11+3\*11] [33] [7 ] [H]*

*Therefore the Encrypted message is HYLH.*

* *Now to Decrypt the data HYLH.*

1. *We must use the Inverse of the key to Decrypt*

*So K=[1 0] becomes K^-1 = [3 -0 ] that is [3 0]*

*[0 3] [ -0 1] [0 1]*

1. *The Determinant of the K [1 0] is calculated that is (1\*3-0\*0) = 3-0 = 3*

*[0 3]*

1. *Now we need to find the modular multiplicative inverse . we can do that When 3 is multiplied by its inverse =3\*1/3 = 1*

*3\*x=1mod26*

*X=9*

1. *We find the modular of the inverse of the key [3 0 ] that is [ 3 0]*

*[0 1] [0 1]*

1. *Now multiply the value of x with the matrix*

*9\* [3 0]=[27 0]*

*[0 1] [0 9]*

1. *Now we find the mod of this matrix [27 0] mod 26 = [1 0] = Decryption key*

*[0 9] [0 9]*

1. *Decrypt text HYLH = [7 11]*

*[24 7]*

1. *Multiply the columns individually*

*For HY [1 0][7] = [ 1\*7+0\*24]= [7]*

*[0 9][24] [0\*7+9\*24] [216]*

*For LH[1 0][11] = [1\*11+0\*7]= [11]*

*[0 9][7] [0\*11+9\*7] [63]*

1. *Now the matrix mod 26 gives = [7 11] = [7 11] mod 26 = [H L]*

*[216 63] [8 11] [I L]*

1. *The Decrypted message is HILL.*