HILL CIPHER

- This multi-letter cipher is developed by the mathematician lester hill in 1929.

- An n-gram substitution may define using an invertible nxn matrix A= aij as the key to map an n-character plaintext m1,m2,…mn to a cipher text n-gram

- $C=E_K(X)=KX \bmod 26$
- $X=D_K(C)= K^{-1}C \bmod 26$

- For n=3
- $C1= (k_{11}x_1+k_{12}x_2+k_{13}x_3) \bmod 26$
- $C2= (k_{21}x_1+k_{22}x_2+k_{23}x_3) \bmod 26$
- $C3= (k_{31}x_1+k_{32}x_2+k_{33}x_3) \bmod 26$

HILL CIPHER (Conti…)

- Example: encrypt ‘meet b’ using 2x2 hill cipher with the key k= $\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$
- $K^{-1}= \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$
- Plain text will be written as ME ET BX
- Letters with there numerical values are as follows

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

- Numerical values for plain text letters are 12 4, 4 19, 1 23

HILL CIPHER (Conti…)

- **ENCRYPTION**
- $\begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{pmatrix} k11 & k12 \\ k21 & k22 \end{pmatrix} x \begin{pmatrix} x1 \\ x2 \end{pmatrix} \bmod 26$
- $\begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} X \begin{pmatrix} 12 \\ 4 \end{pmatrix} \bmod 26$

- C1=(36+4) mod 26 = 14 = o
- C2=(60+8) mod 26 = 16 = q
- C3=(12+19) mod 26 = 5 = f
- C4=(20+38) mod 26 = 6 = g
- C5=(3+23) mod 26 = 0 = a
- C6=(5+46) mod 26 = 25 = z
- Encrypted text is : ‘oq fg az’

HILL CIPHER (Conti…)

- **DECRYPTION**
- $\begin{pmatrix} X1 \\ X2 \end{pmatrix} = \begin{pmatrix} k11 & k12 \\ k21 & k22 \end{pmatrix} x \begin{pmatrix} C1 \\ C2 \end{pmatrix} \bmod 26$
- $\begin{pmatrix} x1 \\ x2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} X \begin{pmatrix} 14 \\ 16 \end{pmatrix} \bmod 26$

- x1=(28-16) mod 26 = 12 = m
- x2=(-70+48) mod 26 = 4 = e
- x3=(10-6) mod 26 = 4 = e
- x4=(-25+18) mod 26 = 19 = t
- x5=(0-25) mod 26 = 1 = b
- x6=(0+75) mod 26 = 23 = x
- Decrypted text is : ‘me et bx’

HILL CIPHER (Conti…)

- Encrypt a message “CIPHER” using 3x3 hill cipher with key=[{2,1,1}, {1,1,2}, {1,0,-2}]

- K= 2 1 1
- 1 1 2
- 1 0 -2

- K^{-1}= 2 -2 -1
- -4 5 3
- 1 -1 -1

- Pain text: CIP HER
- Cipher text: BOY JIP