Hill cipher

The encryption takes m successive plaintext letters & substitutes them m ciphertext letters.

steps :-

1) choose plaintext,
   if plaintext = students.
   choose digram for plaintext
   st ud en ts.

2) choose key.
   * if we are encrypting 2 letters at a time, then ensure key must be a 2×2 matrix
   * Then always choose a key such a way that, key matrix can be invertible,
   * For determinant of key matrix, it should have multiplicate inverse, otherwise matrix cannot be invertible.

Follow above rules while choosing a key size.

Here we have chosen key

dbgf.

write it in matrix form

$$\begin{bmatrix} d & b \\ g & f \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$$

3) Assign numerical equivalent to alphabets.

0	1	2	3	4	5	6	7	8	9	10	11
a	b	c	d	e	f	g	h	i	j	k	c

12	13	14	15	16	17	18	19	20	21	22	23	24	25
m	n	o	p	q	r	s	t	u	v	w	x	y	z

4) convert the plaintext Students to a 2 component vector

plaintext: st ud en ts.

$$= \begin{bmatrix} s \\ t \end{bmatrix} \begin{bmatrix} u \\ d \end{bmatrix} \begin{bmatrix} e \\ n \end{bmatrix} \begin{bmatrix} t \\ s \end{bmatrix}$$

$$= \begin{bmatrix} 18 \\ 19 \end{bmatrix} \begin{bmatrix} 20 \\ 3 \end{bmatrix} \begin{bmatrix} 4 \\ 13 \end{bmatrix} \begin{bmatrix} 19 \\ 18 \end{bmatrix}.$$

5) Encryption

Ciphertext = $k * p \bmod 26$.

$$C_1 = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \times \begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{bmatrix} 18\times3 + 19\times1 \\ 18\times6 + 5\times19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 73 \\ 203 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 \\ 21 \end{bmatrix} = \begin{bmatrix} V \\ V \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \times \begin{bmatrix} 20 \\ 3 \end{bmatrix} = \begin{bmatrix} 63 \\ 135 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 11 \\ 5 \end{bmatrix} = \begin{bmatrix} L \\ F \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \times \begin{bmatrix} 4 \\ 13 \end{bmatrix} = \begin{bmatrix} 12+13 \\ 24+65 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 25 \\ 89 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 25 \\ 11 \end{bmatrix} = \begin{bmatrix} Z \\ L \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \times \begin{bmatrix} 19 \\ 18 \end{bmatrix} = \begin{bmatrix} 57+18 \\ 114+90 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 75 \\ 204 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 23 \\ 22 \end{bmatrix} = \begin{bmatrix} X \\ W \end{bmatrix}$$

Ciphertext = VVCFCXW.

Decryption = $K^{-1} C \bmod 26$.

$$K = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}_{2\times 2}$$

$$K^{-1} = \frac{Adj(K)}{|K|} = \frac{1}{|K|} \times Adj(K)$$

$|K| = 3\times 5 - 6\times 1$
$= 15 - 6 = 9$

[Here $|K| \neq 0$. then Inverse exist When selecting Key this point to be kept in mind]

Make sure Multiplicative inverse of determinant must be found out.

Gcd (9, 26) = 1

i.e. $9X \bmod 26 = 1$

Trial & error

$9\times 1 \bmod 26 = 9$ ✗
$9\times 2 \bmod 26 = 18$ ✗
$9\times 3 \bmod 26 = 27 \bmod 26 = 1$ ✓

So Here Multiplicative inverse is (3)

This point also must be kept in mind while choosing key.

(3)

So. multiplicative inverse must exist — chose the key accordingly, SC2. if multiplicative inverse must be there for determinant otherwise we cannot find inverse a matrix

$$adj(K) = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \quad \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$$

$\left(\frac{1}{|K|}\right) = 3$.

$$K^{-1} = \frac{1}{|K|} \times adj(K)$$

$$= 3 \times \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix} * 3 = \begin{bmatrix} 15 & -3 \\ -18 & 9 \end{bmatrix} \quad +26$$

$+26$

Add +26 wherever -symbol is there (-ve numbers)

So $K^{-1} = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix}_{2\times 2}$

Decryption $= K^{-1} C \mod 26$

$$P1 = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} 21 \\ 21 \end{bmatrix} \mod 26.$$

$$\begin{bmatrix} 315+483 \\ 168+189 \end{bmatrix} \mod 26 = \begin{bmatrix} 798 \\ 357 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{bmatrix} S \\ T \end{bmatrix}$$

$$d_2 = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} 11 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 165+115 \\ 88+45 \end{bmatrix} \bmod 26 = \begin{bmatrix} 280 \\ 133 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 20 \\ 3 \end{bmatrix} = \begin{bmatrix} 4 \\ d \end{bmatrix}$$

$$d_3 = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} 25 \\ 11 \end{bmatrix} \bmod 26$$

~~$\begin{bmatrix} 225+253 \\ 120+99 \end{bmatrix} \bmod 26 = \begin{bmatrix} 478 \\ 219 \end{bmatrix} \bmod 26$~~

~~$= \begin{bmatrix} 10 \\ 11 \end{bmatrix}$~~

$$\begin{bmatrix} 375+253 \\ 200+99 \end{bmatrix} \bmod 26 = \begin{bmatrix} 628 \\ 299 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 4 \\ 13 \end{bmatrix} = \begin{bmatrix} e \\ n \end{bmatrix}$$

$$d_4 = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} 23 \\ 22 \end{bmatrix}$$

$$= \begin{bmatrix} 345+506 \\ 184+198 \end{bmatrix} \bmod 26 = \begin{bmatrix} 851 \\ 382 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 \\ 18 \end{bmatrix} = \begin{bmatrix} t \\ s \end{bmatrix}$$

∴ plaintext calculated from formula $P = K^{-1}C \bmod 26$

∴ plaintext = students //