{Hill Ciphering Technique:}

↳ Can encrypt digraph, trigraph or polygraph at once.

let's take sample matrix of 3^{rd} order:

$$\text{Key matrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

{ Key = qubqrbeus
Key = qubqrbeus }

∴ we have taken a 3^{rd} order matrix, so we can go for trigraph solution.

let's convert / cipher:
"National university of computer and emerging sciences".

Cipher Table:

N a t	i o n	a l u	n i v	e r s	i t y
14 1 20	19 15 14	1 12 21	14 9 22	5 18 19	9 20 25

o f c	o m p	u t e	r a n	d e m	e r g
15 6 3	15 13 16	21 20 5	18 1 14	4 5 13	5 18 7

i n g	s c i	e n c	e s s
9 14 7	19 3 9	5 14 3	5 19 19

Now, let's try to implement Hill cipher on first trigraph, i.e 'Nat'.

So, $C = E(K, P) = PK \bmod 26$

$P = D(K, C) = CK^{-1} \bmod 26$

$= PKK^{-1} \bmod 26$

So, $(C_1 C_2 C_3) = (P_1 P_2 P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$

Here :

$(P_1 P_2 P_3) = (nat)$; $(C_1 C_2 C_3) = ?$

↳ plain text ↳ cipher text

in form:

$C = PK \bmod 26$; K = key matrix

$$(C_1 C_2 C_3)_{nat} = (14 \quad 1 \quad 20) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$= (299 \quad 296 \quad 471) \bmod 26$

$= (13 \quad 10 \quad 3) \Rightarrow (m \quad j \quad c)$

So, plain text

(nat) ⟶ (mjc).

Similarly, we convert all of trigraphs.

Scanned with CamScanner

To find determinant:

$$\text{Det(Key)} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

So, after calculating determinant;

$\text{Det(Key)} = -3 \bmod 26$

$\Rightarrow 23$

To find Adjoint of key matrix;

$$\text{Adj of Key} = \begin{pmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} \cancel{17} & \cancel{17} & \cancel{5} & \cancel{17} & \cancel{17} \\ \cancel{21} & 18 & 21 & 21 & 18 \\ \cancel{2} & 2 & 19 & 2 & 2 \\ \cancel{17} & 17 & 5 & 17 & 17 \\ \cancel{21} & 18 & 21 & 21 & 18 \end{pmatrix}$$

→ Perform column wise

→ Enter row wise.

So,

$$= \begin{pmatrix} 18\times19 - 2\times21 & 2\times5 - 17\times19 & 17\times21 - 18\times5 \\ 21\times2 - 19\times21 & 19\times17 - 5\times2 & 5\times21 - 21\times17 \\ 21\times2 - 2\times18 & 2\times17 - 17\times2 & 17\times18 - 21\times17 \end{pmatrix}$$

$$= \begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{pmatrix} \bmod 26$$

$$\text{Adj of key} = \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix}$$

(add mod to neg val)

$$K^{-1} = \frac{1}{|A|} \times \text{Adj of } A$$

$$= \frac{1}{23} \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$\text{or} \quad 23^{-1} \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

find 23^{-1} ??

we, use, Euclidean Algorithm;

$ax = 1 \bmod 26$, $a = 23$,

So, $26 = (1)(23) + (3)$

$23 = (7)(3) + (2)$

$3 = (1)(2) + (1)$.

So,

$1 = 1\cdot 3 - 1(1\cdot 23 - 7\cdot 3)$

$1 = 1\cdot 3 - 1\cdot 23 + 7\cdot 3$

$1 = 8(1\cdot 26 - 1\cdot 23) - 1\cdot 23$

$1 = 8\cdot 26 - 9\cdot 23$

$1 = (8)(26) + (-9)(23)$

So,

$x = -9 + 26 = 17$

So, $23^{-1} = 17$

So,

$$K^{-1} = 17 \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$

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

Before proceeding verify K^{-1} by $KK^{-1} = I$

or => $(KK^{-1}) \bmod 26 = I$

Formula for decryption:

$P = CK^{-1} \bmod 26$

$$P = \begin{pmatrix} 13 & 10 & 3 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 274 & 287 & 306 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 14 & 1 & 20 \end{pmatrix}$$

= (nat)

↳ This was our original plain text & we decrypted.

similary all trigraphs can be encrypted and decrypted via same technique.

Scanned with CamScanner