Hill cipher 2D Encryption

$P = HeIP \qquad K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$C = K \cdot P \bmod 26$

$P = \underset{7\ 4}{He}\ \underline{IP} \longrightarrow \begin{bmatrix} 11 \\ 15 \end{bmatrix}$

$\downarrow \begin{bmatrix} 7 \\ 4 \end{bmatrix}$

$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}$$

$$= \begin{bmatrix} 33 & 78 \\ 34 & 97 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 & 0 \\ 8 & 19 \end{bmatrix}$$

$C = \boxed{HIaT}$

Decryption

$C = HIAT$

$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

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

How To get inverse of 2x2

$K^{-1} = \frac{1}{|K|} \text{ adj } K$

$|K| = 3 \times 5 - 3 \times 2 = 15 - 6 = 9$

adj K

$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\text{adj } K = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

(3)

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$adj(K) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

for (-ve) values add multiple of 26 to be the

$$adj(K) = \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

$$K^{-1} = \left(\frac{1}{9}\right)\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

To get mode of fracti

number

$n = \left(\frac{1}{9}\right) \bmod 26$

$9n = 1 \pmod{26}$

find The value of n That satisfy equation

if $n = 1$

$9 \times 1 = 9 \bmod 26 = 9 \neq 1$

if $n = 2$

$9 \times 2 = 18 \bmod 26 = 18 \neq 1$

if $n = 3$

$9 \times 3 = 27 \bmod 26 = 1$ ✓

$\therefore \frac{1}{9} \bmod 26 = 3$

$$K^{-1} = 3 \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

(5)

$$K^{-1} = \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$P = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \cdot \begin{bmatrix} 7 & 0 \\ 8 & 19 \end{bmatrix}$$

$$= \begin{bmatrix} 105+136 & 323 \\ 140+72 & 171 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}$$

$$\boxed{H \; E \; L \; P}$$