1

Hill cipher 3X3 Encryption

$$C = K \cdot P \mod 26$$

$$K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

P = ACT

$$C = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \mod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

$$C = \boxed{POH}$$

Decryption

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

How to get inverse of K

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

$$K = \begin{array}{ccc} + & - & + \\ \end{array}$$
$$K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

$|K| = ?$

$$|K| = \Big(6(16 \times 15 - 17 \times 10) - 24(13 \times 15 - 20 \times 10) + 1(13 \times 17 - 20 \times 16) \Big)$$

$$= 6 \times 70 - 24 \times (-5) + 1 \times -99$$

$$= 441$$

adj(A)

$$A = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

- Repeat The first and second column & row.

$$\begin{bmatrix} 6 & 24 & 1 & 6 & 24 \\ 13 & 16 & 10 & 13 & 16 \\ 20 & 17 & 15 & 20 & 17 \\ 6 & 24 & 1 & 6 & 24 \\ 13 & 16 & 10 & 13 & 16 \end{bmatrix}$$

(2) Remove 1st column & 1st row

$$\text{adj}(K) = \begin{bmatrix} 16\times15 - 17\times10 & 17\times1 - 24\times15 & 24\times10 - 16\times1 \\ 10\times20 - 13\times15 & 15\times6 - 20\times1 & 1\times13 - 6\times10 \\ 13\times17 - 16\times20 & 20\times24 - 6\times17 & 6\times16 - 13\times24 \end{bmatrix}$$

$$= \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix}$$

③ Remove (-ve) by adding multiple of (26)

$-343 \longrightarrow 21$

$-47 \longrightarrow 5$

$-99 \longrightarrow 5$

$-216 \longrightarrow 18$

5

$$adj = \begin{bmatrix} 70 & 21 & 224 \\ 5 & 70 & 5 \\ 5 & 378 & 18 \end{bmatrix}$$

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

$$\frac{1}{|K|} = \frac{1}{441} \bmod 26$$

$$n = \frac{1}{441} \bmod 26$$

$$441 \cdot n = 1 \bmod (26)$$

$n = 1$

$441 \bmod 26 = 25$ ×

$n = 2$

$441 \times 2 \bmod 26 = 24$

at $n = 25$

$441 \times 25 \bmod 26 = 1$ ✓

$$\frac{1}{441} \bmod 26 = 25$$

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

$$= 25 \cdot \begin{bmatrix} 70 & 21 & 224 \\ 5 & 70 & 5 \\ 5 & 378 & 18 \end{bmatrix}$$

$$= \begin{bmatrix} 1750 & 525 & 5600 \\ 125 & 1750 & 125 \\ 125 & 9450 & 450 \end{bmatrix}$$

mod 26

$$K^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Scanned with CamScanner

7

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

$$= \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \mod 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

$$\boxed{P = a\,c\,T}$$