Q. Encrypt the plaintext "messages" using Hill cipher for the given key: "ciphering"

Sol:

1. **Key = "ciphering"**

$$k = \begin{bmatrix} c & i & p \\ h & e & r \\ i & n & g \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$$

2. **plaintext = "messages"**

$$P = \begin{bmatrix} m & e & s \\ s & a & g \\ e & s & x \end{bmatrix} = \begin{bmatrix} 12 & 4 & 18 \\ 18 & 0 & 6 \\ 4 & 18 & 23 \end{bmatrix}$$

3. **Encryption:**

$C_i = (P_i * k) \bmod 26$

$C_1 = (P_1 * k) \bmod 26$

$$\mathbf{C_1} = [12 \quad 4 \quad 18] * \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \bmod 26$$

$$= [\ (12*2)+(4*7)+(18*8) \quad (12*8)+(4*4)+(18*13) \quad (12*15)+(4*17)+(18*6)\ ] \bmod 26$$

$$= [196 \quad 346 \quad 356] \bmod 26$$

$$= [14 \quad 8 \quad 18]$$

$$= [o \quad i \quad s]$$

$$\mathbf{C_2} = [18 \quad 0 \quad 6] * \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \bmod 26$$

$$= [\ (18*2)+(0*7)+(6*8) \quad (18*8)+(0*4)+(6*13) \quad (18*15)+(0*17)+(6*6)\ ] \bmod 26$$

$$= [84 \quad 222 \quad 306] \bmod 26$$

$$= [6 \quad 14 \quad 20]$$

$$= [g \quad o \quad u]$$

$$C_3 = \begin{bmatrix} 4 & 18 & 23 \end{bmatrix} * \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \text{ mod } 26$$

$$= [\ (4*2)+(18*7)+(23*8) \quad (4*8)+(18*4)+(23*13) \quad (4*15)+(18*17)+(23*6)\ ] \text{ mod } 26$$

$$= [\ 318 \quad 403 \quad 504\ ] \text{ mod } 26$$

$$= [\ 6 \quad 13 \quad 10\ ]$$

$$= [\ g \quad n \quad k\ ]$$

Ciphertext: $C = \begin{bmatrix} o & i & s \\ g & o & u \\ g & n & k \end{bmatrix}$

4. Decryption:

$$\mathbf{P_i = (C_i * k^{-1}) \text{ mod } 26}$$

$$\mathbf{k^{-1} = \frac{1}{|d|} * Adj\ (k) \qquad OR \qquad k^{-1} = d^{-1} * Adj\ (k)}$$

1. Calculating determinant: $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

$= (2 * (4*6 – 13*17) – 8 * (7*6 – 8*17) + 15 * (7*13 - 8*4))$ mod 26
$= (-394 + 752 + 885)$ mod 26
$= 1243$ mod 26
$= 21$

2. Finding multiplicative inverse:

$d * d^{-1} \equiv 1 \text{ mod } 26$
$21 * x \equiv 1 \text{ mod } 26$
$21 * 5 = 105 \equiv 1 \text{ mod } 26$
$x = 5$

3. Adjoint of matrix:

$$\text{Adj k} = [\ \text{cof}(a_{ij})]^T = \begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}^T$$

$$= \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 11 & 17 & 24 \\ 16 & 22 & 19 \\ 7 & 12 & 4 \end{bmatrix}$$

4. Finalizing: $k^{-1} = d^{-1} * \text{Adj } k$

$$= 5 * \begin{bmatrix} 11 & 17 & 24 \\ 16 & 22 & 19 \\ 7 & 12 & 4 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 55 & 85 & 120 \\ 80 & 110 & 95 \\ 35 & 60 & 20 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

5. Verifying: $(k * k^{-1})$ mod 26 = I

$$= \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 157 & 182 & 468 \\ 182 & 209 & 520 \\ 104 & 182 & 469 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$P_i = (C_i * k^{-1})$ mod 26

$P_1 = (C_1 * k^{-1})$ mod 26

$$\mathbf{P_1} = [14 \quad 8 \quad 18] * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= [220 \quad 290 \quad 720] \text{ mod } 26$$

$$= [12 \quad 4 \quad 18]$$

$$= [m \quad e \quad s]$$

$$\mathbf{P_2} = [6 \quad 14 \quad 20] * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= [226 \quad 286 \quad 734] \text{ mod } 26$$

$$= [18 \quad 0 \quad 6]$$

$$= [s \quad a \quad g]$$

$$\mathbf{P_3} = [6 \quad 13 \quad 10] * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= [134 \quad 200 \quad 517] \text{ mod } 26$$

$$= [4 \quad 18 \quad 23]$$

$$= [e \quad s \quad x]$$

$$P = \begin{bmatrix} m & e & s \\ s & a & g \\ e & s & x \end{bmatrix}$$

2nd approach:

1. **Key = "ciphering"**

$$k = \begin{bmatrix} c & i & p \\ h & e & r \\ i & n & g \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$$

2. **plaintext = "messages"**

$$P = \begin{bmatrix} m & s & e \\ e & a & s \\ s & g & x \end{bmatrix} = \begin{bmatrix} 12 & 18 & 4 \\ 4 & 0 & 18 \\ 18 & 6 & 23 \end{bmatrix}$$

3. **Encryption:**

$C_i = (P_i * k)$ mod 26

$C_1 = (P_1 * k)$ mod 26

$$\mathbf{C_1} = \begin{bmatrix} 12 \\ 4 \\ 18 \end{bmatrix} * \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} (12*2) + (4*8) + (18*15) \\ (12*7) + (4*4) + (18*17) \\ (12*8) + (4*13) + (18*6) \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 326 \\ 406 \\ 256 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 14 \\ 16 \\ 22 \end{bmatrix} \quad = \begin{bmatrix} o \\ q \\ w \end{bmatrix}$$

$$\mathbf{C_2} = \begin{bmatrix} 18 \\ 0 \\ 6 \end{bmatrix} * \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} (18*2)+(0*8)+(6*15) \\ (18*7)+(0*4)+(6*17) \\ (18*8)+(0*13)+(6*6) \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 126 \\ 228 \\ 180 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 22 \\ 20 \\ 24 \end{bmatrix} \quad = \begin{bmatrix} w \\ u \\ y \end{bmatrix}$$

$$\mathbf{C_3} = \begin{bmatrix} 4 \\ 18 \\ 23 \end{bmatrix} * \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} (4*2)+(18*8)+(23*15) \\ (4*7)+(18*4)+(23*17) \\ (4*8)+(18*13)+(23*6) \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 497 \\ 491 \\ 404 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3 \\ 23 \\ 14 \end{bmatrix} \quad = \begin{bmatrix} d \\ x \\ o \end{bmatrix}$$

Ciphertext: $C = \begin{bmatrix} o & w & d \\ q & u & x \\ w & y & o \end{bmatrix}$

5. Decryption:

$\mathbf{P_i = (C_i * k^{-1}) \text{ mod } 26}$

$\mathbf{k^{-1} = \frac{1}{|d|} * Adj(k)}$ **OR** $\mathbf{k^{-1} = d^{-1} * Adj(k)}$

1. Calculating determinant: $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

$= (2 * (4*6 – 13*17) – 8 * (7*6 – 8*17) + 15 * (7*13 - 8*4)) \bmod 26$
$= (-394 + 752 + 885) \bmod 26$
$= 1243 \bmod 26$
$= 21$

2. Finding multiplicative inverse:
$d * d^{-1} \equiv 1 \bmod 26$
$21 * x \equiv 1 \bmod 26$
$21 * 5 = 105 \equiv 1 \bmod 26$
$x = 5$

3. Adjoint of matrix:

$$\text{Adj } k = [\ \text{cof}(a_{ij})]^T = \begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}^T$$

$$= \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 11 & 17 & 24 \\ 16 & 22 & 19 \\ 7 & 12 & 4 \end{bmatrix}$$

4. Finalizing: $k^{-1} = d^{-1} * \text{Adj } k$

$$= 5 * \begin{bmatrix} 11 & 17 & 24 \\ 16 & 22 & 19 \\ 7 & 12 & 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 55 & 85 & 120 \\ 80 & 110 & 95 \\ 35 & 60 & 20 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

5. Verifying: $(k * k^{-1}) \bmod 26 = I$

$$= \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 157 & 182 & 468 \\ 182 & 209 & 520 \\ 104 & 182 & 469 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

P_i = (C_i * k^{-1}) mod 26
P_1 = (C_1 * k^{-1}) mod 26

$$\mathbf{P_1} = \begin{bmatrix} 14 \\ 16 \\ 22 \end{bmatrix} * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 506 \\ 498 \\ 694 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 12 \\ 4 \\ 18 \end{bmatrix} = \begin{bmatrix} m \\ e \\ s \end{bmatrix}$$

$$\mathbf{P_2} = \begin{bmatrix} 22 \\ 20 \\ 24 \end{bmatrix} * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 590 \\ 572 \\ 838 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 18 \\ 0 \\ 6 \end{bmatrix} = \begin{bmatrix} s \\ a \\ g \end{bmatrix}$$

$$\mathbf{P_3} = \begin{bmatrix} 3 \\ 23 \\ 14 \end{bmatrix} * \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 394 \\ 382 \\ 491 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 4 \\ 18 \\ 23 \end{bmatrix} = \begin{bmatrix} e \\ s \\ x \end{bmatrix}$$

$$P = \begin{bmatrix} m & s & e \\ e & a & s \\ s & g & x \end{bmatrix}$$