

K = randomly generated matrix (key)

$$\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$$

Plaintext Message = CODE

$$\begin{bmatrix} C & D \\ O & E \end{bmatrix} \rightarrow \begin{bmatrix} C \\ O \end{bmatrix} \begin{bmatrix} D \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 2 \\ 14 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$\swarrow \quad \swarrow$
 $B_1 \quad B_2$

Encryption

Getting Cipher text

$$C_n = K \cdot B_n$$

Encrypted Message = SIKR

$$C_1 = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \times \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 18 \\ 34 \end{bmatrix} \xrightarrow{\text{mod } 26} \begin{bmatrix} 18 \\ 8 \end{bmatrix} \rightarrow \begin{bmatrix} S \\ I \end{bmatrix}$$

\nwarrow
 C_1

$$C_2 = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \times \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 10 \\ 17 \end{bmatrix} \xrightarrow{\text{mod } 26} \begin{bmatrix} 10 \\ 17 \end{bmatrix} \rightarrow \begin{bmatrix} K \\ R \end{bmatrix}$$

\nwarrow
 C_2

Decryption

$$D(K, C_n) = (K^{-1} \cdot C_n)$$

$$K^{-1} = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$$

Decrypted Message = CODE

$$K^{-1} \cdot C_1 = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} \times \begin{bmatrix} 18 \\ 34 \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} C \\ O \end{bmatrix}$$

$$K^{-1} \cdot C_2 = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} \times \begin{bmatrix} 10 \\ 17 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} D \\ E \end{bmatrix}$$