

# Hill cipher (Transforms m plaintext to m ciphertext)

( $a=0, b=1, \dots, z=25$ )

Example:-  $m=3$

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \underbrace{\begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}}_{K \text{ is } 3 \times 3 \text{ matrix if } m=3} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \pmod{26}$$

Plaintext : Pay more money  
 ①      ②      ③      ④

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Step ① :-

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \rightarrow p \\ 0 \rightarrow a \\ 24 \rightarrow y \end{bmatrix} = \begin{bmatrix} 17 \cdot 15 + 17 \cdot 0 + 5 \cdot 24 \\ 21 \cdot 15 + 18 \cdot 0 + 21 \cdot 24 \\ 2 \cdot 15 + 2 \cdot 0 + 19 \cdot 24 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \pmod{26} = \begin{bmatrix} 11 \rightarrow L \\ 13 \rightarrow N \\ 18 \rightarrow S \end{bmatrix}$$

Step ②

$$\begin{bmatrix} C_4 \\ C_5 \\ C_6 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 12 \rightarrow m \\ 14 \rightarrow o \pmod{26} \\ 17 \rightarrow z \end{bmatrix} = \begin{bmatrix} 7 \\ 3 \\ 11 \end{bmatrix} \begin{matrix} H \\ D \\ L \end{matrix}$$

Step ③

$$\begin{bmatrix} C_7 \\ C_8 \\ C_9 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 4 \rightarrow e \\ 12 \rightarrow m \pmod{26} \\ 14 \rightarrow o \end{bmatrix} = \begin{bmatrix} 4 \\ 22 \\ 12 \end{bmatrix} \begin{matrix} E \\ W \\ M \end{matrix}$$

Step ④

$$\begin{bmatrix} C_{10} \\ C_{11} \\ C_{12} \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 13 \rightarrow n \\ 4 \rightarrow e \pmod{26} \\ 24 \rightarrow y \end{bmatrix} = \begin{bmatrix} 19 \\ 17 \\ 22 \end{bmatrix} \begin{matrix} T \\ R \\ W \end{matrix}$$

Plaintext : Pay more money  
 Ciphertext : LNS HDLEWMTRW