Hill Cipher

Hill Cipher

- Hill cipher, developed by the mathematician Lester Hill in 1929

$$\mathbf{M}(\mathbf{M}^{-1}) = \mathbf{M}^{-1}\mathbf{M} = \mathbf{I},$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

- Hill system can be expressed as :

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

-

Hill Cipher

Keyword : hill

ciphertext : APAD

Keyword matrix

$$K = \begin{bmatrix} h & i \\ l & l \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

$$|K| = 7 \times 11 - 8 \times 11 = 77 - 88 = -11$$

$$= \underline{15 \bmod 26}$$

Hill Cipher

$KK^{-1} = 1 \mod 26$

$\therefore 15 \times x = 1 \mod 26$

$15 \times 7 = 105 = 1 \mod 26$

$Adj(K) = Adj\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$

Hill Cipher

$M_{11} = 11$

$M_{12} = -11$

$M_{21} = -8$

$M_{22} = +7$

$$\begin{bmatrix} 11 & -11 \\ -8 & 7 \end{bmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

If a square matrix A has a nonzero determinant, then the inverse of the matrix is computed as $(A^{-1})_{ij} = (\det A)^{-1}(-1)^{i+j}(D_{ji})$ where D_{ji} the subdeterminant formed by

Hill Cipher

deleting the j^{th} row and i^{th} column of A

$$K^{-1} = \frac{\text{Adj } K}{|K|} = 7\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \bmod 26$$

Hill Cipher

$$C = PK \bmod 26$$

$$\therefore \cancel{C K^{-1} = P \bmod 26}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ P \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 15 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{pmatrix} = \begin{pmatrix} 330 \\ 345 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 18 \\ 7 \end{pmatrix} \bmod 26$$

$$= \underline{\begin{pmatrix} S \\ h \end{pmatrix}}$$

Hill Cipher

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ D \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$= \begin{pmatrix} 25\times 0 + 22\times 3 \\ 1\times 0 + 23\times 3 \end{pmatrix} = \begin{pmatrix} 66 \\ 69 \end{pmatrix} \bmod 26 = \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$= \begin{pmatrix} O \\ R \end{pmatrix}$$

$\therefore$ plaintext = SLOR