Hill Cipher

Dr.N.Gopika Rani,
Assistant Professor (SG),
Department of CSE

Introduction

- Hill cipher is a polygraphic substitution cipher based on linear algebra.
- Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher.
- To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

Example

- Input :

Plaintext: ACT

Key: GYBNQKURP

Encryption

- We have to encrypt the message ‘ACT’ (n=3).
- The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\text{Key} : \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \qquad \text{ACT} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Encryption

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

- which corresponds to ciphertext of 'POH'

Decryption

To decrypt the message, the ciphertext is turned back into a vector, then simply multiply by the inverse matrix of the key matrix

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

which gives us back ‘ACT’.

Thank You