NIS LAB6

Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Hill Cipher

- Polyalphabetic cipher
- Invented by Lester S. Hill
- The plain text is divided into equal-size blocks.
- The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block.
- For this reason, the Hill cipher belongs to a category of ciphers called block ciphers.

- In a Hill cipher, the key is a square matrix of size m x m in which m is the size of the block.
- If we call the key matrix K, each element of the matrix is $K_{i,j}$

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

- How one block of the ciphertext is encrypted.
- If we call the m characters in the plaintext block $P_1, P_2, \ldots. P_m$, the corresponding characters in the cipher text block are C_1, C_2, ...C_m.

$C_1 = P_1 K_{11} + P_2 K_{21} + ..+P_m K_{m1}$

$C_2 = P_1 K_{12} + P_2 K_{22} + ..+P_m K_{m2}$

$C_m = P_1 K_{11} + P_2 K_{2m} + ..+P_m K_{mm}$

- Note- Not all square matrices have multiplicative inverse in Z_{26}
- Bob will not be able to decrypt the cipher text sent by Alice if the matrix does not have a multiplicative inverse.

Example

Plain text: code is ready

Matrix representation of plain text cam make 3 x 4 matrix when adding extra bogus character z to the last block and removing the spaces.

$$\begin{pmatrix} c & o & d & e \\ i & s & r & e \\ a & d & y & z \end{pmatrix} \qquad \begin{pmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{pmatrix}$$

$$P = \begin{pmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{pmatrix}$$

$$K = \begin{pmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{pmatrix}$$

$$C \begin{pmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 05 & 08 & 18 & 18 \end{pmatrix}$$

$$C_1 = P_1 K_{11} + P_2 K_{21} + P_3 K_{31} + P_4 K_{41}$$

$$C_1 = (2)(9) + (14)(4) + (3)(2) + (4)(3)$$

$$= 18 + 56 + 6 + 12$$

$$= 92 \bmod 26$$

$$= 14$$

- Decryption

$$
\begin{pmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{pmatrix} = \begin{pmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 05 & 08 & 18 & 18 \end{pmatrix} \begin{pmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 03 & 23 & 21 & 08 \end{pmatrix}
$$

$$
\qquad P \qquad\qquad\qquad\qquad C \qquad\qquad\qquad\qquad K^{-1}
$$

- $A^{-1} = 1/ |A| * adj (A)$