Semester: VI Subject: CGS Academic Year: 2023-2024.

HILL CIPHER:

Hill Cipher in cryptography was invented and developed in 1929 by Lester S. Hill, a renowned American mathematician.

It represents polygraphic substitution cipher.

The way Hill Cipher works is explained below:-

Step1: Treat every letter in the plaintext message as a number such that A=00, B=01, ..., Z=25.

Step2: Organize the plaintext message as a matrix of numbers based on the above conversion. It can be digraphs, trigraphs (three-letter blocks), or any multiple-sized blocks for building a uniform cipher.

~~The way Hill Cipher works is explained below.~~

Step3: The plaintext matrix is multiplied by a matrix of randomly chosen keys.

Step4: Now, multiply two matrices.

Step5: Compute a modulo 26 value of the above matrix.

Step6: Translate the numbers to alphabets.

Decryption:-

Step1: Take the ciphertext matrix and multiply it by the inverse of original key matrix.

Step2: After this take modulo 26 of this matrix.

Step3: Translate the numbers to alphabets. The original plain Text is retrieved successfully.

Semester: VI Subject: CSS Academic Year: 2023-2024

Example:

Use a Hill Cipher to encipher the message "Attack At Dawn". Use the following key $K = \begin{pmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{pmatrix}$

Solution:-

The key matrix consists of size 3x3, where 3 is the number of rows in the plaintext. Hence, we divide the given plaintext in matrix of size 1x3 as below:

$$\begin{bmatrix} A \\ T \\ T \end{bmatrix}, \begin{bmatrix} A \\ C \\ K \end{bmatrix}, \begin{bmatrix} A \\ T \\ D \end{bmatrix}, \begin{bmatrix} A \\ W \\ N \end{bmatrix}$$

Now organize the plaintext message as a matrix of numbers.

$$\begin{bmatrix} 00 \\ 19 \\ 19 \end{bmatrix}, \begin{bmatrix} 00 \\ 02 \\ 10 \end{bmatrix}, \begin{bmatrix} 00 \\ 19 \\ 03 \end{bmatrix}, \begin{bmatrix} 00 \\ 22 \\ 13 \end{bmatrix}$$

Now, multiply each plaintext matrix with the key matrix and perform modulo 26 operations on the product:

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \times \begin{bmatrix} 00 \\ 19 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 171 \bmod 26 \\ 57 \bmod 26 \\ 456 \bmod 26 \end{bmatrix} = \begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} = \begin{matrix} P \\ F \\ O \end{matrix}$$

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \times \begin{bmatrix} 00 \\ 02 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 58 \bmod 26 \\ 14 \bmod 26 \\ 104 \bmod 26 \end{bmatrix} = \begin{bmatrix} 6 \\ 14 \\ 00 \end{bmatrix} = \begin{matrix} G \\ O \\ A \end{matrix}$$

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \times \begin{bmatrix} 00 \\ 19 \\ 03 \end{bmatrix} \bmod 26 = \begin{bmatrix} 91 \bmod 26 \\ 41 \bmod 26 \\ 344 \bmod 26 \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \\ 06 \end{bmatrix} = \begin{matrix} N \\ P \\ G \end{matrix}$$

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \times \begin{bmatrix} 00 \\ 22 \\ 13 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 153 \text{ mod } 26 \\ 57 \text{ mod } 26 \\ 465 \text{ mod } 26 \end{bmatrix} = \begin{bmatrix} 23 \\ 5 \\ 23 \end{bmatrix} = \begin{matrix} X \\ F \\ X \end{matrix}.$$

The result is "PFOGDANPGXFX".

Example 2:

Use a Hill cipher to encipher the message "WE LIVE IN AN INSECURE WORLD". Use the following key. $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

Solution :-

The key matrix consists of size 2x2, where 2 is the number of rows in the plaintext. Hence, we divide the given plaintext in matrix of size 1x2 as below.

$$\begin{pmatrix} W \\ E \end{pmatrix}, \begin{pmatrix} L \\ I \end{pmatrix}, \begin{pmatrix} V \\ E \end{pmatrix}, \begin{pmatrix} I \\ N \end{pmatrix}, \begin{pmatrix} A \\ N \end{pmatrix}, \begin{pmatrix} I \\ N \end{pmatrix}, \begin{pmatrix} S \\ E \end{pmatrix}, \begin{pmatrix} C \\ U \end{pmatrix}, \begin{pmatrix} R \\ E \end{pmatrix}, \begin{pmatrix} W \\ O \end{pmatrix}, \begin{pmatrix} R \\ L \end{pmatrix}, \begin{pmatrix} D \\ Z \end{pmatrix}.$$

Now organize the plaintext message as a matrix of numbers.

$$\begin{pmatrix} 22 \\ 04 \end{pmatrix}, \begin{pmatrix} 11 \\ 08 \end{pmatrix}, \begin{pmatrix} 21 \\ 04 \end{pmatrix}, \begin{pmatrix} 08 \\ 13 \end{pmatrix}, \begin{pmatrix} 00 \\ 13 \end{pmatrix}, \begin{pmatrix} 08 \\ 13 \end{pmatrix}, \begin{pmatrix} 18 \\ 04 \end{pmatrix}, \begin{pmatrix} 02 \\ 20 \end{pmatrix}, \begin{pmatrix} 17 \\ 04 \end{pmatrix}, \begin{pmatrix} 22 \\ 14 \end{pmatrix}, \begin{pmatrix} 17 \\ 11 \end{pmatrix}, \begin{pmatrix} 03 \\ 25 \end{pmatrix}$$

Now, multiply each plaintext matrix with the key matrix and perform modulo 26 operations on the product.

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 22 \\ 04 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 74 \text{ mod } 26 \\ 138 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 22 \\ 8 \end{pmatrix} = \begin{pmatrix} W \\ I \end{pmatrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 11 \\ 08 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 49 \text{ mod } 26 \\ 111 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 23 \\ 7 \end{pmatrix} = \begin{pmatrix} X \\ H \end{pmatrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 21 \\ 04 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 71 \text{ mod } 26 \\ 133 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 19 \\ 3 \end{pmatrix} = \begin{pmatrix} T \\ D \end{pmatrix}$$

Semester : VI Subject : CSS Academic Year: 2023-2024.

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 8 \\ 13 \end{pmatrix} \bmod 26 = \begin{pmatrix} 50 \bmod 26 \\ 131 \bmod 26 \end{pmatrix} = \begin{pmatrix} 24 \\ 01 \end{pmatrix} = \begin{matrix} Y \\ B \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 0 \\ 13 \end{pmatrix} \bmod 26 = \begin{pmatrix} 26 \bmod 26 \\ 91 \bmod 26 \end{pmatrix} = \begin{pmatrix} 0 \\ 13 \end{pmatrix} = \begin{matrix} A \\ N \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 08 \\ 13 \end{pmatrix} \bmod 26 = \begin{pmatrix} 50 \bmod 26 \\ 131 \bmod 26 \end{pmatrix} = \begin{pmatrix} 24 \\ 01 \end{pmatrix} = \begin{matrix} Y \\ B \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 18 \\ 04 \end{pmatrix} \bmod 26 = \begin{pmatrix} 62 \bmod 26 \\ 118 \bmod 26 \end{pmatrix} = \begin{pmatrix} 10 \\ 4 \end{pmatrix} = \begin{matrix} K \\ O \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 02 \\ 20 \end{pmatrix} \bmod 26 = \begin{pmatrix} 46 \bmod 26 \\ 150 \bmod 26 \end{pmatrix} = \begin{pmatrix} 20 \\ 20 \end{pmatrix} = \begin{matrix} U \\ U \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 17 \\ 04 \end{pmatrix} \bmod 26 = \begin{pmatrix} 59 \bmod 26 \\ 113 \bmod 26 \end{pmatrix} = \begin{pmatrix} 7 \\ 9 \end{pmatrix} = \begin{matrix} H \\ J \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 22 \\ 14 \end{pmatrix} \bmod 26 = \begin{pmatrix} 16 \bmod 26 \\ 208 \bmod 26 \end{pmatrix} = \begin{pmatrix} 16 \\ 00 \end{pmatrix} = \begin{matrix} Q \\ A \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 17 \\ 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 73 \bmod 26 \\ 162 \bmod 26 \end{pmatrix} = \begin{pmatrix} 21 \\ 6 \end{pmatrix} = \begin{matrix} V \\ G \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 03 \\ 25 \end{pmatrix} \bmod 26 = \begin{pmatrix} 59 \bmod 26 \\ 190 \bmod 26 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{matrix} H \\ I \end{matrix}$$

The result is "WIXHTDYBANYBKOUUHJQAVGHI".