Practical No. 3

Aim: To implement Hill Cipher Substitution Techniques:

Date :

Practical No. 3

Aim: To implement Hill Cipher Substitution Techniques.

Theory:

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 (consider as an n-component vector) is multiplied by an invertible n x n matrix, against modulus 26. To decrypted the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n x n matrix -- (modulo 26)

Algorithm:

1. Organize character alphabetically with numeric A→1, B→2, ... Z→26 or in ASCII (256 characters)
2. Create a key matrix measuring m x m
3. matrix K is an invertible matrix that has multiplicative inverse K-1 so that K. K-1 = 1
4. Plaintext P = P1 P2 ... Pn, blocked with the same size as the row or column K.
5. Transpose matrix P and became
6. multiply matrix K with transposed P in modulo 26 or 256
7. Then transpose to
8. change the result of step 7 into the alphabet using alphabetical correspondence with numeric in step 1 to obtain the ciphertext.

Date :

Example :

Sample Input :

Message : ACT

Key : GYBNQKURP

Sample Output :

Cipher text : POH

Conclusion :

The concept of Hill Cipher is implemented successfully.

Viva Questions :

1. What is Hill Cipher ?

→ The Hill Cipher is also a block cipher, it is based on linear algebra and use matrix multiplication and matrix inverse as well as rules for modulo arithmetic. It is used to encrypt and decrypt data for purpose of data security.

2. What are advantages of Hill Cipher ?

→ (1) Hill Cipher provides higher level of security compared to other Substitution cipher as it operates on blocks of letter rather than individual letters.

(2) High speed and High throughput.

(3) Simplicity because of using basic matrix operations.

3. What is disadvantage of Hill Cipher ?

→ (1) Vulnerable to known-plaintext attacks

(2) The hill cipher's performance might be affected when dealing with larger texts, as it requires matrix operations that can become computationally intensive.

(3) Limited applicability to only alphabetic character

(4) Vulnerable to frequency analysis attack