PRIYADARSHINI COLLEGE OF ENGINEERING
(Recognised by A.I.C.T.E., New Delhi & Govt. of Maharashtra, Affiliated to R.T.M.Nagpur University)Near CRPF Campus, Hingna Road, Nagpur-440 019, Maharashtra (India)
Phone : 07104 - 236381, 237307, Fax : 07104 - 237681,

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 (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt 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 × n matrices (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 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.

Example:

Sample Input :

Message: ACT
Key: GYBNQKURP

Sample Output:

Cipher text: POH

Conclusion:
The concept of Hill cipher is implemented sucessfully.

Q. 1 What is Hill Cipher?
Q. 2 What are advantages of Hill Cipher?
Q. 3 What is disadvantage of Hill Cipher ?