Exp No: 2

Hill Cipher

Aim

To implement encryption and decryption using Hill cipher substitution technique

Algorithm

1. Obtain a plain text message to encode in Standard English with no spaces.

2. Split the plain text into group of length three. To fill this, add X at the end.

3. Convert each group of letters with length three into plain text vectors.

4. Replace each letter by the number corresponding to its position in the alphabet i.e. A=1, B=2, C=3…Z=0.

5. Create the key word in a 3*3 matrix.

6. Multiply the two matrices to obtain the cipher text of length three.

7. For decryption, convert each entry in the cipher text vector into its plain text vector by multiplying the cipher text vector and inverse of a matrix.

8. Thus plaintext is obtained from the corresponding plaintext vector by corresponding position in the alphabet.

SAMPLE INPUT & OUTPUT:

1)

Enter the Plain text for Encryption:

Analytics

Padded Text:ANALYTICS

Encrypted Message: ANATCAWGE

Decrypted Message: ANALYTICS

2)

Enter the Plain text for Encryption:

velloreinstituteoftechnology

Padded Text:VELLOREINSTITUTEOFTECHNOLOGYXX

Encrypted Message: ZYOVUEUGHUFMTGAQILFCDJDVZYTMHP

Decrypted Message: VELLOREINSTITUTEOFTECHNOLOGYXX