**NIRMA UNIVERSITY**

**Institute of Technology**

**B.Tech. Computer Science and Engineering**

**2CSDE54 Information and Network Security**

Perform encryption, decryption using the following substitution techniques

1. Playfair
2. Hill Cipher

The **Playfair Cipher** Encryption Algorithm:

The Algorithm consists of 2 steps:

* + - 1. Generate the key square:

1. The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
2. The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.
3. Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

**PlainText: "instruments"**

**After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'**

Plain Text: **“hello”**

After Split: **‘he’ ‘lx’ ‘lo’**

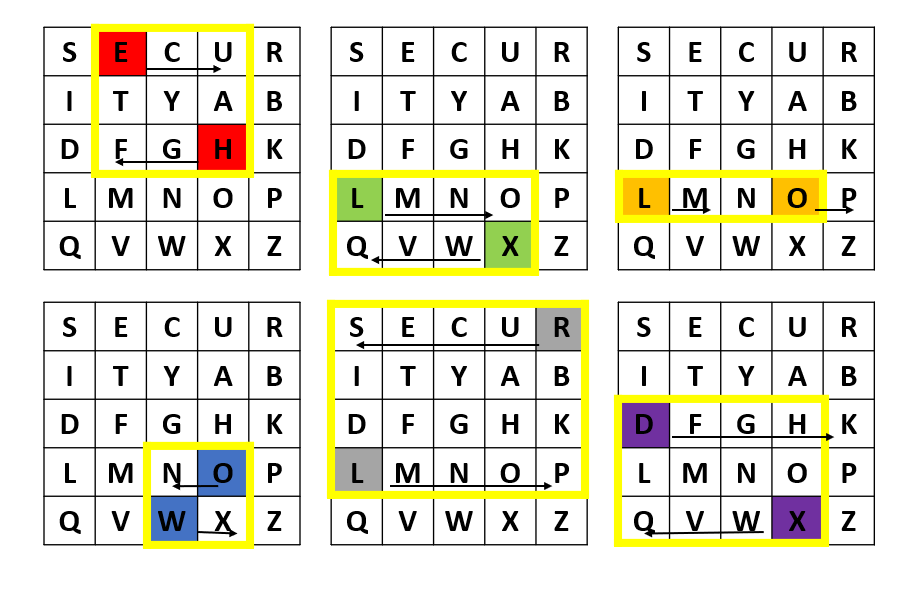
Plain Text: **“helloe”**

AfterSplit: **‘he’ ‘lx’ ‘lo’ ‘ex’**

**Rules for Encryption:**

1. If both letters in the pair are in the same row of the key square, we replace each letter with the letter to its right (wrapping around if necessary).
2. If both letters in the pair are in the same column of the key square, we replace each letter with the letter below it (wrapping around if necessary).
3. If the letters are in different rows and columns, we form a rectangle with the pair and replace each letter with the letter at the rectangle’s opposite corner (moving only left or right).

Using the matrix with the keyword SECURITY, let?s find the row and column of each pair and apply the encryption rules to HELLOWORLD, whose pairs are HE LX LO WO RL DX:

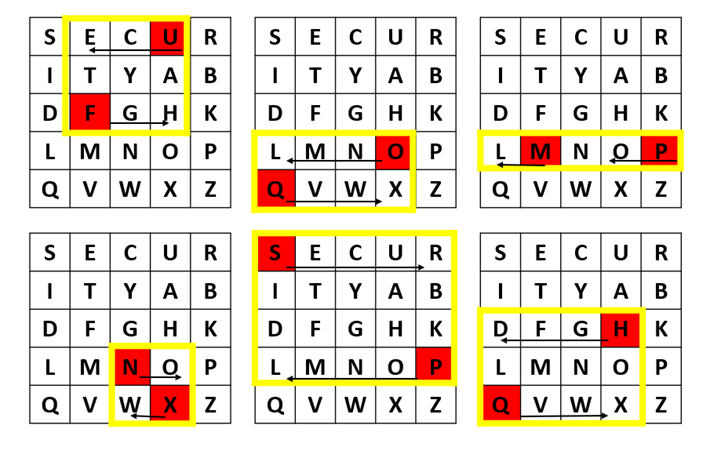


After applying the encryption rules to all the letter pairs, we get FUOQMPXNSPHQ.

**Decryption rule:** The decryption rules are reverse encryption rules.

Let’s decrypt the message FUOQMPXNSPHQ using these decryption rules.

The pairs are:



At this point, we have HELXLOWORLDX. After dealing with Xs, we get HELLOWORLD

**Instruction:** You need to take the **input.txt** file and generate the cipher text in the **output.txt**

**Hill cipher:** 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).

**Input :** Plaintext: ACT

Key: GYBNQKURP

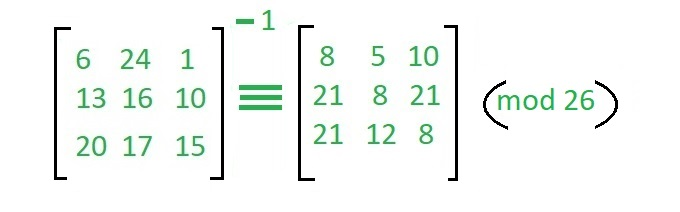
**Output :** Ciphertext: POH

We have to encrypt the message ‘ACT’ (n=3).

|  |  |
| --- | --- |
| The key is ‘GYBNQKURP’ which can be written as the nxn matrix Lightbox | The message ‘ACT’ is written as vector: Lightbox |
| The enciphered vector is given as: which corresponds to ciphertext of ‘POH’ Lightbox | |

**Decryption :**

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:



For the previous Ciphertext ‘POH’: which gives us back ‘ACT’.

Assume that all the alphabets are in upper case.

