**JAYPEE UNIVERSITY OF ENGINEERING AND TECHNOLOGY, GUNA**

**Data Security Lab**

**Experiment No. 2**

**IMPLEMENTATION OF PLAYFAIR CIPHER**

**AIM:**

To implement the substitution technique named Playfair Substitution using C language.

**DESCRIPTION:**

The Playfair cipher starts with creating a key table. The key table is a 5×5 grid of letters that will act as the key for encrypting your plaintext. Each of the 25 letters must be unique and one letter of the alphabet is omitted from the table (as there are 25 spots and 26 letters in the alphabet).

To encrypt a message, one would break the message into diagrams (groups of 2 letters) such that, for example, "HelloWorld" becomes "HELLO WORLD", and map them out on

the key table. The two letters of the diagram are considered as the opposite corners of a

rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

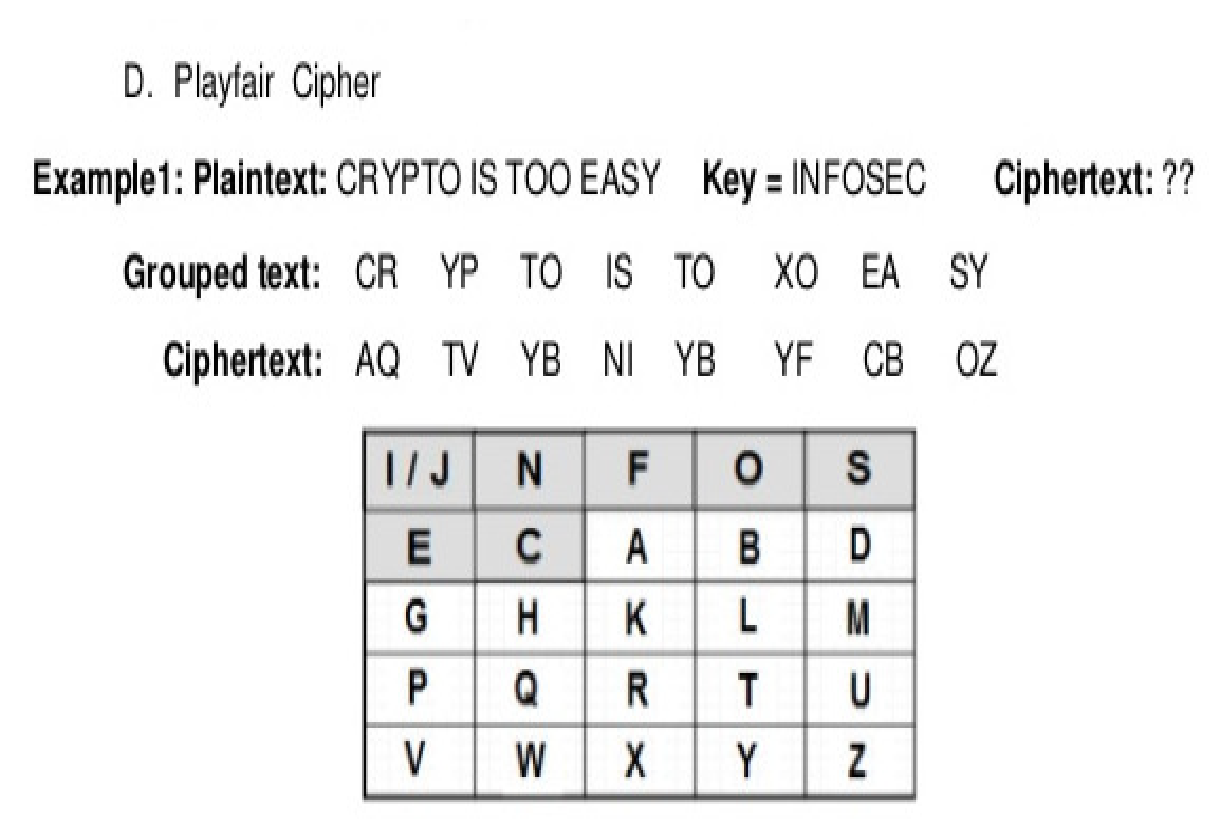
1. If both letters are the same (or only one letter is left), add an "X" after the first letter

2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively

3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively

4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

**EXAMPLE:**

****

**ALGORITHM:**

**STEP-1:** Read the plain text from the user.

**STEP-2:** Read the keyword from the user.

**STEP-3:** Arrange the keyword without duplicates in a 5\*5 matrix in the row order and fill the remaining cells with missed out letters in alphabetical order. Note that ‘i’ and ‘j’ takes the same cell.

**STEP-4:** Group the plain text in pairs and match the corresponding corner letters by forming a rectangular grid.

**STEP-5:** Display the obtained cipher text.