Name:-Vinesh M

Batch :- B3 PRN:-123A3061

Experiment No: 3

**PLAY FAIR CIPHER**

**Aim**: Cryptanalysis or decoding Playfair

# Theory:



The Playfair cipher or Playfair square or Wheatstone–Playfair cipher is a manual symmetric encryption technique and was the first literal diagram substitution cipher. The technique encrypts pairs of letters (bigrams or diagrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. The frequency analysis of bigrams is possible, but considerably more difficult. With 600 possible bigrams rather than the 26 possible monograms (single symbols, usually letters in this context), a considerably larger cipher text is required in order to be useful.

**Procedure:**

Playfair cipher

1. Generate the key Square(5×5): • 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. • 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.

2. 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: IT DEPARTMENT SIES GST ` Security Lab 11

3. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter. Plain Text: “hello” After Split: ‘he’ ‘lx’ ‘lo’ Here ‘x’ is the bogus letter.

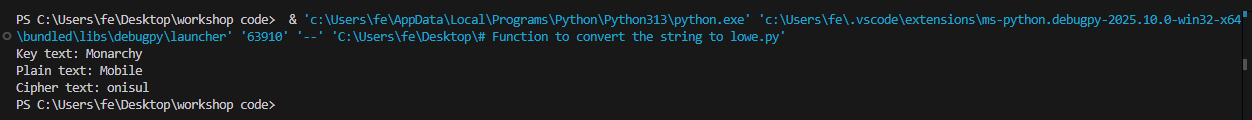
4. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter Plain Text: “helloe” AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’ Here ‘z’ is the bogus letter.

5. Rules for Encryption: a. If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom). b. If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position). c. If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

# Code:

# 

# Output:





# Conclusion:

# Reference:

# 1. https://www.geeksforgeeks.org/dsa/playfair-cipher-with-examples