**INFORMATION SECURITY LAB**

**BCA-VI SEMESTER**

**LAB SHEET 3**

**Name: Tanmay Dangat**

**PRN NO: 20220801070**

**Objective**

To implement the **Play fair Cipher** algorithm in Python for **encryption and decryption** of a given plaintext using a secret key

**Play fair Cipher**

The **Play fair Cipher** is a **classical encryption method** that was invented in **1854 by Charles Wheatstone** but was popularized by **Lord Play fair**. It is a **digraph substitution cipher**, meaning it encrypts **pairs of letters (DIGRAPH)** instead of single letters like simple substitution ciphers (e.g., Caesar cipher).

**Key Concepts**

**1. Create a 5×5 Matrix (Key Table)**

1. Choose a **secret key** (e.g., "SECRET").
2. Remove **duplicate letters** from the key.

Fill the **5×5 matrix** with the key, followed by the **remaining alphabet (A-Z, excluding 'J')**.

**2. Prepare the Plaintext**

* Convert all letters to **uppercase**.
* Replace **'J' with 'I'** (if present).
* Split text into **pairs of two letters (digrams)**.
* If a **pair has the same letter** (like "LL"), insert an **'X' or ‘Q’** (filler letters) between them.

If the text has an **odd number of letters**, add an **extra 'X'(filler letter)** at the end.

**3. Apply Play fair Encryption Rules**

For **each pair of letters (digraphs)**, follow these **three rules**:

1. **Same Row:** Replace each letter with the **next letter to the right** (wrap around if needed).
2. **Same Column:** Replace each letter with the **letter below it** (wrap around if needed).
3. **Rectangle Rule:** If letters **form a rectangle**, replace them with the **opposite corners**.

**4. Decrypting Play fair Cipher**

To decrypt, **reverse the encryption rules**:

* **Same row:** Replace with the **letter to the left**.
* **Same column:** Replace with the **letter above**
* **Rectangle rule:** Swap letters **diagonally** back

**Tasks**

1. Run the **Play fair Cipher** Python program in your IDE.

2. Test the encryption & decryption with different key words/ plain text.

3. Paste your Python code & output below with the date & time of execution

Output:

For Encryption and Decryption:

Date: 14-02-2025

Time 11:25 a.m.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.

A white rectangular object with a white border

AI-generated content may be incorrect.