Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 3

Date: 16/08/2024

Title : Playfair Cipher Implementation

Problem Definition : Implement Playfair cipher and illustrate encoding and decoding process on user entered sentence.

Theory :

The Playfair cipher is a **digraph substitution cipher** that encrypts pairs of letters (digraphs) instead of single letters. This provides better security than monoalphabetic substitution ciphers, which operate on individual letters.

Playfair Cipher Rules:

1. A **5x5 grid** is used where each letter of the alphabet (excluding 'J') is placed. Typically, 'I' and 'J' are combined into one position.
2. The plaintext is divided into digraphs (pairs of letters). If two letters in a pair are the same, a filler character (like 'X') is inserted between them.
3. If a pair of letters:
    - Appear in the **same row**, each letter is replaced by the letter immediately to its right (wrapping around if necessary).
    - Appear in the **same column**, each letter is replaced by the letter immediately below it (wrapping around if necessary).
    - Form a **rectangle**, the letters are replaced by the letters on the opposite corners of the rectangle.

Procedure/ Algorithm :

Playfair Cipher Encryption Algorithm:

1. Prepare the key matrix:
   - Input a keyword from the user.
   - Remove any duplicate letters from the keyword.
   - Fill the remaining spaces in the 5x5 grid with the remaining letters of the alphabet (excluding 'J').
2. Prepare the plaintext:
   - Input a sentence from the user.
   - Convert the sentence to uppercase and remove non-alphabetic characters.
   - Insert 'X' between identical pairs of letters if needed.
   - Append 'X' if the total number of letters is odd.
3. Encrypt the digraphs:

   For each pair of letters:

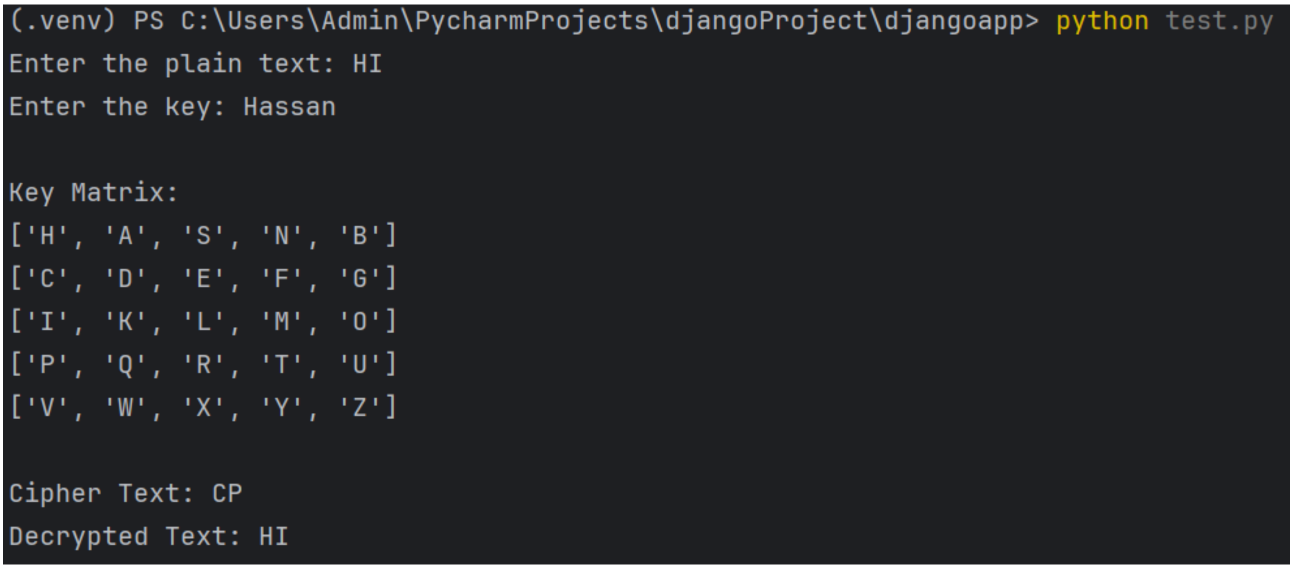
   - If they are in the same row, replace them with the letters to their immediate right.
   - If they are in the same column, replace them with the letters immediately below.
   - If they form a rectangle, replace each with the letter on the opposite corner of the rectangle.

4. Output the ciphertext.

Playfair Cipher Decryption Algorithm:

1. Reverse the encryption process:
   - For each encrypted digraph, perform the opposite operations of encryption to recover the original message.

Results :



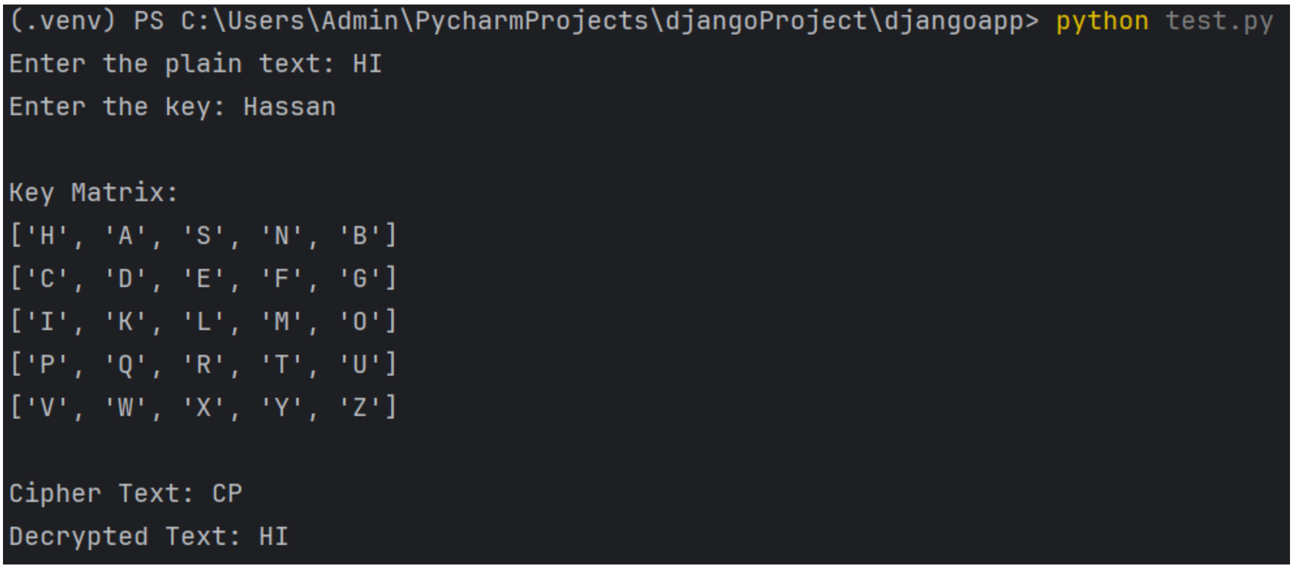
```
(.venv) PS C:\Users\Admin\PycharmProjects\djangoProject\djangoapp> python test.py
Enter the plain text: HI
Enter the key: Hassan

Key Matrix:
['H', 'A', 'S', 'N', 'B']
['C', 'D', 'E', 'F', 'G']
['I', 'K', 'L', 'M', 'O']
['P', 'Q', 'R', 'T', 'U']
['V', 'W', 'X', 'Y', 'Z']

Cipher Text: CP
Decrypted Text: HI
```

References :

1) https://www.educba.com/types-of-cipher/

Lab practice (optional) :

L1. Implement Vigenere cipher.



```
(.venv) PS C:\Users\Admin\PycharmProjects\djangoProject\djangoapp> python test.py
Enter the plain text: HI
Enter the key: Hassan

Key Matrix:
['H', 'A', 'S', 'N', 'B']
['C', 'D', 'E', 'F', 'G']
['I', 'K', 'L', 'M', 'O']
['P', 'Q', 'R', 'T', 'U']
['V', 'W', 'X', 'Y', 'Z']

Cipher Text: CP
Decrypted Text: HI
```

Questions (Short, Long, MCQs) (optional) :

S1: Monoalphabetic substitution v/s Polyalphabetic sustitution.

→Monoalphabetic substitution uses the same cipher alphabet for all letters in the plaintext (e.g,Caesar Cipher).

→Polyalphabetic substitution uses multiple cipher alphabets in sequence to make the ciphertext more secure (e.g., Vigenère Cipher).