Shri Vile Parle Kelavani Mandal's
**DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

Department of Computer Science and Engineering (Data Science)

## SUB: Information Security

## AY 2023-24 (Semester-V)

**NAME:DIVYESH KHUNT** **SAPID:60009210116** **BATCH:D12**

## Experiment No: 5

**Aim:** Design and implement Encryption and Decryption Algorithm using Play fair Cipher.

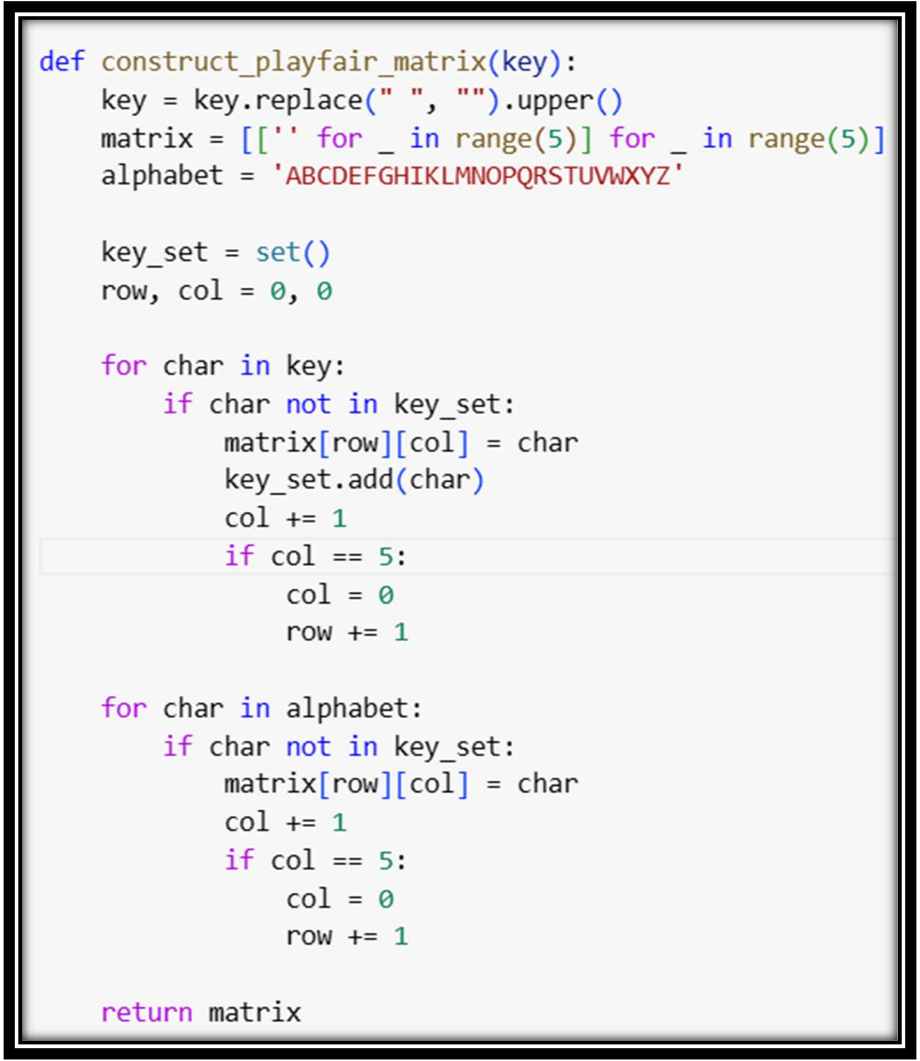
**Theory:**

1. Playfair Cipher

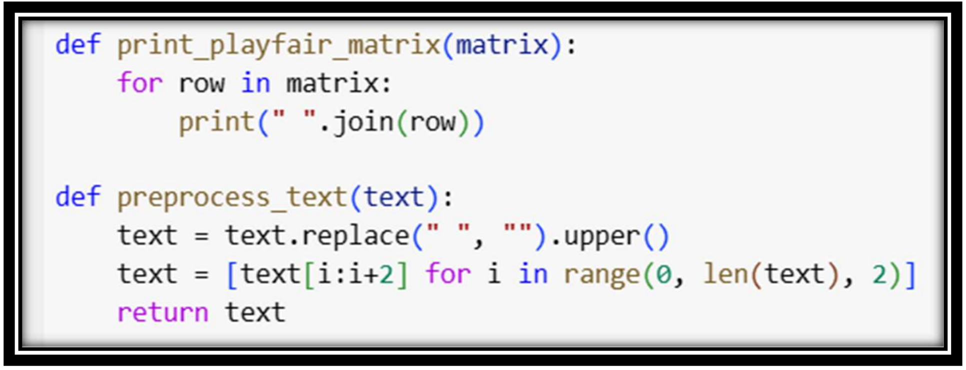
**Example:**

1) **Plaintext: ATTACK**
**Keyword: MONARCHY**

## SUB: Information Security

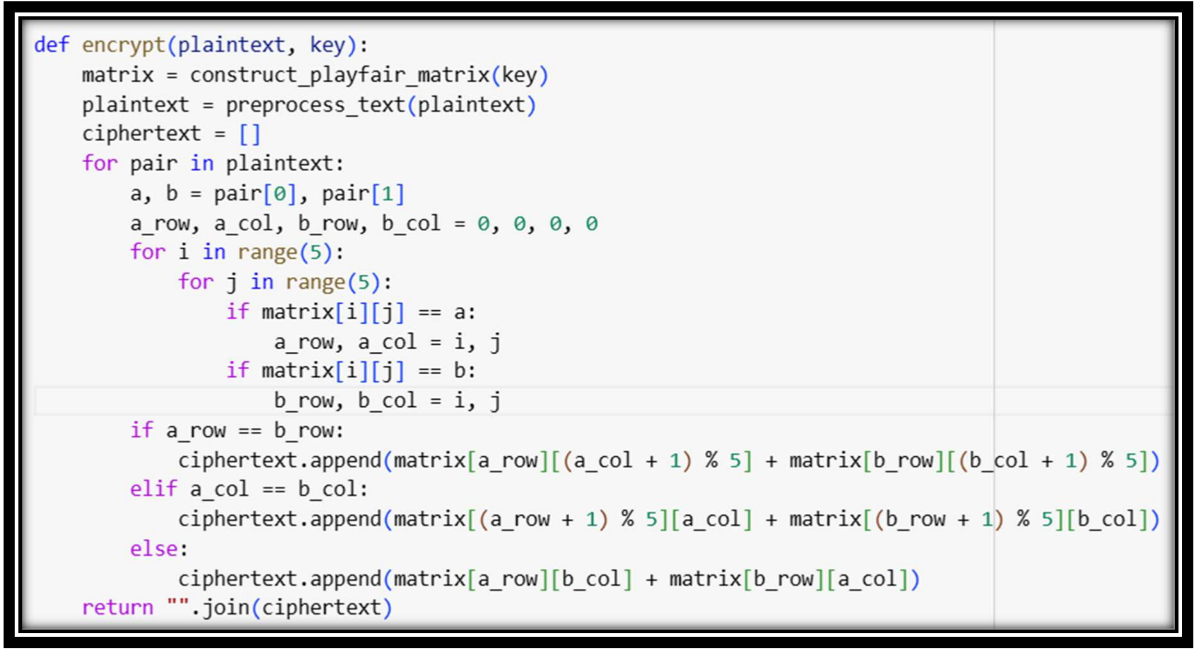


```
def construct_playfair_matrix(key):
    key = key.replace(" ", "").upper()
    matrix = [['' for _ in range(5)] for _ in range(5)]
    alphabet = 'ABCDEFGHIKLMNOPQRSTUVWXYZ'

    key_set = set()
    row, col = 0, 0

    for char in key:
        if char not in key_set:
            matrix[row][col] = char
            key_set.add(char)
            col += 1
            if col == 5:
                col = 0
                row += 1

    for char in alphabet:
        if char not in key_set:
            matrix[row][col] = char
            col += 1
            if col == 5:
                col = 0
                row += 1

    return matrix
```

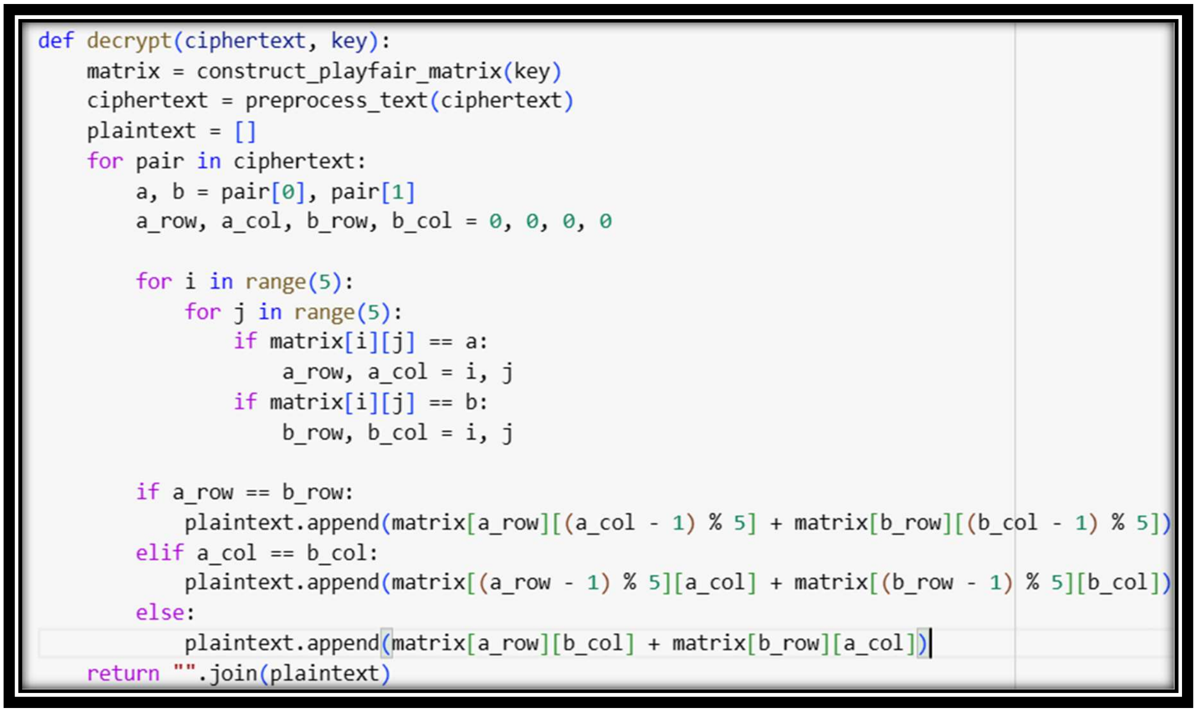


```
def print_playfair_matrix(matrix):
    for row in matrix:
        print(" ".join(row))

def preprocess_text(text):
    text = text.replace(" ", "").upper()
    text = [text[i:i+2] for i in range(0, len(text), 2)]
    return text
```

## SUB: Information Security

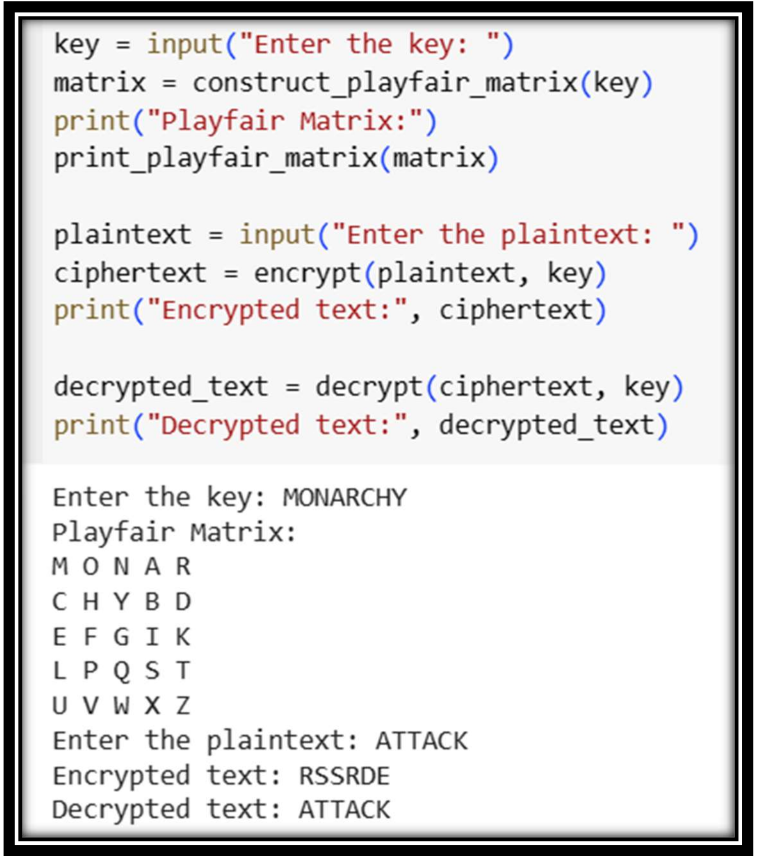


```python
def encrypt(plaintext, key):
    matrix = construct_playfair_matrix(key)
    plaintext = preprocess_text(plaintext)
    ciphertext = []
    for pair in plaintext:
        a, b = pair[0], pair[1]
        a_row, a_col, b_row, b_col = 0, 0, 0, 0
        for i in range(5):
            for j in range(5):
                if matrix[i][j] == a:
                    a_row, a_col = i, j
                if matrix[i][j] == b:
                    b_row, b_col = i, j
        if a_row == b_row:
            ciphertext.append(matrix[a_row][(a_col + 1) % 5] + matrix[b_row][(b_col + 1) % 5])
        elif a_col == b_col:
            ciphertext.append(matrix[(a_row + 1) % 5][a_col] + matrix[(b_row + 1) % 5][b_col])
        else:
            ciphertext.append(matrix[a_row][b_col] + matrix[b_row][a_col])
    return "".join(ciphertext)
```



```python
def decrypt(ciphertext, key):
    matrix = construct_playfair_matrix(key)
    ciphertext = preprocess_text(ciphertext)
    plaintext = []
    for pair in ciphertext:
        a, b = pair[0], pair[1]
        a_row, a_col, b_row, b_col = 0, 0, 0, 0

        for i in range(5):
            for j in range(5):
                if matrix[i][j] == a:
                    a_row, a_col = i, j
                if matrix[i][j] == b:
                    b_row, b_col = i, j

        if a_row == b_row:
            plaintext.append(matrix[a_row][(a_col - 1) % 5] + matrix[b_row][(b_col - 1) % 5])
        elif a_col == b_col:
            plaintext.append(matrix[(a_row - 1) % 5][a_col] + matrix[(b_row - 1) % 5][b_col])
        else:
            plaintext.append(matrix[a_row][b_col] + matrix[b_row][a_col])
    return "".join(plaintext)
```

## SUB: Information Security



```
key = input("Enter the key: ")
matrix = construct_playfair_matrix(key)
print("Playfair Matrix:")
print_playfair_matrix(matrix)

plaintext = input("Enter the plaintext: ")
ciphertext = encrypt(plaintext, key)
print("Encrypted text:", ciphertext)

decrypted_text = decrypt(ciphertext, key)
print("Decrypted text:", decrypted_text)
```

```
Enter the key: MONARCHY
Playfair Matrix:
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
Enter the plaintext: ATTACK
Encrypted text: RSSRDE
Decrypted text: ATTACK
```

**Conclusion:**

**Thus Playfair cipher was successfully executed on python.**