Course Code : CSL604	**Course Name : System Security Lab**
Class : TE-CO	**Batch : Computer Engineering**
Roll no : 18CO63	**Name : SHAIKH TAUSEEF MUSHTAQUE ALI**

Experiment : 02

Aim : Implementation and analysis of Playfair cipher.

Code :

```python
print("\n\t\t PLAYFAIR CIPHER \n")

key=input("ENTER KEY: ")
key=key.replace(" ", "")
key=key.upper()
def matrix(x,y,initial):
    return [[initial for i in range(x)] for j in range(y)]

result=list()
for c in key:
    if c not in result:
        if c=='J':
            result.append('I')
        else:
            result.append(c)
flag=0
for i in range(65,91):
    if chr(i) not in result:
        if i==73 and chr(74) not in result:
            result.append("I")
            flag=1
        elif flag==0 and i==73 or i==74:
            pass
        else:
            result.append(chr(i))
k=0
my_matrix=matrix(5,5,0)
for i in range(0,5):
    for j in range(0,5):
        my_matrix[i][j]=result[k]
        k+=1

def locindex(c):
    loc=list()
    if c=='J':
        c='I'
```

```python
    for i ,j in enumerate(my_matrix):
        for k,l in enumerate(j):
            if c==l:
                loc.append(i)
                loc.append(k)
                return loc

def encrypt():
    msg=str(input("\nENTER MESSAGE: "))
    msg=msg.upper()
    msg=msg.replace(" ", "")
    i=0
    for s in range(0,len(msg)+1,2):
        if s<len(msg)-1:
            if msg[s]==msg[s+1]:
                msg=msg[:s+1]+'X'+msg[s+1:]
    if len(msg)%2!=0:
        msg=msg[:]+'X'
    print("\nCIPHER TEXT: ",end=' ')
    while i<len(msg):
        loc=list()
        loc=locindex(msg[i])
        loc1=list()
        loc1=locindex(msg[i+1])
        if loc[1]==loc1[1]:

print("{}{}".format(my_matrix[(loc[0]+1)%5][loc[1]],my_matrix[(loc1[0]+1)%5][loc1[1]]),end=' ')
        elif loc[0]==loc1[0]:

print("{}{}".format(my_matrix[loc[0]][(loc[1]+1)%5],my_matrix[loc1[0]][(loc1[1]+1)%5]),end=' ')
        else:
            print("{}{}".format(my_matrix[loc[0]][loc1[1]],my_matrix[loc1[0]][loc[1]]),end=' ')
        i=i+2

    print("")

def decrypt():
    msg=str(input("\nENTER CIPHER TEXT: "))
    msg=msg.upper()
    msg=msg.replace(" ", "")
    print("\nPLAIN TEXT: ",end=' ')
    i=0
    while i<len(msg):
        loc=list()
        loc=locindex(msg[i])
        loc1=list()
```

```python
        loc1=locindex(msg[i+1])
        if loc[1]==loc1[1]:
            print("{}{}".format(my_matrix[(loc[0]-1)%5][loc[1]],my_matrix[(loc1[0]-
1)%5][loc1[1]]),end=' ')
        elif loc[0]==loc1[0]:
            print("{}{}".format(my_matrix[loc[0]][(loc[1]-1)%5],my_matrix[loc1[0]][(loc1[1]-
1)%5]),end=' ')
        else:
            print("{}{}".format(my_matrix[loc[0]][loc1[1]],my_matrix[loc1[0]][loc[1]]),end=' ')
        i=i+2

    print("")

while(1):
    print("\nCHOOSE AN OPTION: \n")
    choice=int(input(" 1.ENCRYPTION \n 2.DECRYPTION \n 3.EXIT \n\n"))
    if choice==1:
        encrypt()
    elif choice==2:
        decrypt()
    elif choice==3:
        print("\n EXITING PLAYFAIR CIPHER... \n")
        exit()
    else:
        print("\nINVALID OPTION! CHOOSE CORRECT OPTION \n")
```

Output:

```
mastmac@MASTMACs-Mac-mini EXP02 % python3 EXP02_PLAYFAIRCIPHER.py

                PLAYFAIR CIPHER

ENTER KEY: 3

CHOOSE AN OPTION:

 1.ENCRYPTION
 2.DECRYPTION
 3.EXIT

1

ENTER MESSAGE: hello

CIPHER TEXT:  IF NV MK

CHOOSE AN OPTION:

 1.ENCRYPTION
 2.DECRYPTION
 3.EXIT

2

ENTER CIPHER TEXT: ifnvmk

PLAIN TEXT:  HE LX LO

CHOOSE AN OPTION:

 1.ENCRYPTION
 2.DECRYPTION
 3.EXIT

3

 EXITING PLAYFAIR CIPHER...

mastmac@MASTMACs-Mac-mini EXP02 %
```

Conclusion:

A playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.