Kartik Padave

A022

70362019039

Experiment 3

Aim

To implement Playfair Cipher.

Theory

The Playfair cipher or Playfair square or Wheatstone–Playfair cipher is a manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but bears the name of Lord Playfair for promoting its use. The technique encrypts pairs of letters (bigrams or digrams), 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 to be useful.

Code

```
def matrix(x,y,initial):
    return [[initial for i in range(x)] for j in range(y)]

def locindex(c):
    loc=list()
    if c=='J':
        c='I'
    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("Enter plain text: "))
    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("Cipher 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[(loc
1[0]+1)%5][loc1[1]]).lower(),end=' ')
        elif loc[0]==loc1[0]:
            print("{}{}".format(my_matrix[loc[0]][(loc[1]+1)%5],my_matrix[loc1
[0]][(loc1[1]+1)%5]).lower(),end=' ')
        else:
            print("{}{}".format(my_matrix[loc[0]][loc1[1]],my_matrix[loc1[0]][
loc[1]]).lower(),end=' ')
        i=i+2

key=input("Enter key: ")
key=key.replace(" ", "")
key=key.upper()

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

print("Encryption:")
encrypt()
```

Output

```
E:\Programs\College-Labs\CRYPTO-Lab>python playfair.py
Enter key: monarchy
Encryption:
Enter plain text: an apple a day keeps the doctor away
Cipher Text: ra os qp im br dg iu fl tl cf hr dl nm nx nb
```

Conclusion

Hence, we were able to perform Playfair Cipher.