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

Name: Swasti Jain
Sem: 5, Branch: IT, Batch: 2

Experiment No. : 4

Date: 07/09/2022

Title: Create a product cipher.

Problem Definition: Design and implement a product cipher using S-box, D-box and few other components of a Modern Block Cipher.

Pre-requisite: Modern Block Ciphers

Theory:

Product cipher, data encryption scheme in which the ciphertext produced by encrypting a plaintext document is subjected to further encryption. By combining two or more simple transposition ciphers or substitution ciphers, a more secure encryption may result.

Product cipher is a combination of these six methods

1. Substitution
2. Transposition
3. Split and Combination
4. X-OR
5. Shift (Left/Right)
6. Swap

Procedure/ Algorithm :

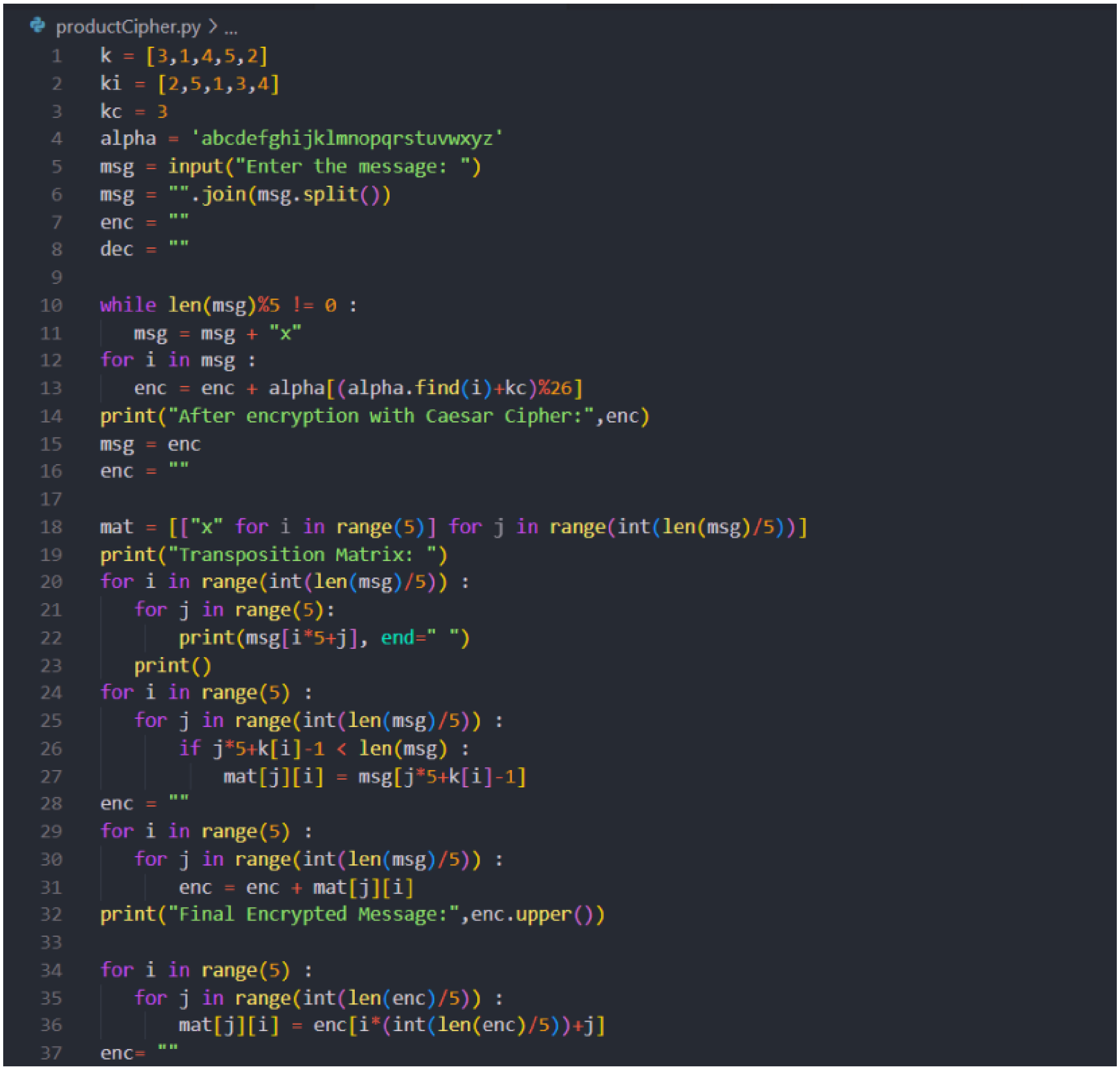
Process for Encryption

Step 1: Take a message from user

Step 2: Split the message in group of 5

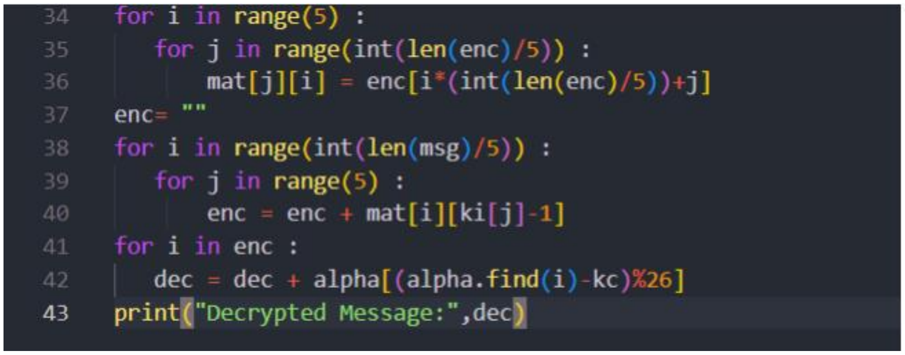
Step 3: Use substitution of each group

Step 4: Appy Transposition to each group and then combine



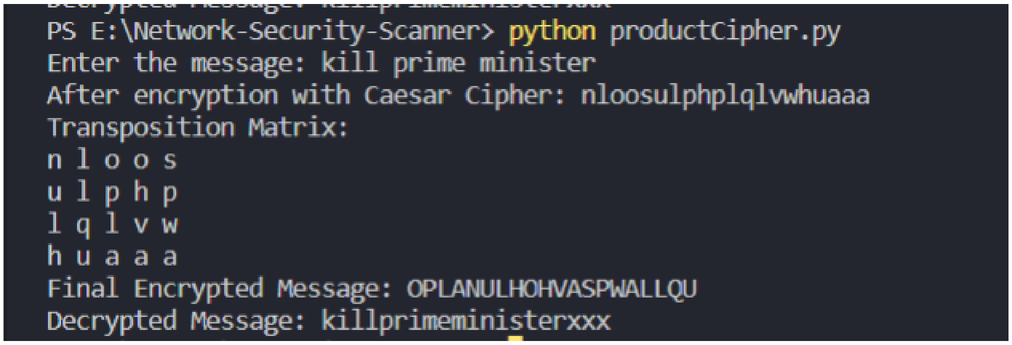
```
k = [3,1,4,5,2]
ki = [2,5,1,3,4]
kc = 3
alpha = 'abcdefghijklmnopqrstuvwxyz'
msg = input("Enter the message: ")
msg = "".join(msg.split())
enc = ""
dec = ""

while len(msg)%5 != 0 :
    msg = msg + "x"
for i in msg :
    enc = enc + alpha[(alpha.find(i)+kc)%26]
print("After encryption with Caesar Cipher:",enc)
msg = enc
enc = ""

mat = [["x" for i in range(5)] for j in range(int(len(msg)/5))]
print("Transposition Matrix: ")
for i in range(int(len(msg)/5)) :
    for j in range(5):
        print(msg[i*5+j], end=" ")
    print()
for i in range(5) :
    for j in range(int(len(msg)/5)) :
        if j*5+k[i]-1 < len(msg) :
            mat[j][i] = msg[j*5+k[i]-1]
enc = ""
for i in range(5) :
    for j in range(int(len(msg)/5)) :
        enc = enc + mat[j][i]
print("Final Encrypted Message:",enc.upper())

for i in range(5) :
    for j in range(int(len(enc)/5)) :
        mat[j][i] = enc[i*(int(len(enc)/5))+j]
enc= ""
```

o



```python
for i in range(5) :
    for j in range(int(len(enc)/5)) :
        mat[j][i] = enc[i*(int(len(enc)/5))+j]
enc= ""
for i in range(int(len(msg)/5)) :
    for j in range(5) :
        enc = enc + mat[i][ki[j]-1]
for i in enc :
    dec = dec + alpha[(alpha.find(i)-kc)%26]
print("Decrypted Message:",dec)
```

Result:



```
PS E:\Network-Security-Scanner> python productCipher.py
Enter the message: kill prime minister
After encryption with Caesar Cipher: nloosulphplqlvwhuaaa
Transposition Matrix:
n l o o s
u l p h p
l q l v w
h u a a a
Final Encrypted Message: OPLANULHOHVASPWALLQU
Decrypted Message: killprimeministerxxx
```

References :

[What are the components of Modern Block Cipher in Information Security? (tutorialspoint.com)]