DOP: / /2023 DOS: / /2023

Experiment No: 02

Title: Design and implement a product cipher using substitution ciphers

Theory:

Product cipher:

“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.”

This system used a 6 × 6 matrix to substitution-encrypt the 26 letters and 10 digits into pairs of the symbols A, D, F, G, V, and X. The resulting biliteral cipher was then written into a rectangular array and route encrypted by reading the columns in the order indicated by a key word, a.

●Substitution ciphers:

When plain text is encrypted, it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Algorithm for Substitution Cipher:

Input:

- A String of both lower and upper case letters, called Plaintext.
- An Integer denoting the required key.

Procedure:

- Create a list of all the characters.
- Create a dictionary to store the substitution for all characters.
- For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
- Print the new string generated.

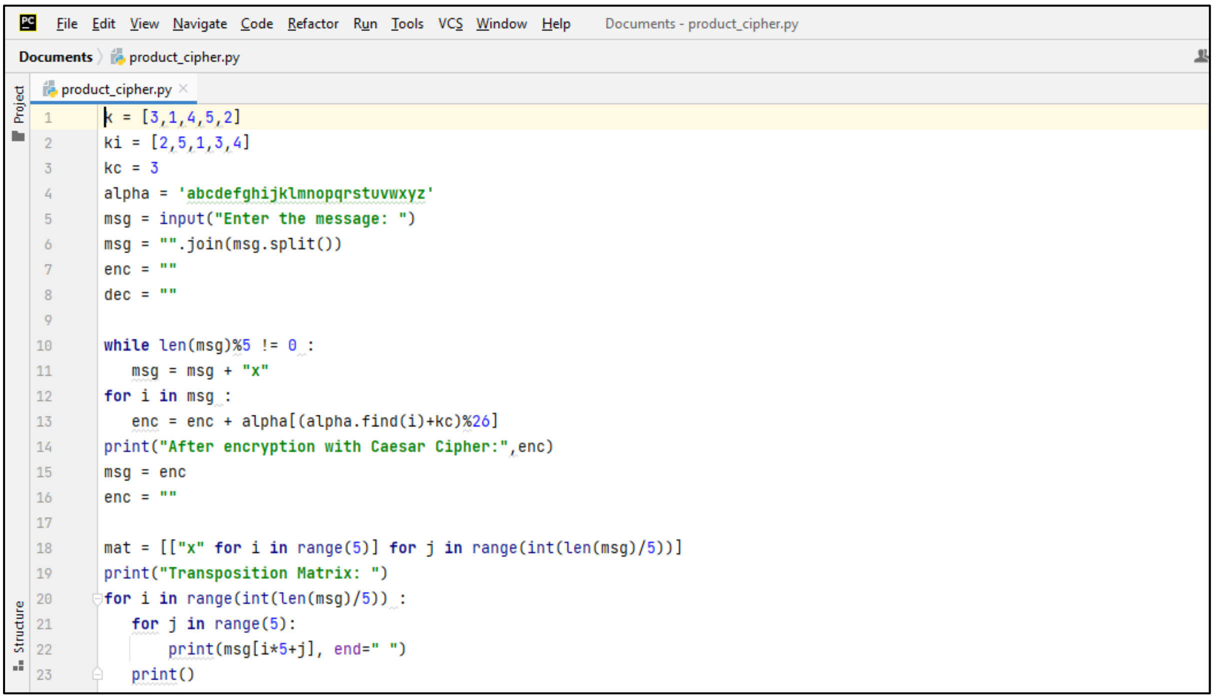
●Transposition Cipher:

“Transposition cipher, simple data encryption scheme in which plain text characters are shifted in some regular pattern to form cipher text. In manual systems transpositions are generally carried out with the aid of an easily remembered mnemonic.”

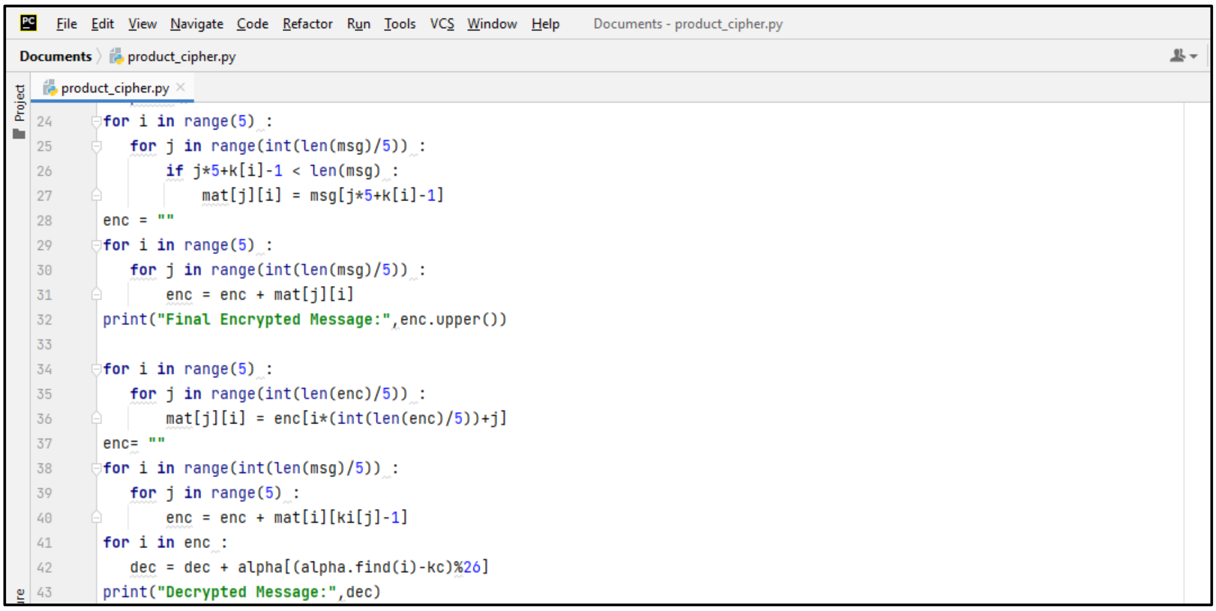
●ALGORITHM

- STEP-1: Read the plain text from the user.
- STEP-2: Read the plan text position from the user.
- STEP-3: comparing the character and adding the corresponding char to the encrypted String
- STEP-4: Run the for loop for total string.
- STEP-5: Display the Transposition Matrix
- STEP-6: Display the cipher text obtained above.

●Input:

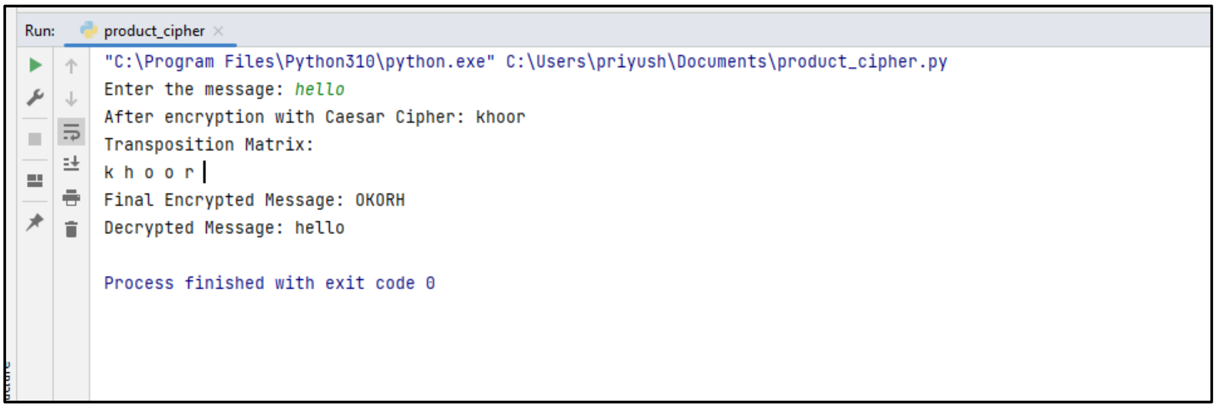

File Edit View Navigate Code Refactor Run Tools VCS Window Help
Documents - product_cipher.py
Documents
product_cipher.py
product_cipher.py
Project
Structure

```
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()
```


File Edit View Navigate Code Refactor Run Tools VCS Window Help
Documents - product_cipher.py
Documents
product_cipher.py
product_cipher.py
Project

```
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= ""
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)
```

●**Output:**



```
"C:\Program Files\Python310\python.exe" C:\Users\priyush\Documents\product_cipher.py
Enter the message: hello
After encryption with Caesar Cipher: khoor
Transposition Matrix:
k h o o r |
Final Encrypted Message: OKORH
Decrypted Message: hello

Process finished with exit code 0
```

Conclusion: -

Thus we have studied, design and implement a product cipher using substitution ciphers..