Experiment No. : 2

Title : Cryptanalysis of Mono-alphabetic Substitution Cipher

Problem Definition : Break down the Mono-alphabetic Substitution Cipher using Frequency analysis method. Decode the given cipher text “slaz tlla avupnoa ha aol whyr”.

Pre-requisite : Any programming knowledge – C, C++, Java, Python and concepts of symmetric cryptography.

Theory: A mono-alphabetic substitution cipher is a type of substitution ciphers in which the equivalent letters of the plaintext are restored by the same letters of the ciphertext. Mono, which defines one, it signifies that each letter of the plaintext has a single substitute of the ciphertext.

Caesar cipher is a type of Monoalphabetic cipher. It uses the similar substitution method to receive the cipher text characters for each plain text character. In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher.

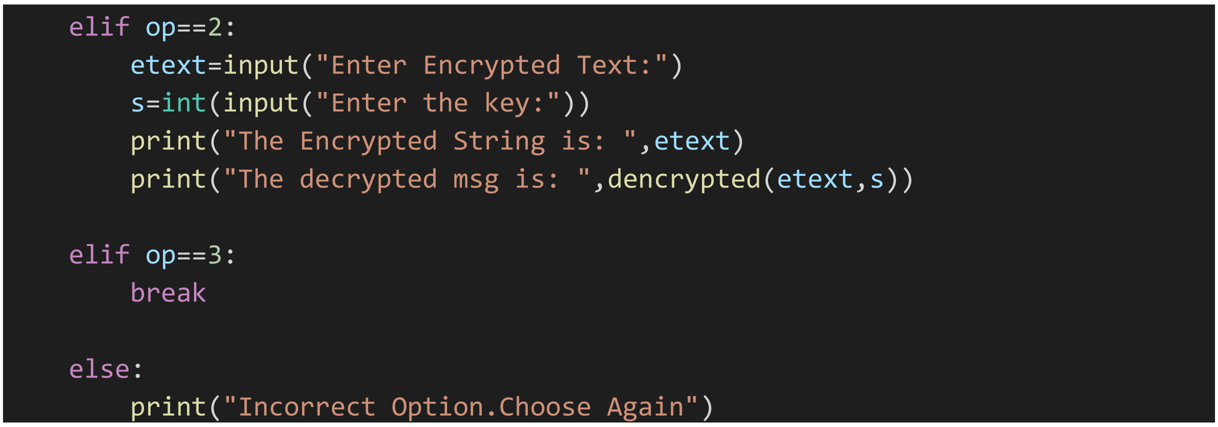
Procedure/ Algorithm:

```
def encrypted(string,shift):
            cipher=''
            for char in string:
                if char=='':
                    cipher=cipher+char
                elif char.isupper():
                    cipher=cipher+chr((ord(char)+shift-65)%26+65)
                else:
                    cipher=cipher+chr((ord(char)+shift-97)%26+97)
            return cipher

def dencrypted(string,shift):
            cipher=''
            for char in string:
                if char=='':
                    cipher=cipher+char
                elif char.isupper():
                    cipher=cipher+chr((ord(char)-shift-65)%26+65)
                else:
                    cipher=cipher+chr((ord(char)-shift-97)%26+97)
            return cipher

while True:
    op=int(input("\nChoose:\n1.Encryption\n2.Decryption\n3.Exit\n"))

    if op==1:
        text=input("Enter Text You Want to Encrypt:")
        s=int(input("Enter the key:"))
        print("The original String is: ",text)
        print("The Encrypted msg is: ",encrypted(text,s))
```

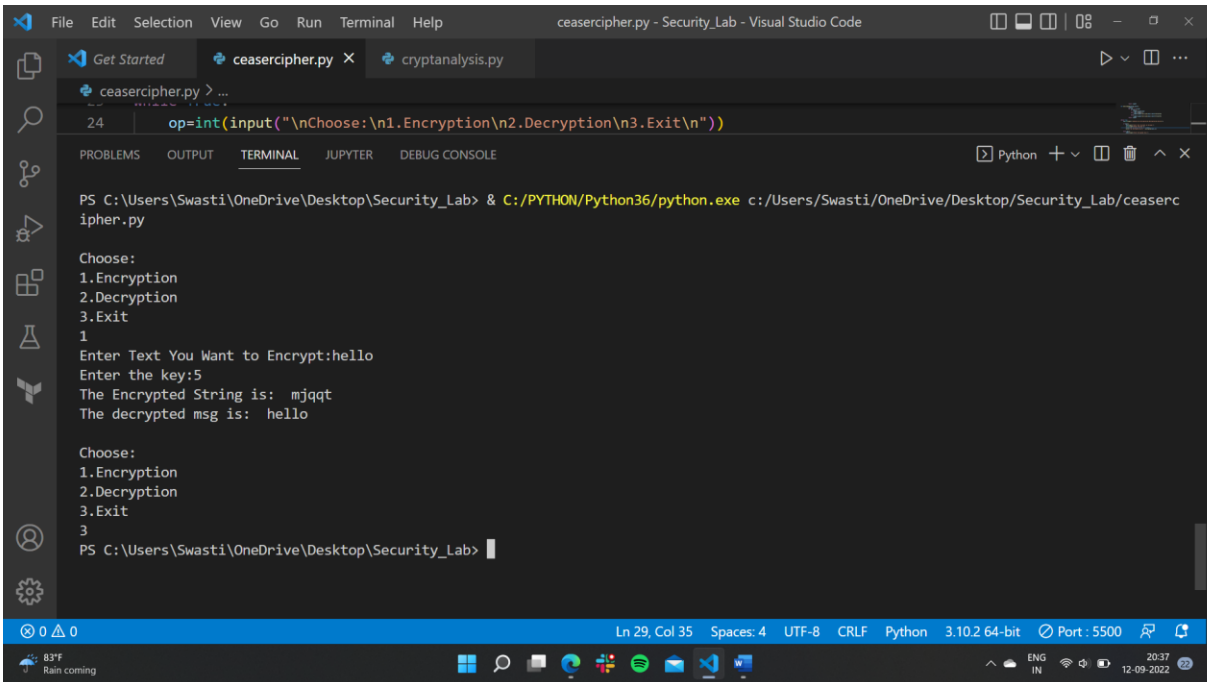


```
    elif op==2:
        etext=input("Enter Encrypted Text:")
        s=int(input("Enter the key:"))
        print("The Encrypted String is: ",etext)
        print("The decrypted msg is: ",dencrypted(etext,s))

    elif op==3:
        break

    else:
        print("Incorrect Option.Choose Again")
```

Results :


File Edit Selection View Go Run Terminal Help
ceasercipher.py - Security_Lab - Visual Studio Code
Get Started
ceasercipher.py
cryptanalysis.py
ceasercipher.py > ...
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE
Python
⊗ 0 ⚠ 0
Ln 29, Col 35 Spaces: 4 UTF-8 CRLF Python 3.10.2 64-bit Port : 5500
83°F
Rain coming
ENG
IN
20:37
12-09-2022

```
    op=int(input("\nChoose:\n1.Encryption\n2.Decryption\n3.Exit\n"))
```

```
PS C:\Users\Swasti\OneDrive\Desktop\Security_Lab> & C:/PYTHON/Python36/python.exe c:/Users/Swasti/OneDrive/Desktop/Security_Lab/ceaserc
ipher.py

Choose:
1.Encryption
2.Decryption
3.Exit
1
Enter Text You Want to Encrypt:hello
Enter the key:5
The Encrypted String is:  mjqqt
The decrypted msg is:  hello

Choose:
1.Encryption
2.Decryption
3.Exit
3
PS C:\Users\Swasti\OneDrive\Desktop\Security_Lab> 
```