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.

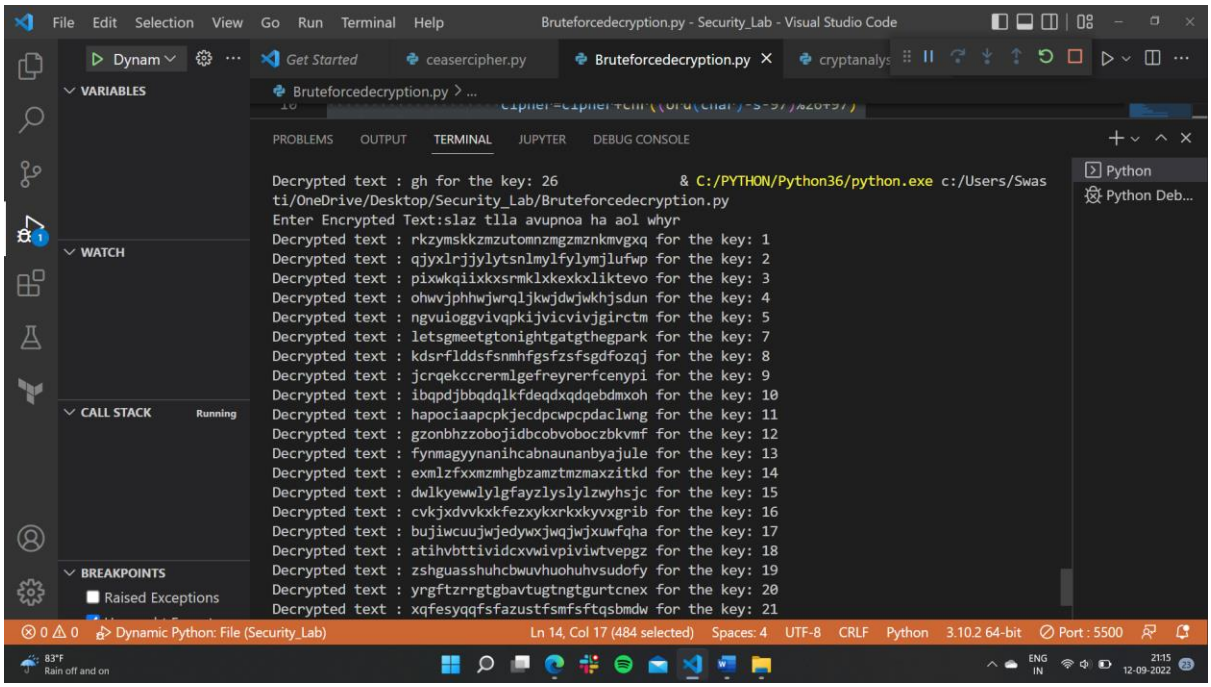
Procedure/ Algorithm:

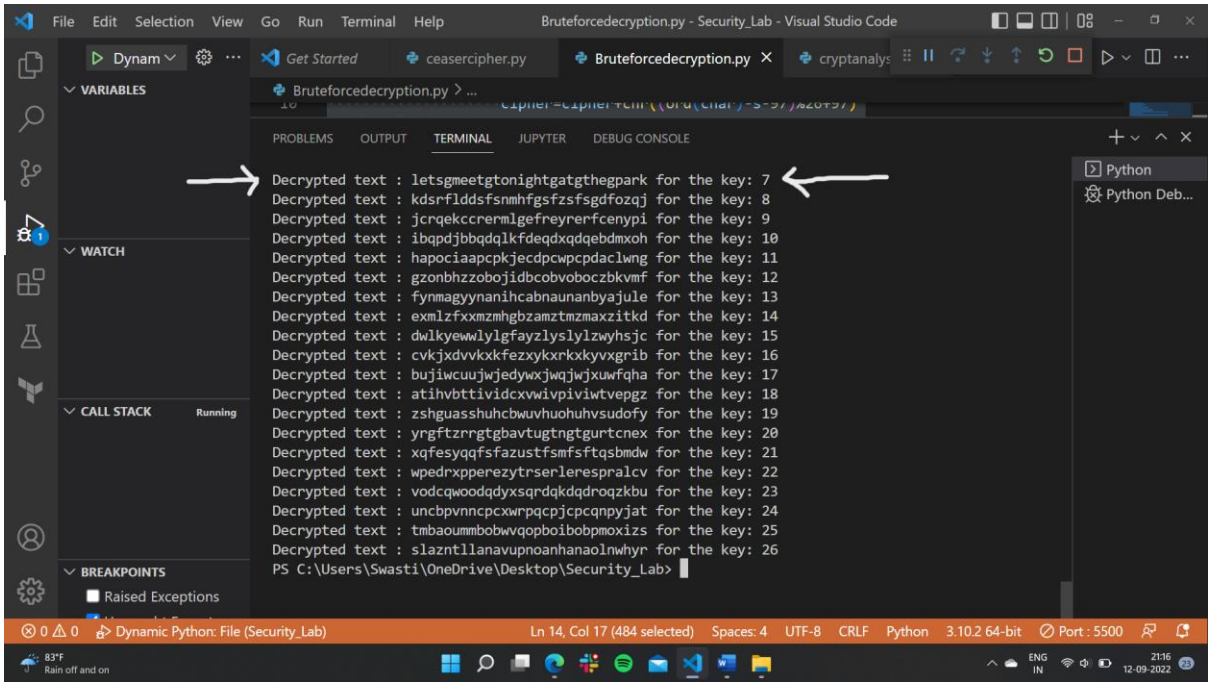
<u>BRUTEFORCE CEASER CIPHER</u>

```
def decrypted(string):
     for s in range(1,27):
            cipher=''
            for char in string:
                if char==':
                    cipher=cipher+char
                elif char.isupper():
                    cipher=cipher+chr((ord(char)-s-65)%26+65)
                else:
                    cipher=cipher+chr((ord(char)-s-97)%26+97)
            print("Decrypted text :",cipher,"for the key:",s)

etext=input("Enter Encrypted Text:")
decrypted(etext)
```

Q1:Decrypt “slaz tlla avupnoa ha aol whyr” using bruteforce ceaser cipher.

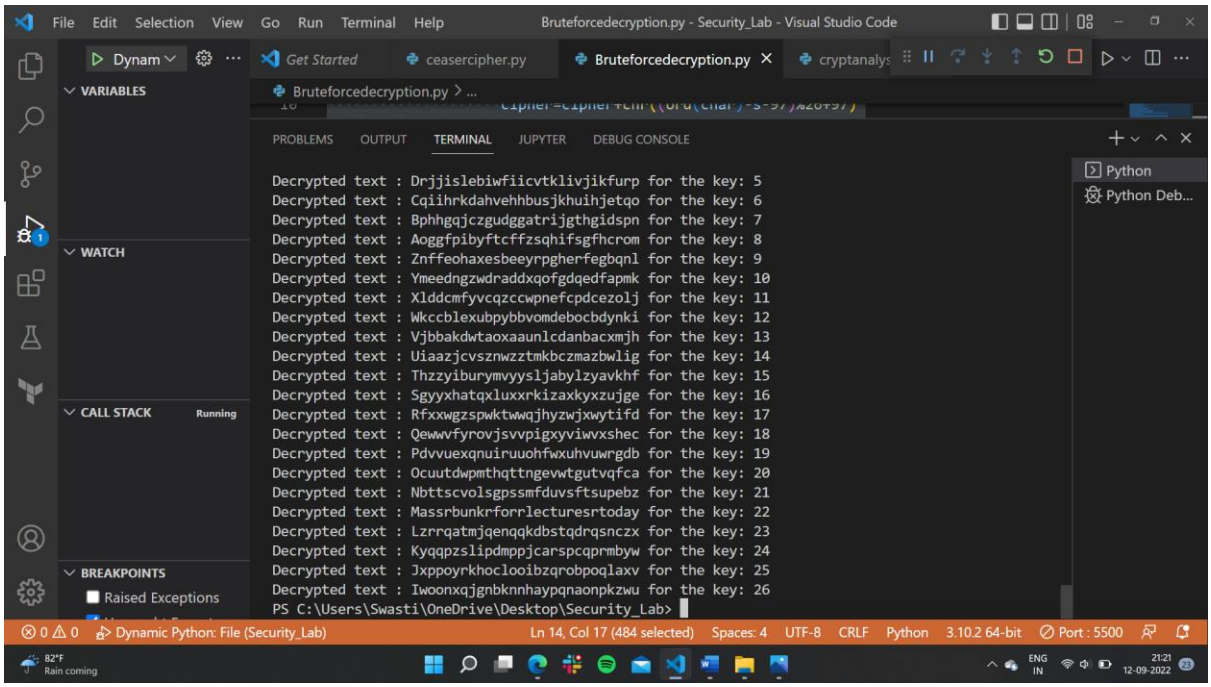




So the key for decryption is 7 and the text decrypted is “lets meet tonight at the park”

(Here g represents space between two words)

Q2:Decrypt “lwoo xqjg bkn haypqnao pkzwu” **using bruteforce ceaser cipher.**



So the key for decryption is 22 and the text decrypted is “Mass bunk for lectures today”

(Here r represents space between two words)

```
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 :