

## 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:**

### BRUTEFORCE CEASER CIPHER

```
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 caesar cipher.

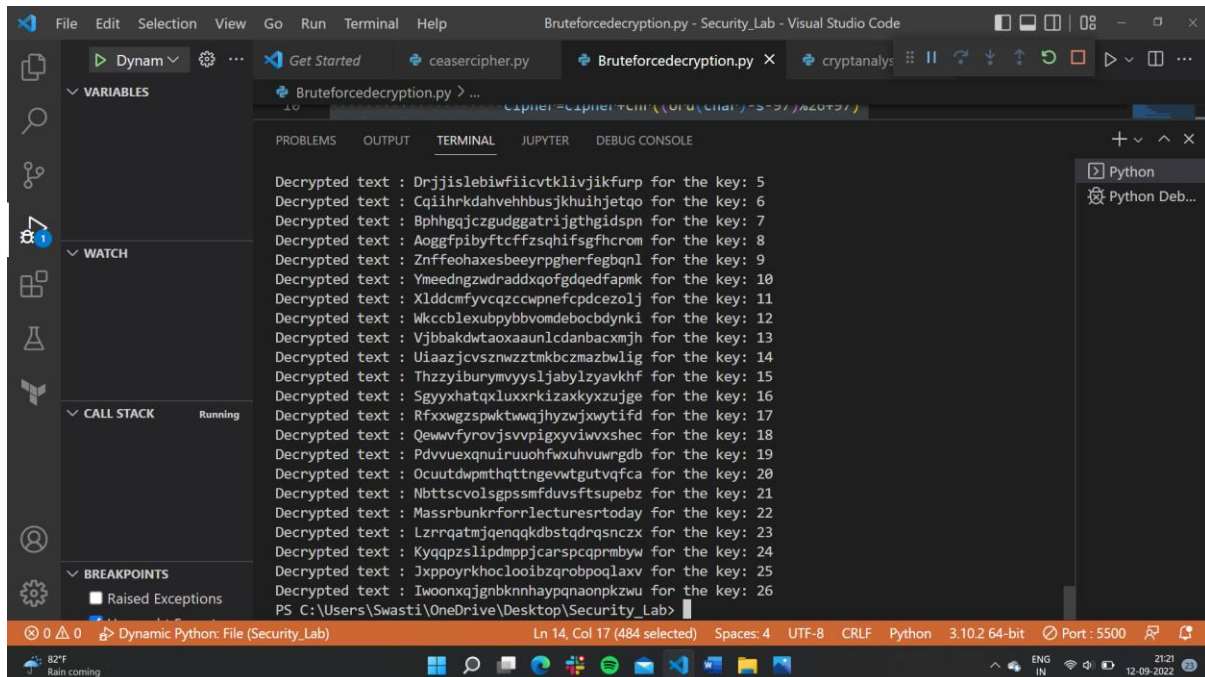
```
Decrypted text : gh for the key: 26
ti/OneDrive/Desktop/Security_Lab/Bruteforcedecryption.py
Enter Encrypted Text:slaz tlla avupnoa ha aol whyr
Decrypted text : rkzyskkmzmzutomnzmzmznmvmgxq for the key: 1
Decrypted text : qjyxlrjjlyltsnlmlyfymjlfufwp for the key: 2
Decrypted text : pixwkqiixksrmlkxkxkxlktevo for the key: 3
Decrypted text : ohwvjphhwjwqljkwjdjwkhjsdun for the key: 4
Decrypted text : ngvuogvgvivqpkijvicvivjginctm for the key: 5
Decrypted text : letsgmeetgtonightgatgthegpark for the key: 7
Decrypted text : kdsrflddsfsnmhfgsfzsfsgdfozqj for the key: 8
Decrypted text : jcrqekccrermllgefeyrerfrcenyapi for the key: 9
Decrypted text : ibqpdjbbdqqlkfdeqdxqdeqdbmdxoh for the key: 10
Decrypted text : hapociaapckjecdpcwpcdaclwng for the key: 11
Decrypted text : gzonbhzzobojidbcobvoboczbkvmf for the key: 12
Decrypted text : fynmagyynanihcabnaunanbyajule for the key: 13
Decrypted text : exmlzfxxmzmhgbzamztmzmaxzitkd for the key: 14
Decrypted text : dwlkyewlylgfayzlyslzlyzwyhsjc for the key: 15
Decrypted text : cvkjxdvkvkfezykxrkxkyvvgrib for the key: 16
Decrypted text : bujiwcuujjedyxwjwqjwjuwfgqa for the key: 17
Decrypted text : atihvttividcxwvpiwivtvepgz for the key: 18
Decrypted text : zshguasshuhcbwuvhuohvhsudofy for the key: 19
Decrypted text : yrgftzrrgtgbavtugtngturtcnex for the key: 20
Decrypted text : xqfesyqqfsfazustfsmfsftqsbmdw for the key: 21
```

```
Decrypted text : letsgmeetgtonightgatgthegpark for the key: 7
Decrypted text : kdsrflddsfsnmhfgsfzsfsgdfozqj for the key: 8
Decrypted text : jcrqekccrermllgefeyrerfrcenyapi for the key: 9
Decrypted text : ibqpdjbbdqqlkfdeqdxqdeqdbmdxoh for the key: 10
Decrypted text : hapociaapckjecdpcwpcdaclwng for the key: 11
Decrypted text : gzonbhzzobojidbcobvoboczbkvmf for the key: 12
Decrypted text : fynmagyynanihcabnaunanbyajule for the key: 13
Decrypted text : exmlzfxxmzmhgbzamztmzmaxzitkd for the key: 14
Decrypted text : dwlkyewlylgfayzlyslzlyzwyhsjc for the key: 15
Decrypted text : cvkjxdvkvkfezykxrkxkyvvgrib for the key: 16
Decrypted text : bujiwcuujjedyxwjwqjwjuwfgqa for the key: 17
Decrypted text : atihvttividcxwvpiwivtvepgz for the key: 18
Decrypted text : zshguasshuhcbwuvhuohvhsudofy for the key: 19
Decrypted text : yrgftzrrgtgbavtugtngturtcnex for the key: 20
Decrypted text : xqfesyqqfsfazustfsmfsftqsbmdw for the key: 21
Decrypted text : wpedrpperezytrserlerespralcv for the key: 22
Decrypted text : vodcqwoodqdxsqrdqkdqdroqzkbu for the key: 23
Decrypted text : uncbpvnnccpxwqpqpcjpcqnpjyat for the key: 24
Decrypted text : tmbaoumbobwvqopboibobpmoxizs for the key: 25
Decrypted text : slazntllanavupnoanhanalnwhy for the key: 26
PS C:/Users/Swasti/OneDrive/Desktop/Security_Lab>
```

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 pkzww” using brute force ceaser cipher.**



```
Bruteforcedecryption.py > ...
cipher=cipher+chr((ord(char)-shift-97)%26+97)

Decrypted text : Drjjislebiwficvtklivjikfurf for the key: 5
Decrypted text : Cqiihrkdahvehhbusjkhuihjetqo for the key: 6
Decrypted text : Bphhgqjczgudggatrijgthgidspn for the key: 7
Decrypted text : Aoggfpibyftcfffzsqhifsgfhcrom for the key: 8
Decrypted text : Znffeoaxesbeeyrpgherfegbqnl for the key: 9
Decrypted text : Ymeedngzwdraddxqofgdqdfapmk for the key: 10
Decrypted text : Xlddcmfyvcqzccwpnefcpcdezoij for the key: 11
Decrypted text : Wkccblexubpybbvmdobocbdynki for the key: 12
Decrypted text : Vjbbakdwtaoxaaulcdanbacxmjh for the key: 13
Decrypted text : Uiaazjcvsnwzztmkbczmazbwlig for the key: 14
Decrypted text : Thzzyiburymvyysljabylyzavkhf for the key: 15
Decrypted text : Sgyxhatqxluxxrkizaxkxyzujge for the key: 16
Decrypted text : Rfxxwgzspwktwwqjhyzjwxytifi for the key: 17
Decrypted text : Qewwrfyrovjsvvpigxyvixwshec for the key: 18
Decrypted text : Pdvuexqnuiruohfwxuhvuwrgdb for the key: 19
Decrypted text : Ocuutdwpmthqttngevwgtutvqfca for the key: 20
Decrypted text : Nbttsvolsgpssmfduvsftsupebz for the key: 21
Decrypted text : Massrbunkrforlecturesrtoday for the key: 22
Decrypted text : Lzrrqatmjgenqqkdbstqdrqscxz for the key: 23
Decrypted text : Kyqqpzslipdmppjcarspcqprmbwy for the key: 24
Decrypted text : Jxppoyrkhocloobzqrobpqolaxv for the key: 25
Decrypted text : Iwoonxqjgnbknnhaypqnaonpkzww for the key: 26
PS C:\Users\Swasti\OneDrive\Desktop\Security_Lab>
```

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 decrypted(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))

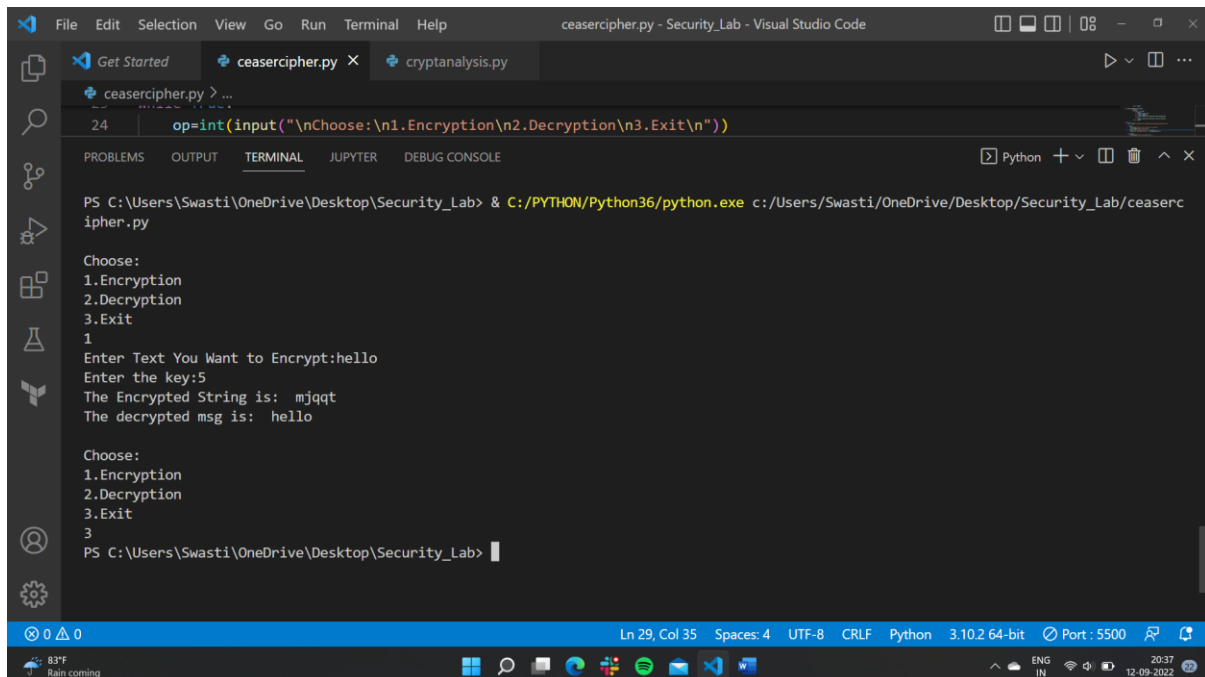
    elif op==2:
        etext=input("Enter Encrypted Text:")
        s=int(input("Enter the key:"))
        print("The Encrypted String is: ",etext)
        print("The decrypted msg is: ",decrypted(etext,s))

    elif op==3:
        break

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

```

## Results :



The screenshot shows the Visual Studio Code interface with a file named `ceasercipher.py` open. The terminal window is active, showing the command prompt and the execution of the program. The program prompts the user to choose an option (1 for Encryption, 2 for Decryption, 3 for Exit). The user enters 1, and the program prompts for text and key. The user enters "hello" for text and 5 for key. The program outputs "The Encrypted String is: mjqqt" and "The decrypted msg is: hello". The user then enters 3 to exit the program.

```

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>

```