**Name: Madhuri Ramakrishnan**

**PRN: 119A3032**

**TE-IT (E2)**

**EXPERIMENT-01**

**Aim:** - Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

**Resources Used: -**

1. VS code IDE
2. Programming Language - Python

**Theory:**

***Mono-alphabetic Substitution Cipher***

* A mono-alphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of mono-alphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key.
* A simple example is where each letter is encrypted as the next letter in the alphabet: "*a simple message*" becomes "*b tjnqmf nfttbhf*".
* There are many different mono-alphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter.
* The history of simple substitution ciphers can be traced back to the very earliest civilisations, and for a long time they were more than adequate for the purposes for which they were needed. By today's standards they are very weak, and incredibly easy to break, but they were a very important step in developing cryptography.

***Frequency analysis***

* It is the study of the **frequency of letters** or groups of letters in a cipher text.
* The method is used as an aid to breaking **substitution ciphers.**
* Frequency analysis consists of **counting the occurrence of each letter** in a text.
* It is useful to look for popular pairs of letters or even try to predict some frequent longer sequences of letters or whole words. The intruder always tries to find sequences of letters which are often used in the selected language.

**Procedure/Algorithm -**

1. The Caesar cipher is another mono-alphabetic substitution cipher which is easy to break.

* Encryption :

1. First we create the cipher text of the plain text by shifting the alphabets of the plain text to the left by the no. Of places given by the key(user input)
2. E.g. we must create a cipher text of "SHOBHANA". Thus a shift of 3 moves the plain text to “VKREKDQD".

* Decryption :

1. If we have rcvd the cipher text “VKREKDQD” and we know that it has been enciphered using the key 3, we can generate the Plaintext alphabets using a shift of -3.

2. Frequency analysis:

* + When trying to decrypt a cipher text based on a substitution cipher, we can use a frequency analysis to help identify the most recurring letters in a cipher text and hence make hypothesis of what these letters have been encoded as (e.g. E, T, A, O, etc.). This will help us decrypt some of the letters in the text.
  + In the code below, we have taken a plaintext – “Shobhana” which is of length 8.
  + The letters “h” and “a” occur two times, which makes their frequency (2/8)\*100 = 25.0 and rest letters occur once hence their frequency came as 12.5.[ (1/8)\*100]

*Code:*

txt = input("Enter your plain text:")

key = int(input("Enter shift key:"))

def encrypt\_txt(txt,k):

    ans = "";

    for i in range(len(txt)):

        ch = txt[i]

        if(ch == " "):

            ans = ans + ch

        elif(ch.isupper()):

            new = (ord(ch)+k - 65)%26 + 65

            ans = ans + chr(new)

        else:

            new = (ord(ch)+k - 97)%26 + 97

            ans = ans + chr(new)

    return ans

def decrypt\_txt(txt,k):

    ans = "";

    for i in range(len(txt)):

        ch = txt[i]

        if(ch == " "):

            ans = ans + ch

        elif(ch.isupper()):

            new = (ord(ch)-k - 65)%26 + 65

            ans = ans + chr(new)

        else:

            new = (ord(ch)-k - 97)%26 + 97

            ans = ans + chr(new)

    return ans

def frequencyAnalysis(entxt):

    freq = {}

    for i in entxt:

        if(i in freq):

            freq[i] += 1  #More than one

        else:

            freq[i] = 1   #First Occurance

    for i in freq:

        freq[i] = (freq[i]\*100) / len(entxt)

    print(freq)

print("Plain Text :"+txt)

print("Shift Key :"+ str(key))

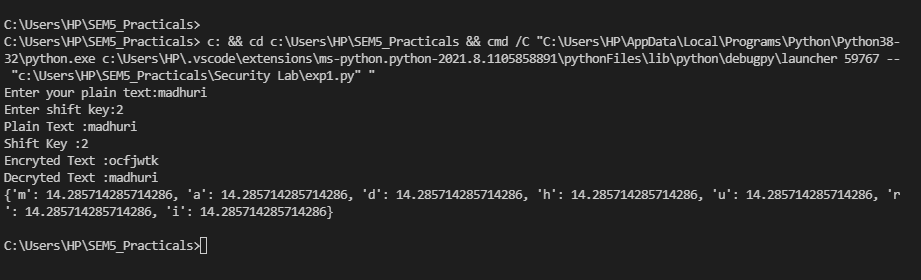
en = encrypt\_txt(txt,key)

print("Encryted Text :"+en)

print("Decryted Text :"+decrypt\_txt(en,key))

frequencyAnalysis(txt)

**Results:**



**Conclusion:**

In this experiment we have learned about:

* Working of mono-alphabetic substitution Caesar-shift cipher
* Implemented encryption and decryption of plain text keeping the key as 3 and verified the results.
* We also observed the result of frequency analysis (Performed on the plain-text) and verified the results.

Hence, we successfully completed the breaking of Mono – alphabetic cipher using Frequency Analysis method.