**Cryptography & Network Security**

PRN - 2019BTECS00026

Name - Niraja Vasudev Kulkarni

Batch - B1

**Assignment - 2**

* **Title - Cryptanalysis (Decryption of Caeser Cipher)**
* **Objective -**

Decrypting the cipher text encrypted using Caesar Cipher

* **Theory** -

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text.

Here , the task is to perform cryptanalysis that is , to decrypt the cipher text which is actually encrypted by the Caeser Cipher . We can write another function decrypt that’ll apply the shift in the opposite direction to decrypt the original text. The shift is not known , so we will have to try all possible combinations and find out which one gives meaningful output.

Procedure -

1. Take the cipher text as an input from the user
2. Considering all possible 26 shifts , decrypt the given text by applying shift in opposite direction
3. Find the meaningful output using PyEnchant library that returns whether the translated word is present in the dictionary or not

* **Code snapshots -**

import enchant

d = enchant.Dict("en\_US")

message = input('Enter Cipher text')

LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

actualText=''

actualKey=0

no\_of\_words=len(message.split())

words=[]

for key in range(len(LETTERS)):

   translated = ''

   word=''

   for symbol in message:

      if symbol in LETTERS:

         num = LETTERS.find(symbol)

         num = num - key

         if num < 0:

            num = num + len(LETTERS)

         translated = translated + LETTERS[num]

         word=word+LETTERS[num]

      else:

        if d.check(word):

            words.append(word)

        else:

            words.clear()

        word=''

   if d.check(word):

        words.append(word)

   if len(words)==no\_of\_words:

        actualText=translated

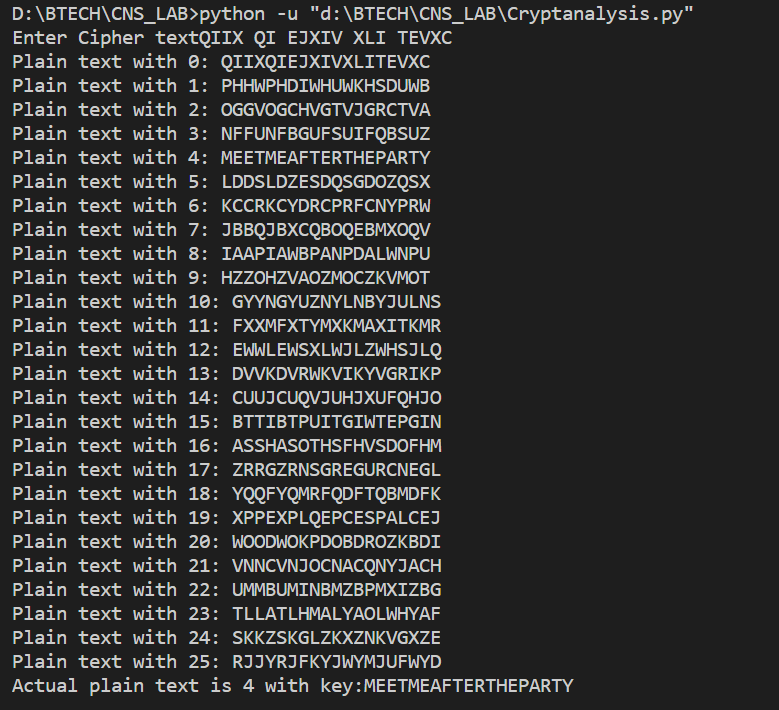
        actualKey=key

        words.clear()

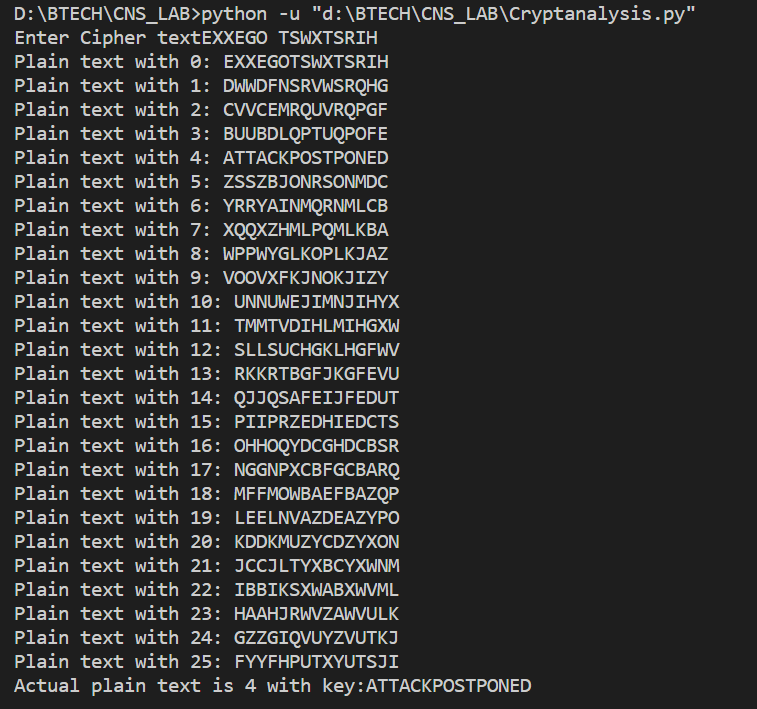
   print('Plain text with %s: %s' % (key, translated))

print('Actual plain text is %s with key:%s' % (actualKey,actualText))

* **Outputs -**
* **Sample Output 1 -**



* Sample Output 2 -



* **Conclusion** -

Caeser Cipher is a monoalphabetic classical cipher which can be easily decrptyed. It is a naive way of encrypting. Here , PyEnchant lilbrary is used for finding the meaningful output from suggested set of sentences as the shift is unknown.