**Final Year B.Tech. (CSE) – II [ 2021-22 ]**

**Cryptograpy and Network Security Lab**

**PRN: 2019BTECS00015**

**Full name: Shraddha Sanjay Kharat**

**Batch: B1**

**Assignment no -2**

**Date: 23-08-2022**

**Que )** **Cryptanalysis**

**Objective :**

Decrypting the cipher text encrypted using Caesar Cypher

**Theory:**

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them.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 similar to encrypt, 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.

**Code Snapshots:**

import enchant

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

alphabet = ['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

text = input('Enter Text: ')

transAlphabet = {}

def createDict(shift):

    for i in range(0, 26):

        letter = alphabet[i]

        transAlphabet[letter] = alphabet[(i-shift+26) % 26]

def decodeText(text, key):

    real = False

    total = 0

    cipherText = ''

    for letter in text:

        if letter in transAlphabet:

            cipherText = cipherText+transAlphabet[letter]

        else:

            cipherText = cipherText+letter

    t = cipherText.split()

    for word in t:

        if d.check(word) == True:

            real = True

            total = total+1

    if total == len(t):

        print("Key:", key)

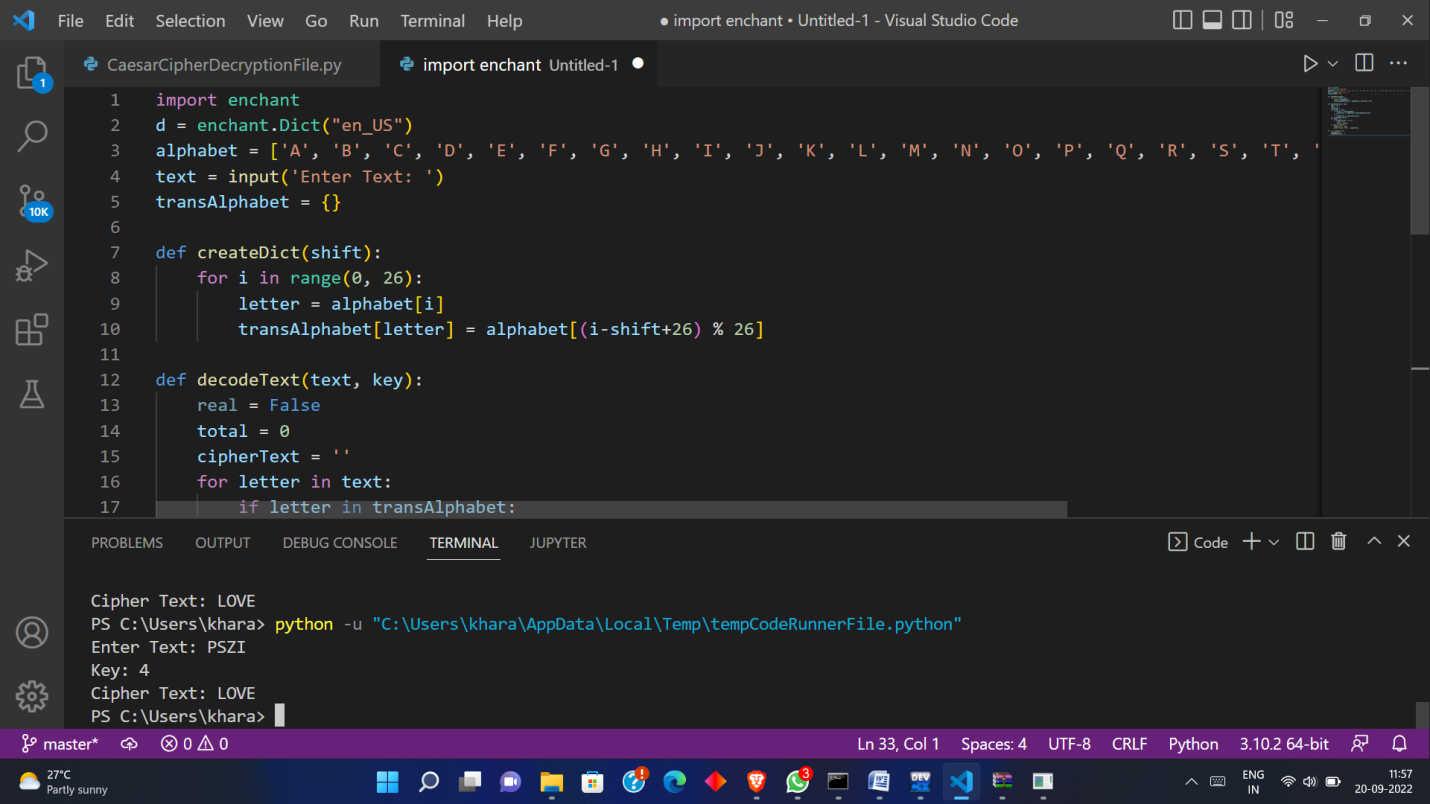
        print("Cipher Text:", cipherText)

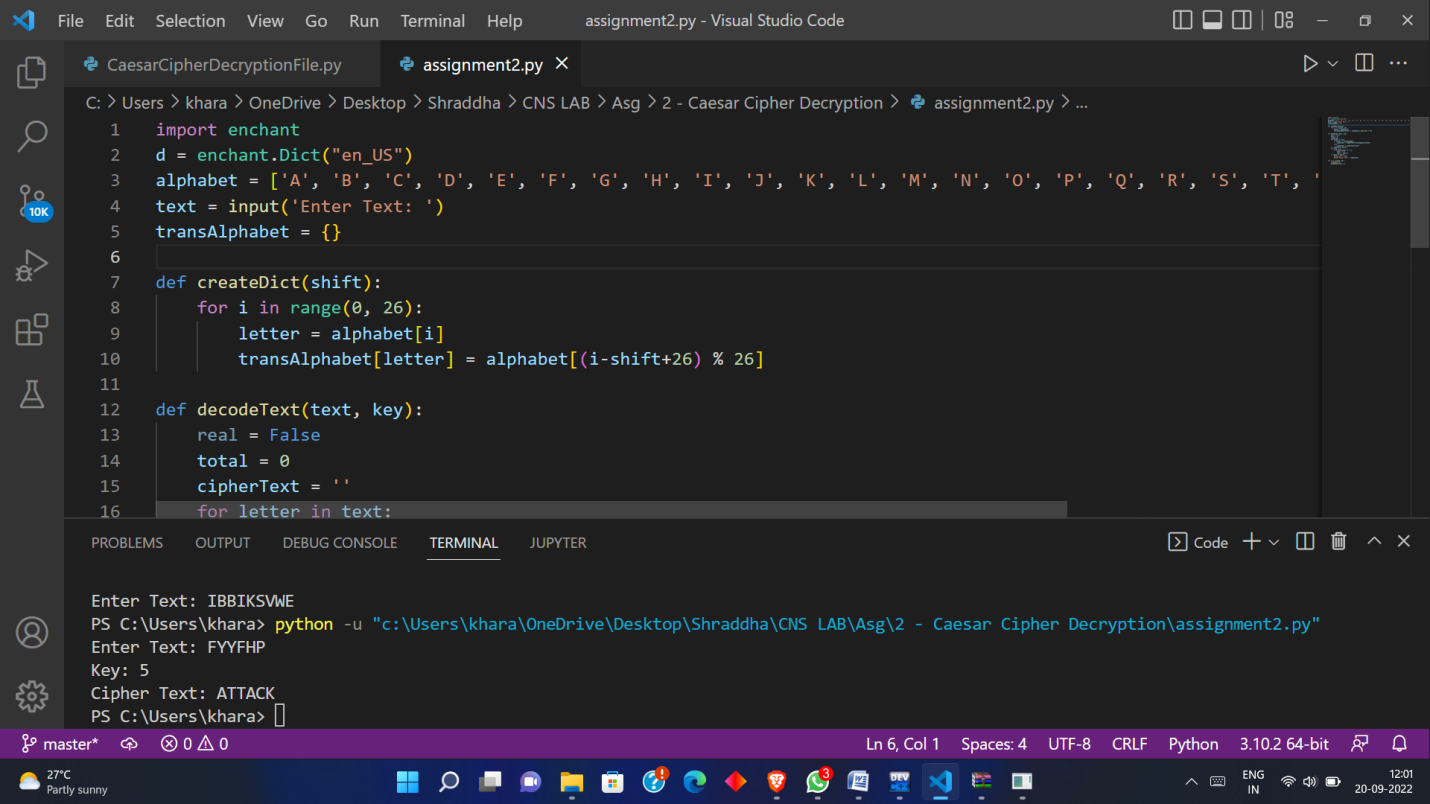
for i in range(0, 26):

    createDict(i)

    decodeText(text, i)

**Output:**





* **Conclusion** :

PyEnchant lilbrary is used for finding the meaningful output from suggested set of sentences as the shift is unknown.