**Assignment No 1**

**Cryptography and Network Security Lab (5CS453)**

**Name: Sumit Narake PRN: 2020BTECS00023**

**Class: Final Year - CSE**

**Title:**

**Encryption and Decryption using Ceaser Cipher.**

**Aim:**

**To Study and Implement Encryption and Decryption using Ceaser Cipher**

**Theory:**

* Caesar Cipher, also known as the Shift Cipher, is one of the simplest and oldest encryption techniques used to secure information.
* It's a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.
* The number of positions a letter is shifted is determined by a key.

**Encryption:**

**In Encryption, input is a Plain text and output is a Cipher text.**

* Choose a secret key (a positive integer).
* Take the plaintext message you want to encrypt.
* Shift each letter in the message forward in the alphabet by the key positions.
* Non-alphabetical characters remain unchanged.
* The result is the ciphertext, the encrypted message.

**Decryption:**

**In Decryption, input is a Cipher text and output is a Plain text.**

* Have the same key used for encryption.
* Take the ciphertext (the encrypted message).
* Shift each letter in the ciphertext backward in the alphabet by the key positions.
* Non-alphabetical characters remain unchanged.
* The result is the plaintext, the original message.

**Code:**

**Encryption:**

def encrypt(plain\_text, shift):

    caesar\_cipher = ""

    for char in plain\_text:

        if char == ' ':

            caesar\_cipher += ' '

        elif char.isupper():

            caesar\_cipher += chr((ord(char) + shift - 65) % 26 + 65)

        else:

            caesar\_cipher += chr((ord(char) + shift - 97) % 26 + 97)

    return caesar\_cipher

def main():

    plain\_text = input("enter plain text: ")

    print()

    shift = int(input("enter value of shift: "))

    print()

    caesar\_cipher = encrypt(plain\_text, shift)

    print("The Caesar cipher encrypted text is:")

    print(caesar\_cipher)

if \_\_name\_\_ == "\_\_main\_\_":

    main()

**Decryption:**

import nltk

from nltk.corpus import words

nltk.download("words")

english\_words = set(words.words())

def decrypt(ciphertext, s):

    result = ""

    for char in ciphertext:

        if char == " ":

            result += " "

        elif char.isupper():

            result += chr((ord(char) - s - 65) % 26 + 65)

        else:

            result += chr((ord(char) - s - 97) % 26 + 97)

    return result

def main():

    ciphertext = input("Enter encrypted text: ")

    print()

    shift\_key=0

    decrypted\_text\_store=""

    for s in range(1, 27):

        decrypted\_text = decrypt(ciphertext, s)

        decrypted\_words = decrypted\_text.split()

        # print(decrypted\_words)

        is\_valid = all(word.lower() in english\_words for word in decrypted\_words)

        if is\_valid:

            shift\_key=s

            decrypted\_text\_store=decrypted\_text

            break

    if s and decrypted\_text\_store:

        print("Valid decryption with shift key", shift\_key)

        print("Decrypted Text:", decrypted\_text)

    else:

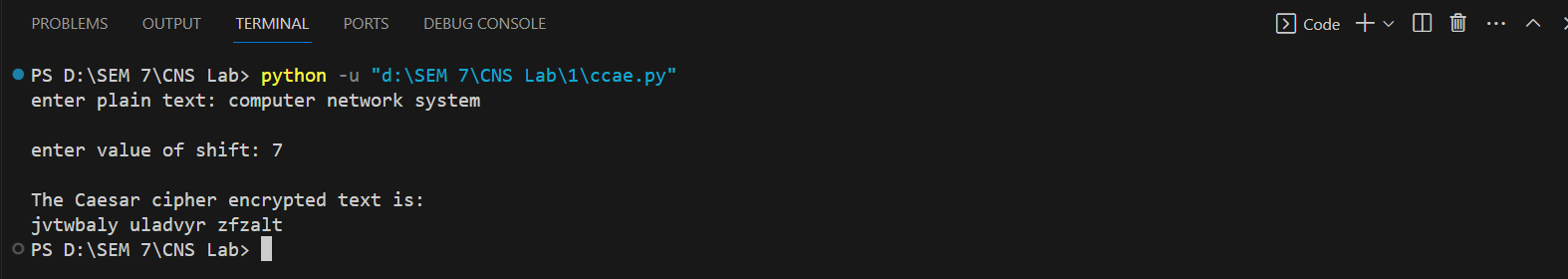
            print("Decryption Unsuccessful")

if \_\_name\_\_ == "\_\_main\_\_":

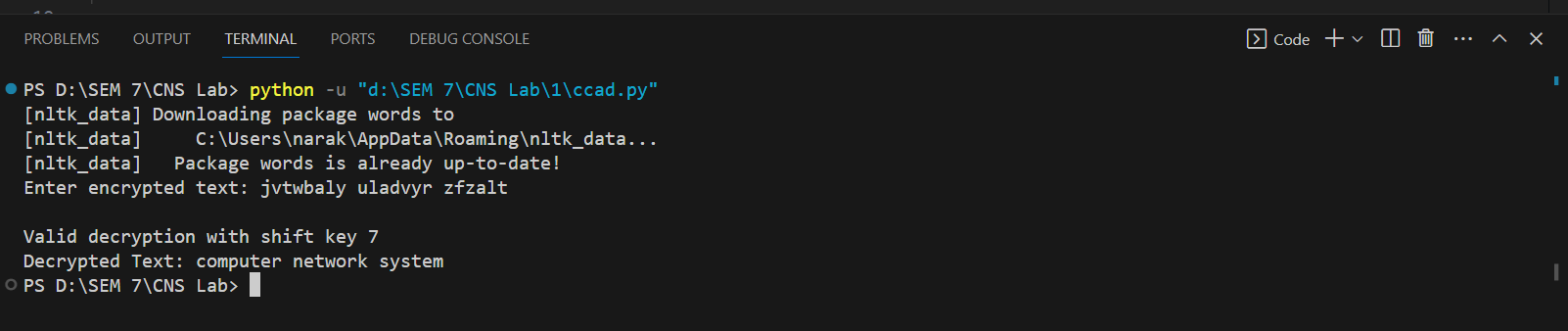
    main()

**Output:**

**Encryption:**

****

**Decryption:**

****