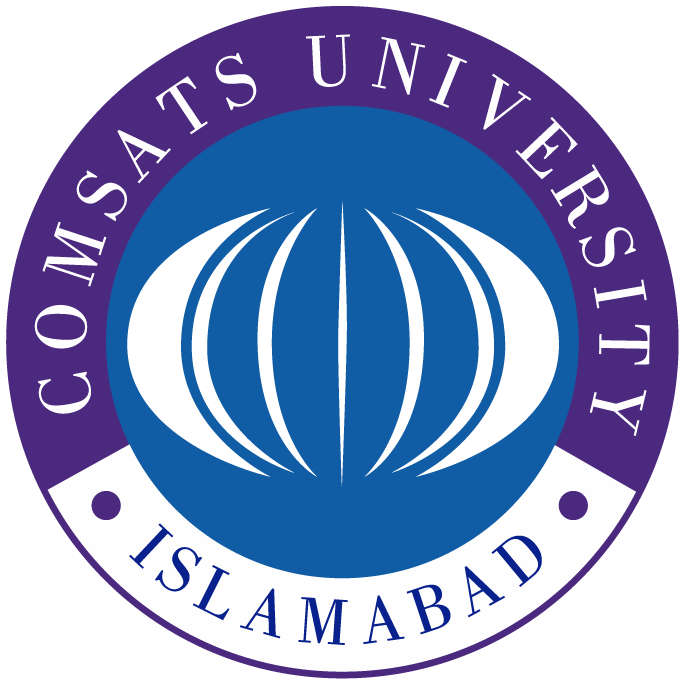
****

**COMSATS University Islamabad**

**(Attock Campus)**

**Professional Practices**

**lab**

**Instructor:** maam

**DATE:** October 20, 2025

**Submitted By:**

**Muhammad Hassan**

**SP24-BSE-008**

**Qno1:**

def caesar\_cipher(message, shift):

    encrypted\_message = ""

    for char in message:

        if char.isalpha():

            shift\_base = ord('a') if char.islower() else ord('A')

            encrypted\_char = chr((ord(char) - shift\_base + shift) % 26 + shift\_base)

            encrypted\_message += encrypted\_char

        else:

            encrypted\_message += char

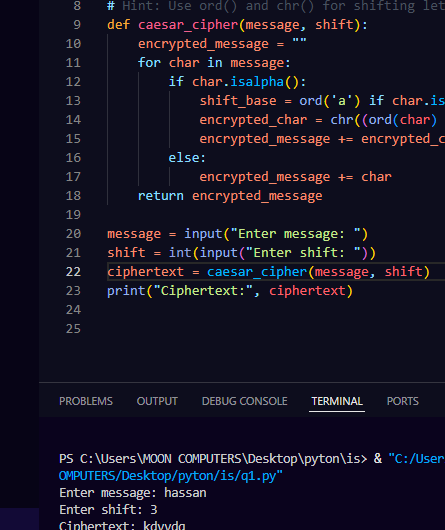
    return encrypted\_message

message = input("Enter message: ")

shift = int(input("Enter shift: "))

ciphertext = caesar\_cipher(message, shift)

print("Ciphertext:", ciphertext)



**Qno 2:**

def vigenere(text, key):

    result = ""

    key = key.upper()

    for i, char in enumerate(text):

        if char.isalpha():

            shift = ord(key[i % len(key)]) - 65

            if char.isupper():

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

            else:

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

        else:

            result += char

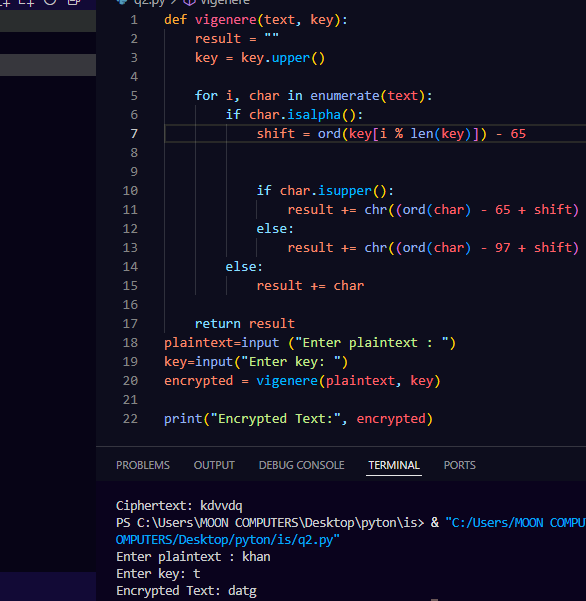
    return result

plaintext=input ("Enter plaintext : ")

key=input("Enter key: ")

encrypted = vigenere(plaintext, key)

print("Encrypted Text:", encrypted)



**Qno3:**

def xor\_encrypt(text, key):

    result = ""

    key\_index = 0

    for char in text:

        result += chr(ord(char) ^ ord(key[key\_index]))

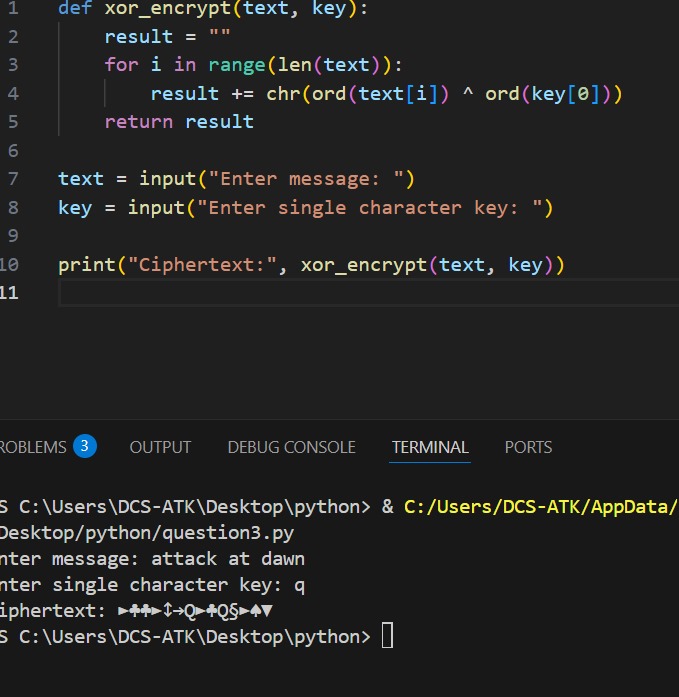
        key\_index = (key\_index + 1) % len(key)

    return result

text = input("Enter message: ")

key = input("Enter key: ")

print("Ciphertext:", xor\_encrypt(text, key))



**Qno5:**

## a) One difference between DES and AES

**DES (Data Encryption Standard)** uses a Feistel network structure, while **AES (Advanced Encryption Standard)** uses a substitution-permutation network (SPN) structure. DES operates on 64-bit blocks, whereas AES operates on 128-bit blocks.

## b) AES block size and one key size

* **AES block size:** 128 bits
* **One AES key size:** 128 bits (other options are 192 bits and 256 bits)

## c) One reason why AES is more secure than DES

## AES is more secure than DES because it uses much longer key lengths (128/192/256 bits) compared to DES's 56-bit effective key length, making AES resistant to brute-force attacks that are practical against DES