# Comsats university islamabad, attock campus

# LAB MIDTERM



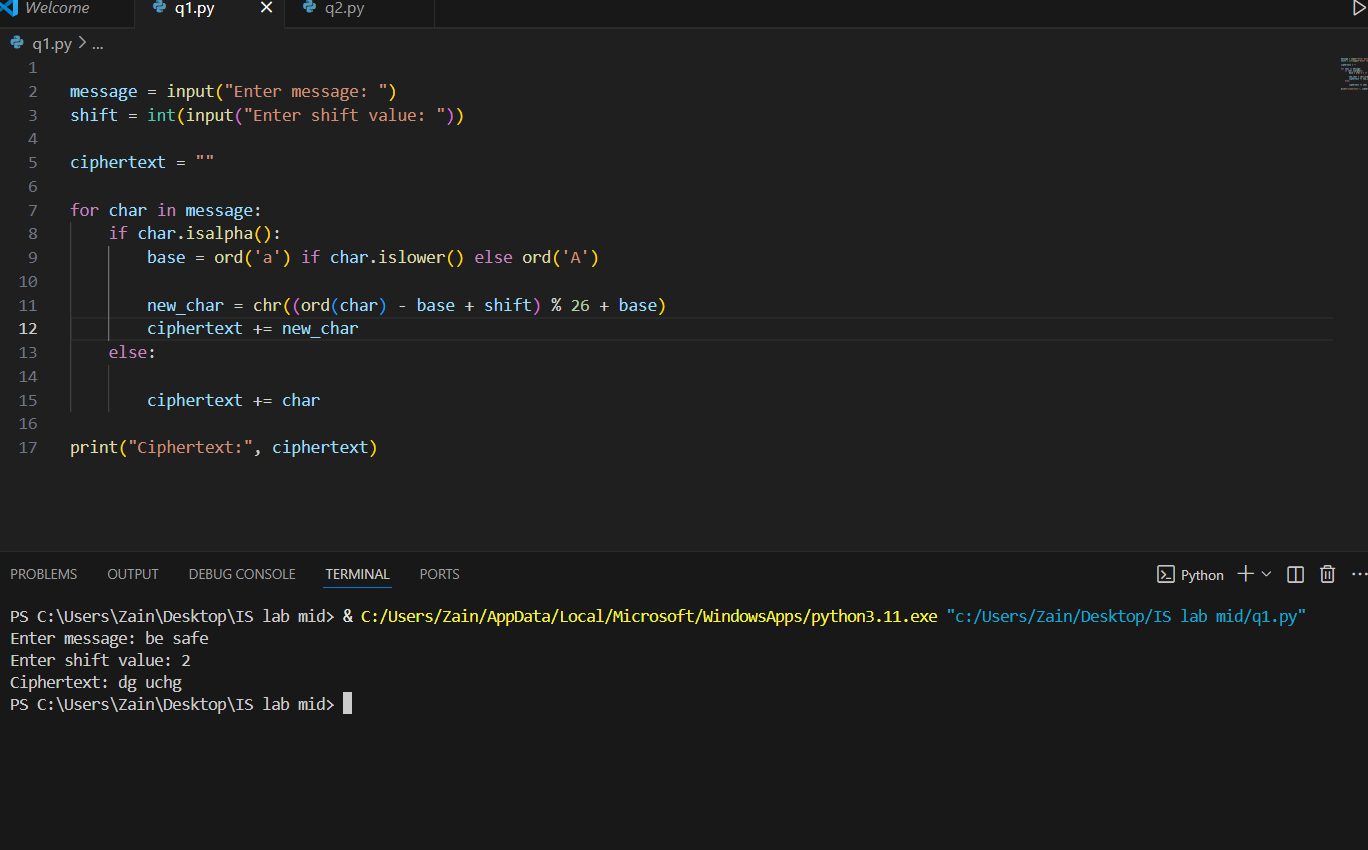
|  |  |
| --- | --- |
| NAME | ZAIN-UL-ABEDIN |
| REG NO. | SP24-BSE-029 |
| LAB MID TERM | IS LAB |
| DATE | 20-10-2025 |
| Submitted to | Mam,Ambreen khan |

**Question 1**

**Caesar Cipher**

Write a Python program that encrypts a message using the Caesar Cipher with a user-given shift value.  
  
Example:  
Enter message: hello  
Enter shift: 3  
Ciphertext: khoor  
  
Hint: Use ord() and chr() for shifting letters.

**Screenshots**



**CODE**

message = input("Enter message: ")

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

ciphertext = ""

for char in message:

    if char.isalpha():

        base = ord('a') if char.islower() else ord('A')

        new\_char = chr((ord(char) - base + shift) % 26 + base)

        ciphertext += new\_char

    else:

        ciphertext += char

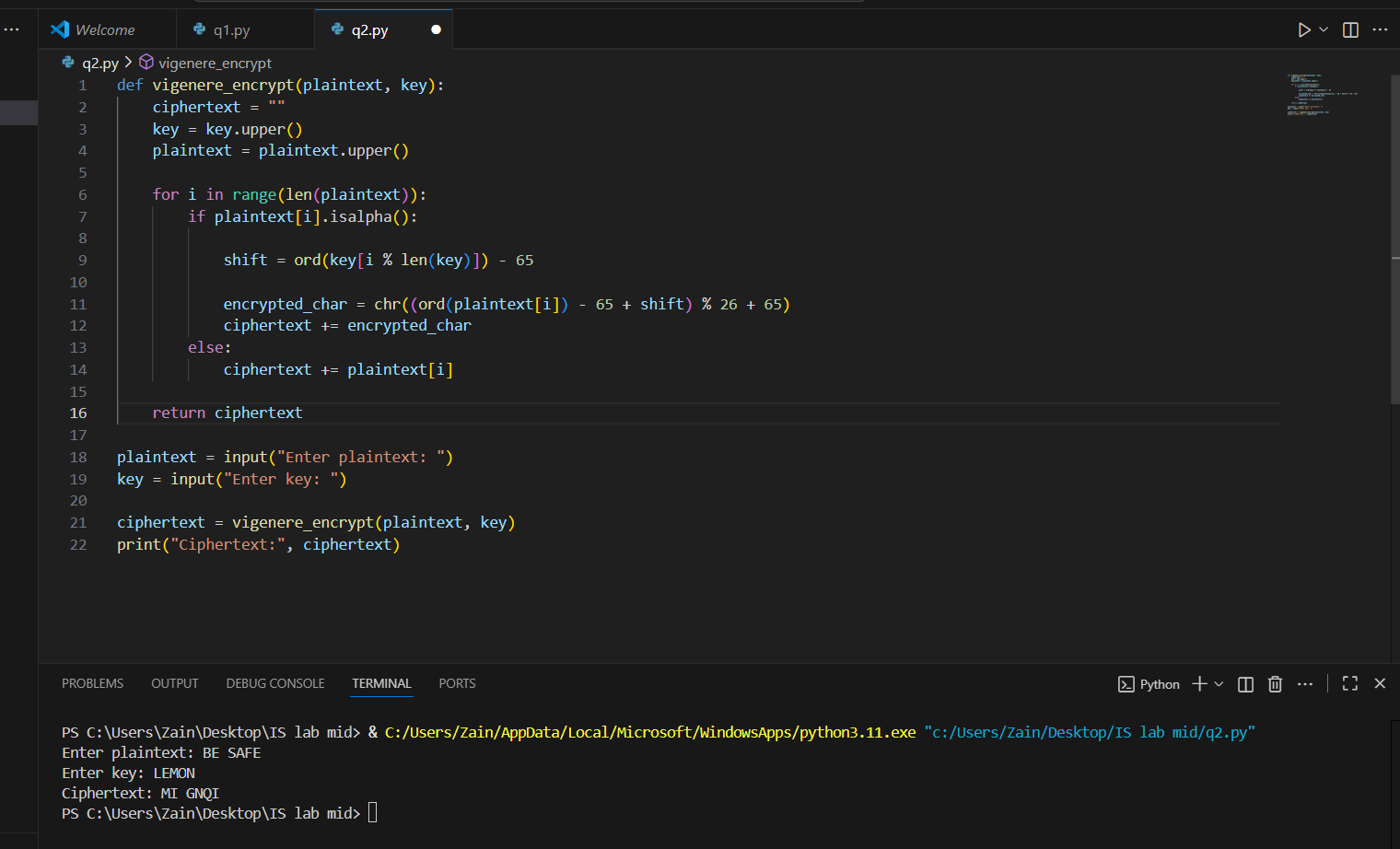
print("Ciphertext:", ciphertext)

**Question 2**

**Vigenère Cipher (Encryption Only)**

Write a Python program to encrypt a plaintext message using the Vigenère Cipher. Ask the user for plaintext and keyword. Display the ciphertext only.  
  
Example:  
Enter plaintext: BE SAFE  
Enter key: LEMON  
Ciphertext: LXFOPVEFRNHR

**SCREENSHOT**



**CODE**

def vigenere\_encrypt(plaintext, key):

    ciphertext = ""

    key = key.upper()

    plaintext = plaintext.upper()

    for i in range(len(plaintext)):

        if plaintext[i].isalpha():

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

            encrypted\_char = chr((ord(plaintext[i]) - 65 + shift) % 26 + 65)

            ciphertext += encrypted\_char

        else:

            ciphertext += plaintext[i]

    return ciphertext

plaintext = input("Enter plaintext: ")

key = input("Enter key: ")

ciphertext = vigenere\_encrypt(plaintext, key)

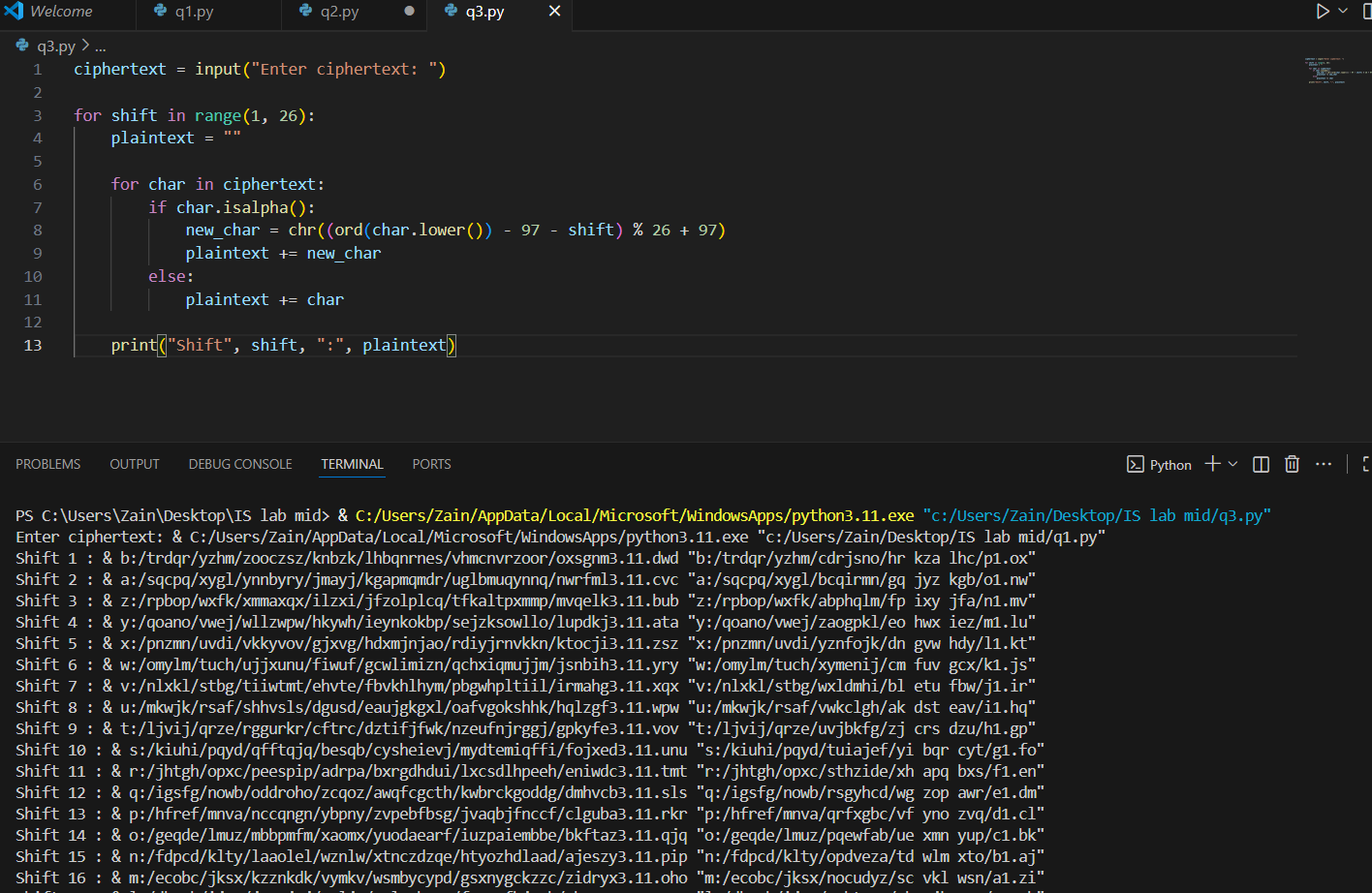
print("Ciphertext:", ciphertext)

**QUESTION 3 (part ii)**

**Caesar Cipher Decryption (Simple Brute Force)**

You are given a Caesar Cipher ciphertext. Write a Python program to try all 25 possible shift values and print each possible plaintext.  
  
Example Input:  
Ciphertext: khoor  
  
Expected Output:  
Shift 1: jgnnq  
Shift 2: ifmmp  
Shift 3: hello <-- correct plaintext

**SCREENSHOT**



**CODE**

ciphertext = input("Enter ciphertext: ")

for shift in range(1, 26):

    plaintext = ""

    for char in ciphertext:

        if char.isalpha():

            new\_char = chr((ord(char.lower()) - 97 - shift) % 26 + 97)

            plaintext += new\_char

        else:

            plaintext += char

    print("Shift", shift, ":", plaintext)

**Question (5)**

**ANSWERS.**

**a)**

One difference between DES and AES:

DES uses a 56-bit key, while AES uses 128, 192, or 256-bit keys.

**b)**

AES block size and one key size:

AES block size is 128 bits, and one key size is 128 bits.

**c)**

One reason why AES is more secure than DES:

AES has a larger key size, making it much harder to break by brute-force attacks.