**IS LAB**

**MID TERM**

**By:**

**SAARAM HUSSNAIN**

**SP24-BSE-011**

**Submitted to:**

**MAM. AMBREEN GUL**

**Department of Computer Science**

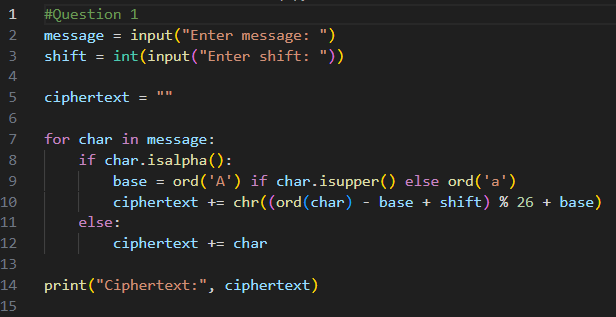
COMSATS University Islamabad,

Attock Campus

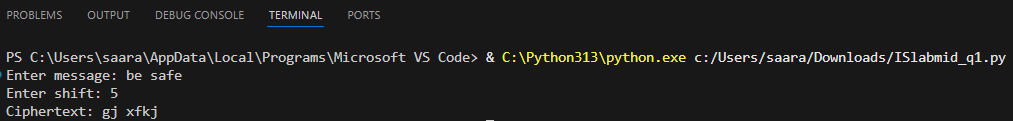
**Question 1**

**Caesar Cipher**

Write a Python program that encrypts a message using the Caesar Cipher with a user-given shift value.



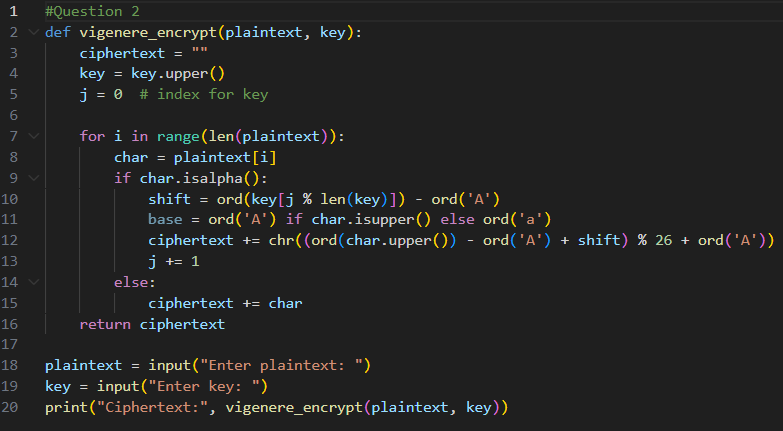
OUTPUT:



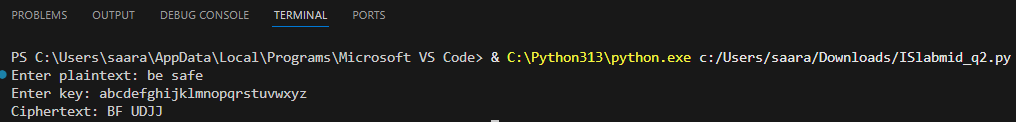
**Question 2**

**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.



OUTPUT:

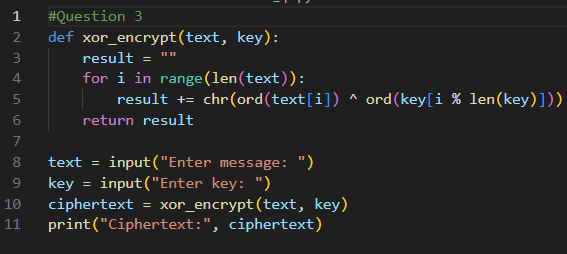


**Question 3**

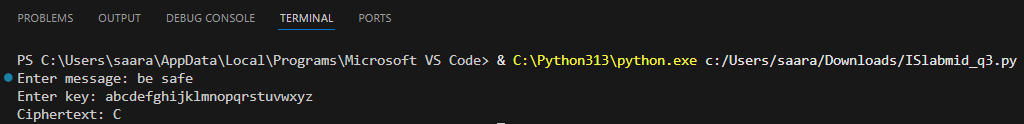
**Debugging Task (Simple XOR Encryption)**

The following program is supposed to perform XOR encryption, but it contains an error. Fix the mistake so that it correctly shows the ciphertext.

def xor\_encrypt(text, key):  
 result = ""  
 for i in range(len(text)):  
 result += chr(ord(text[i]) ^ ord(key)) # Error in code  
 return result  
  
text = input("Enter message: ")  
key = input("Enter single character key: ")  
print("Ciphertext:", xor\_encrypt(text, key))

****

**Output:**

****

**Question 4**

**DES and AES**

Answer briefly:  
  
a) One difference between DES and AES.  
b) AES block size and one key size.  
c) One reason why AES is more secure than DES.

**a) One difference between DES and AES:**

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

**b) AES block size and one key size:**

AES block size = 128 bits.

One key size = 128 bits.

**c) One reason why AES is more secure than DES:**

AES uses a larger key size and stronger substitution permutation structure, making it harder to break by brute force.