**COMSATS University Islamabad, Attock Campus**

**Department of Computer Science**

**Program: SE IV**

**Fall 2025: Mid Term Examination Group-B**

**Course: Information Security**

**Time Allowed: 90 Minutes Marks: 25**

**Name:- Tehseen Hamid Regn. No:- SP24-BSE-046**

**Note:- Don’t write anything on Question Paper except your Name & Regn. No.**

## Question 1 – Simple XOR Encryption & Decryption [10 Marks]

Write a Python program that performs both encryption and decryption using XOR operation.  
  
Requirements:  
1. Ask the user for message and a single-character key.  
2. Encrypt the message using XOR (ord() and chr()).  
3. Decrypt it by applying XOR again with the same key.  
4. Show both ciphertext and decrypted plaintext.  
  
Example:  
Enter message: HELLO  
Enter key: A  
Ciphertext: !%&&$  
Decrypted text: HELLO

OR

## Question 2 – Caesar Cipher (Decryption) [10 Marks]

Write a Python program to decrypt a message that was encrypted using the Caesar Cipher. The program should take ciphertext (LXFOPVEFRNHR) and key (5) as input and display the plaintext.  
  
Example:  
Enter ciphertext: khoor  
Enter shift: 3  
Plaintext: hello  
  
Hint: Use ord() and chr() for letter shifting backward.

*[CLO4: Implement a cryptographic algorithm to ensure information security.]*

## Question 3 – Vigenère Cipher (Decryption Only) [5 Marks]

Write a Python program to decrypt a ciphertext using the Vigenère Cipher. Ask the user for ciphertext and key, and display the decrypted plaintext.  
  
Example:  
Enter ciphertext: LXFOPVEFRNHR  
Enter key: LEMON  
Plaintext: ATTACKATDAWN

*[CLO4: Implement a cryptographic algorithm to ensure information security.]*

## Question 4 – Debugging Task (Caesar Cipher Code) [5 Marks]

The following program is intended to encrypt text using the Caesar Cipher, but it contains an error. Fix the mistake so that it runs correctly and gives the right output.

* def caesar\_encrypt(text, shift):  
   result = ""  
   for char in text:  
   if char.isalpha():  
   result += chr(ord(char) + shift)   
   else:  
   result += char  
   return result  
    
  msg = input("Enter message: ")  
  s = int(input("Enter shift: "))  
  print("Ciphertext:", caesar\_encrypt(msg, s))

Hint: The code doesn’t wrap around alphabets (A–Z or a–z). Use modular arithmetic to fix the shifting logic.

*[CLO4: Implement a cryptographic algorithm to ensure information security.]*

## Question 5 – Conceptual: DES and AES [5 Marks]

Answer briefly:  
  
a) Write one similarity between DES and AES. (2 marks)  
b) What does CBC mode stand for in block ciphers? (2 marks)  
c) Why is AES faster than DES? (1 mark)

*[CLO4: Implement a cryptographic algorithm to ensure information security.]*

**Instructions for submission:-**

Create a Word file (.docx) named:

YourName\_YourRegNo\_ISMid.docx

Total five questions are given. Attempt any four questions.

For Each Programming Question:

1. Write the Python code for the question.

2. Run the code on your system (e.g., IDLE, PyCharm, Jupyter Notebook, or Google Colab).

3. Take screenshots of input and output for each question.

4. Paste the code and screenshots neatly in the Word file.

For Question 5 (Conceptual):

Type your short answers directly in the Word file below the question.

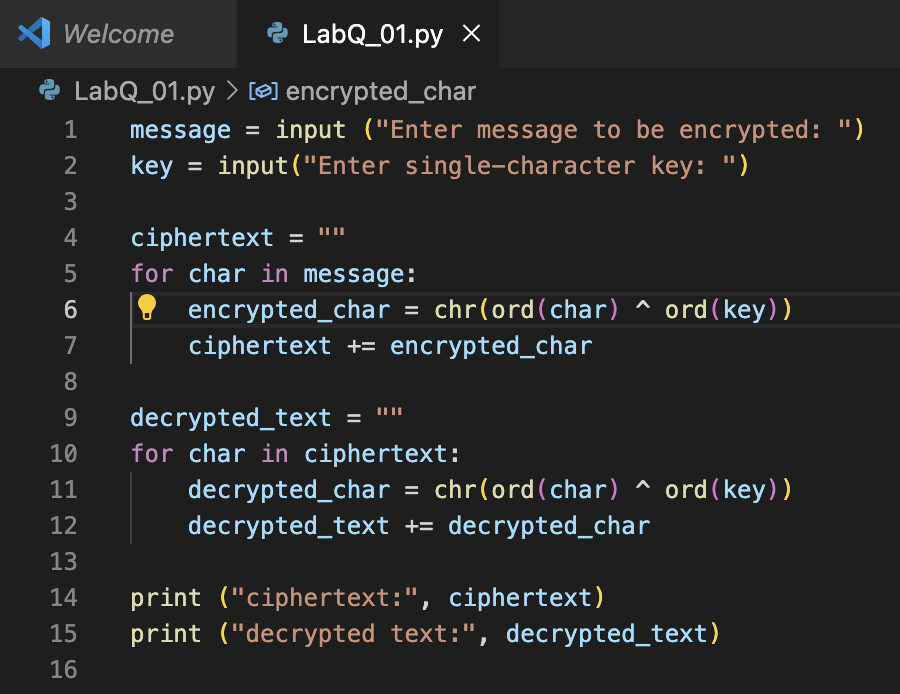
Upload on github and submit via Google forms link

**:SOLUTION:**

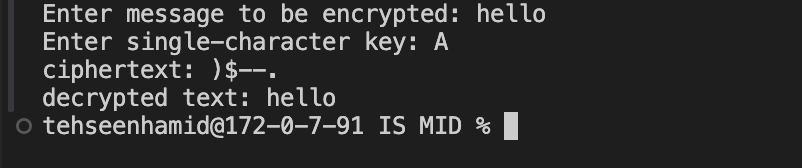
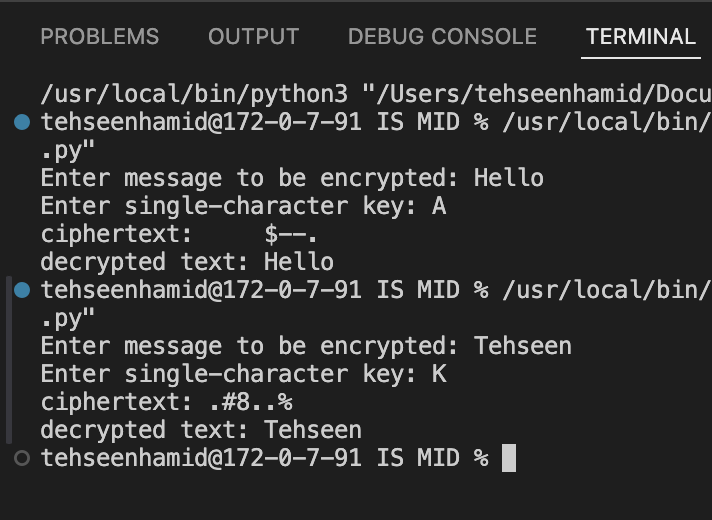
## Question 1 – Simple XOR Encryption & Decryption [10 Marks]

Write a Python program that performs both encryption and decryption using XOR operation.  
  
Requirements:  
1. Ask the user for message and a single-character key.  
2. Encrypt the message using XOR (ord() and chr()).  
3. Decrypt it by applying XOR again with the same key.  
4. Show both ciphertext and decrypted plaintext. **SOLUTION**

***Code:***



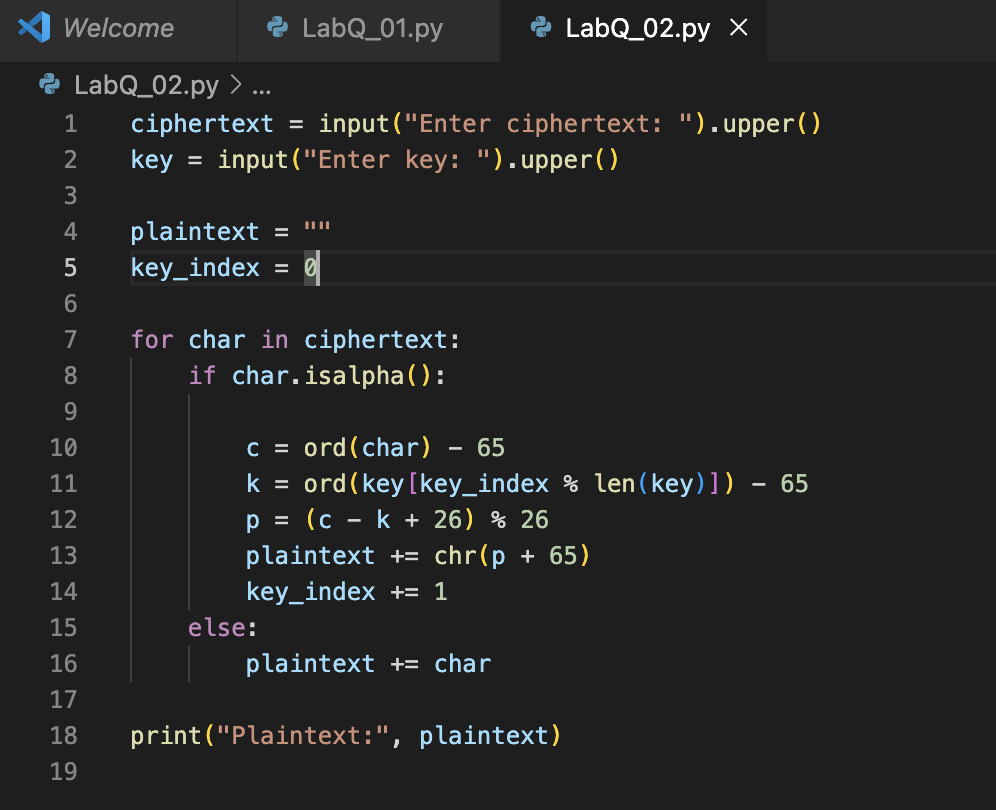
***Output:***

******

## Question 3 – Vigenère Cipher (Decryption Only) [5 Marks]

Write a Python program to decrypt a ciphertext using the Vigenère Cipher. Ask the user for ciphertext and key, and display the decrypted plaintext.  
  
**SOLUTION:**

***Code:***

******

***Output:***

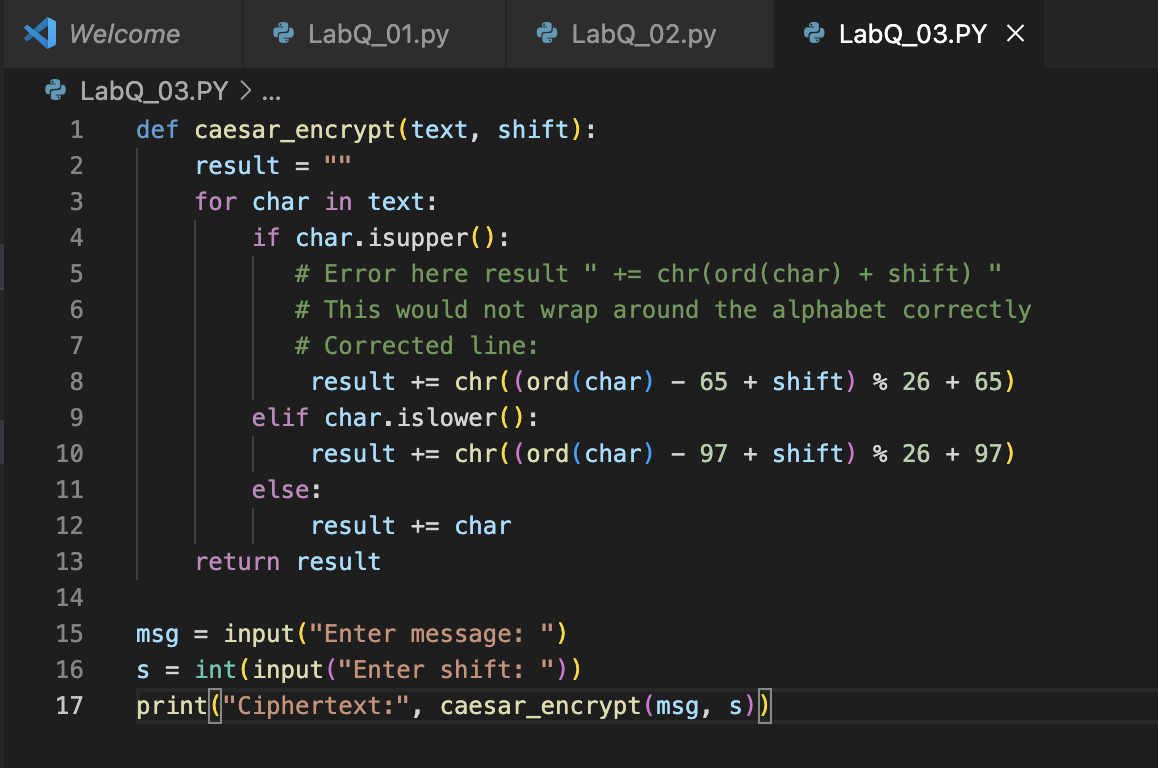
******

## Question 4 – Debugging Task (Caesar Cipher Code) [5 Marks]

The following program is intended to encrypt text using the Caesar Cipher, but it contains an error. Fix the mistake so that it runs correctly and gives the right output.

**SOLUTION:**

***Code:***



***Output:***

******

## Question 5 – Conceptual: DES and AES [5 Marks]

Answer briefly:  
  
a) Write one similarity between DES and AES. (2 marks)  
b) What does CBC mode stand for in block ciphers? (2 marks)  
c) Why is AES faster than DES? (1 mark)

*[CLO4: Implement a cryptographic algorithm to ensure information security.]*

***SOLUTION:***

1. **Similarity between DES and AES**

***ANSWER:***

🡪 Both DES and AES are **symmetric key block ciphers**, meaning they use the **same key** for both encryption and decryption.

1. **What does CBC mode stand for?**

***ANSWER:***

🡪 CBC stands for **Cipher Block Chaining**

***Definition:*** It is a block cipher mode where **each plaintext block is XORed with the previous ciphertext block** before encryption to increase security.

1. **Why is AES faster than DES?**

***ANSWER:***

🡪 AES is faster because it works on **larger 128-bit blocks** and uses **more efficient substitution–permutation operations**, while DES uses **smaller 64-bit blocks** and slower bit-level processing.