**COMSATS University Islamabad, Attock Campus**

**Department of Computer Science**

**Program: SE IV**

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

**Course: Information Security**

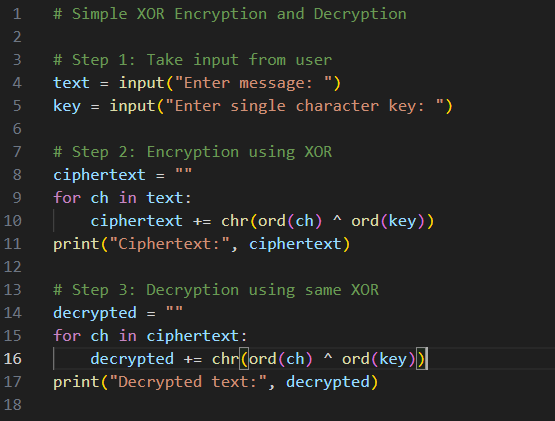
**Time Allowed: 90 Minutes Marks: 25**

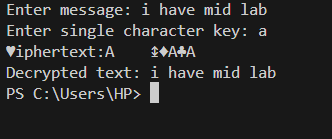
**Name:- MISBAH UR REHMAN SAIM**

**Regn. NoSP24-BSE-036**

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

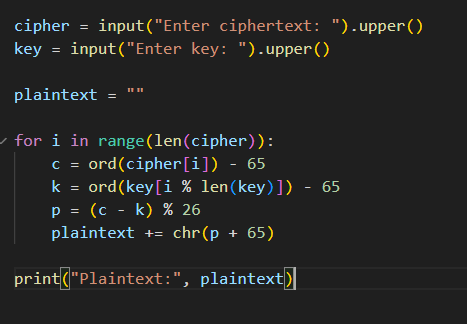
**Answer:**

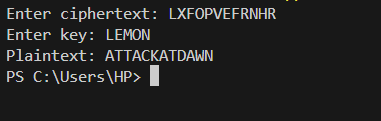




**Question 3 – Vigenère Cipher (Decryption Only)**

**Answer:**





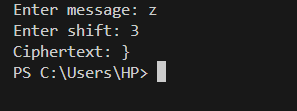
**Question 4 – Debugging Task**

**Answer:**

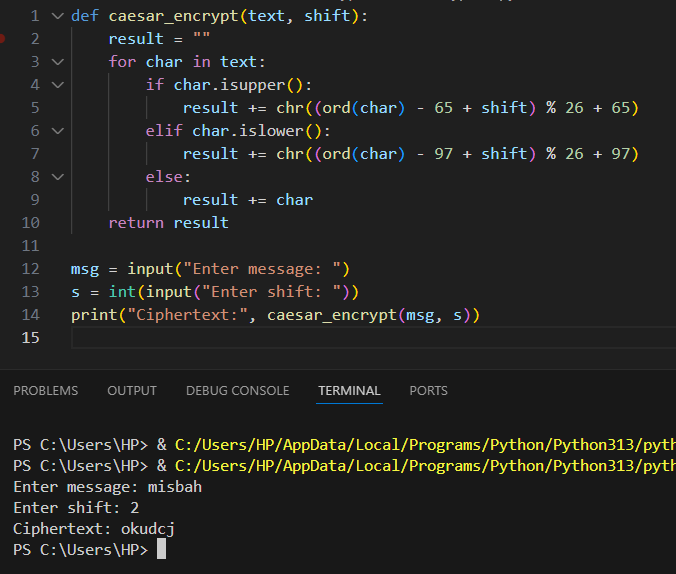
**Problem**

The given code didn’t wrap around alphabets when the shift went past ‘Z’ or ‘z’.

**result += chr(ord(char) + shift) # ❌ Problem line**



**Solution:**



**Question 5 – Conceptual: DES and AES**

**Answer:**

1. **Write one similarity between DES and AES.**

Both are **symmetric block ciphers** that use the **same secret key** for encryption and decryption.

1. **What does CBC mode stand for in block ciphers?**

CBC stands for **Cipher Block Chaining**. Each plaintext block is **XORed with the previous ciphertext block** before encryption to add randomness.

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

AES is faster because it operates on **128-bit blocks** and uses efficient **byte-oriented operations** optimized for modern hardware.