COMSATS University Islamabad, Attock Campus

Department of Computer Science

Program: SE IV

Fall 2025: Mid Term Examination Group-B

Course: Information Security

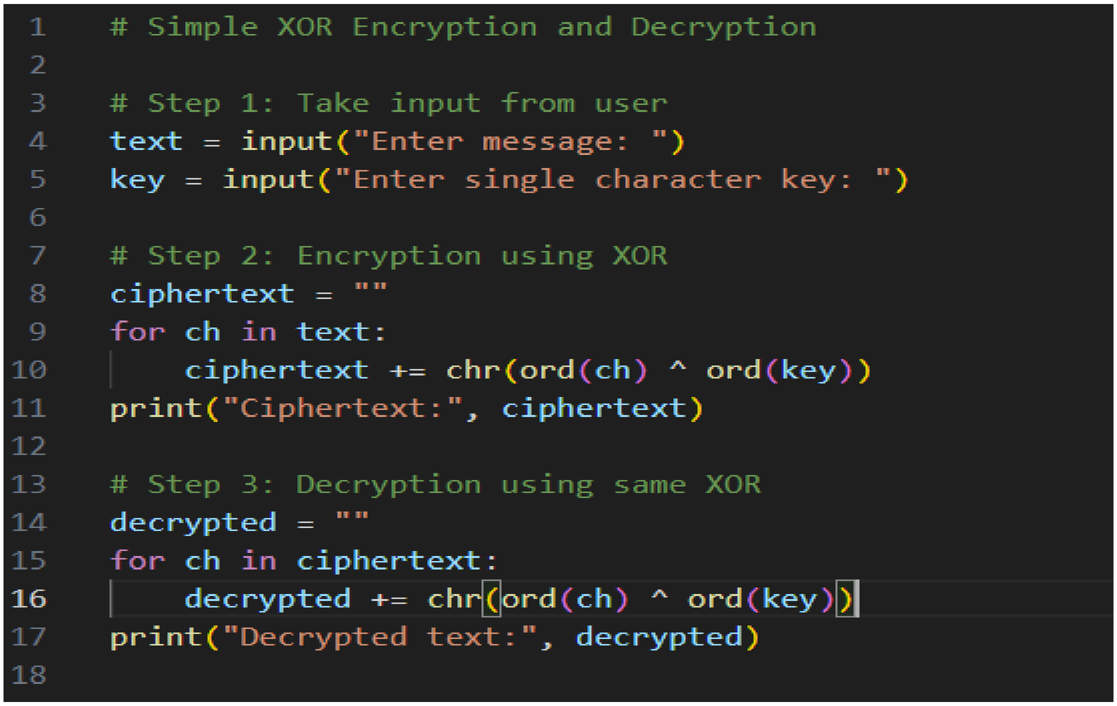
Time Allowed: 90 Minutes **Marks: 25**

Name:- MISBAH UR REHMAN SAIM

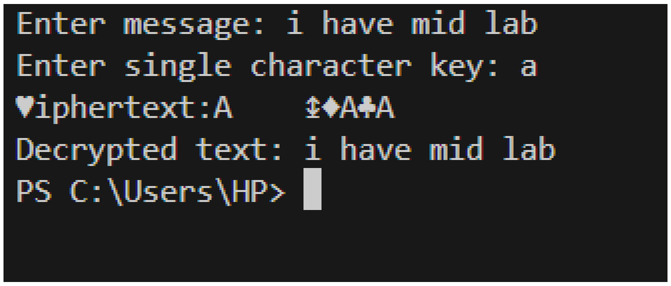
Regn. NoSP24-BSE-036

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

Answer:



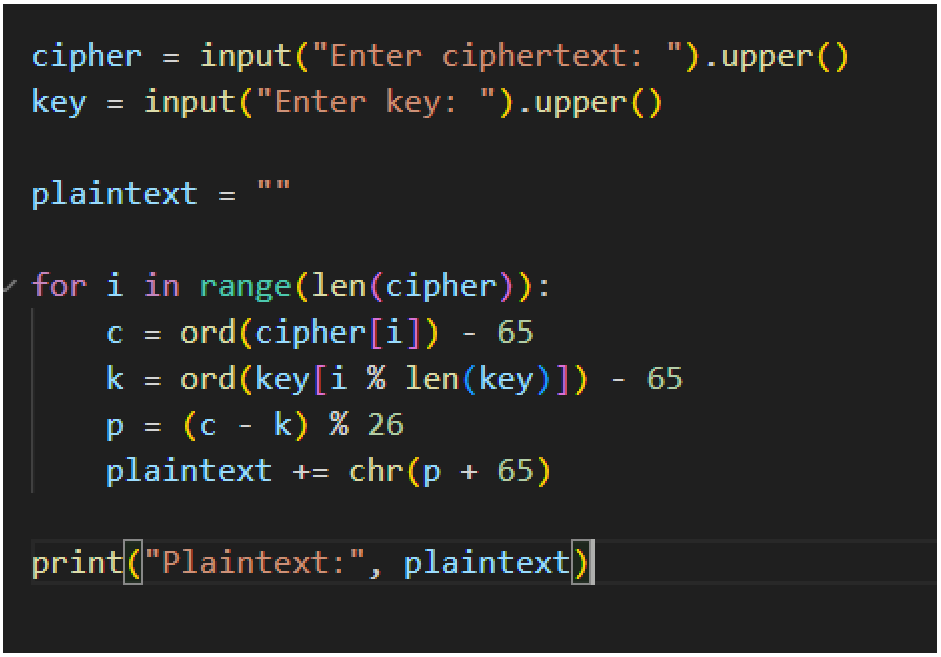
```python
# Simple XOR Encryption and Decryption

# Step 1: Take input from user
text = input("Enter message: ")
key = input("Enter single character key: ")

# Step 2: Encryption using XOR
ciphertext = ""
for ch in text:
    ciphertext += chr(ord(ch) ^ ord(key))
print("Ciphertext:", ciphertext)

# Step 3: Decryption using same XOR
decrypted = ""
for ch in ciphertext:
    decrypted += chr(ord(ch) ^ ord(key))
print("Decrypted text:", decrypted)
```



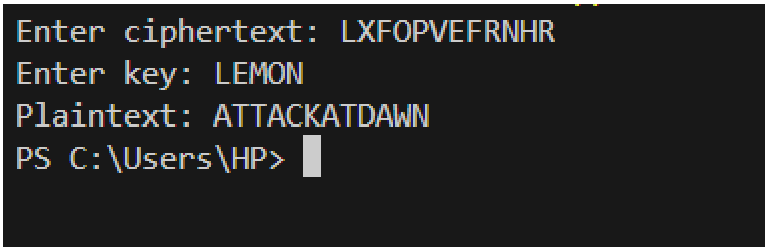
```
Enter message: i have mid lab
Enter single character key: a
♥iphertext:A    ↨♦A♣A
Decrypted text: i have mid lab
PS C:\Users\HP> 
```

Question 3 – Vigenère Cipher (Decryption Only)

Answer:



```python
cipher = input("Enter ciphertext: ").upper()
key = input("Enter key: ").upper()

plaintext = ""

for i in range(len(cipher)):
    c = ord(cipher[i]) - 65
    k = ord(key[i % len(key)]) - 65
    p = (c - k) % 26
    plaintext += chr(p + 65)

print("Plaintext:", plaintext)
```



```
Enter ciphertext: LXFOPVEFRNHR
Enter key: LEMON
Plaintext: ATTACKATDAWN
PS C:\Users\HP> 
```

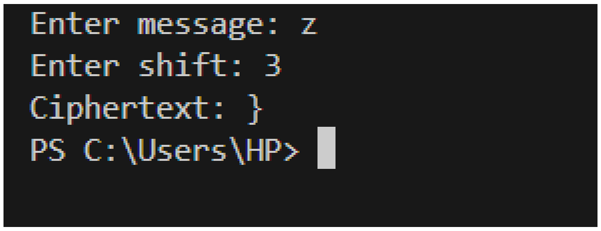
Question 4 – Debugging Task

Answer:

Problem

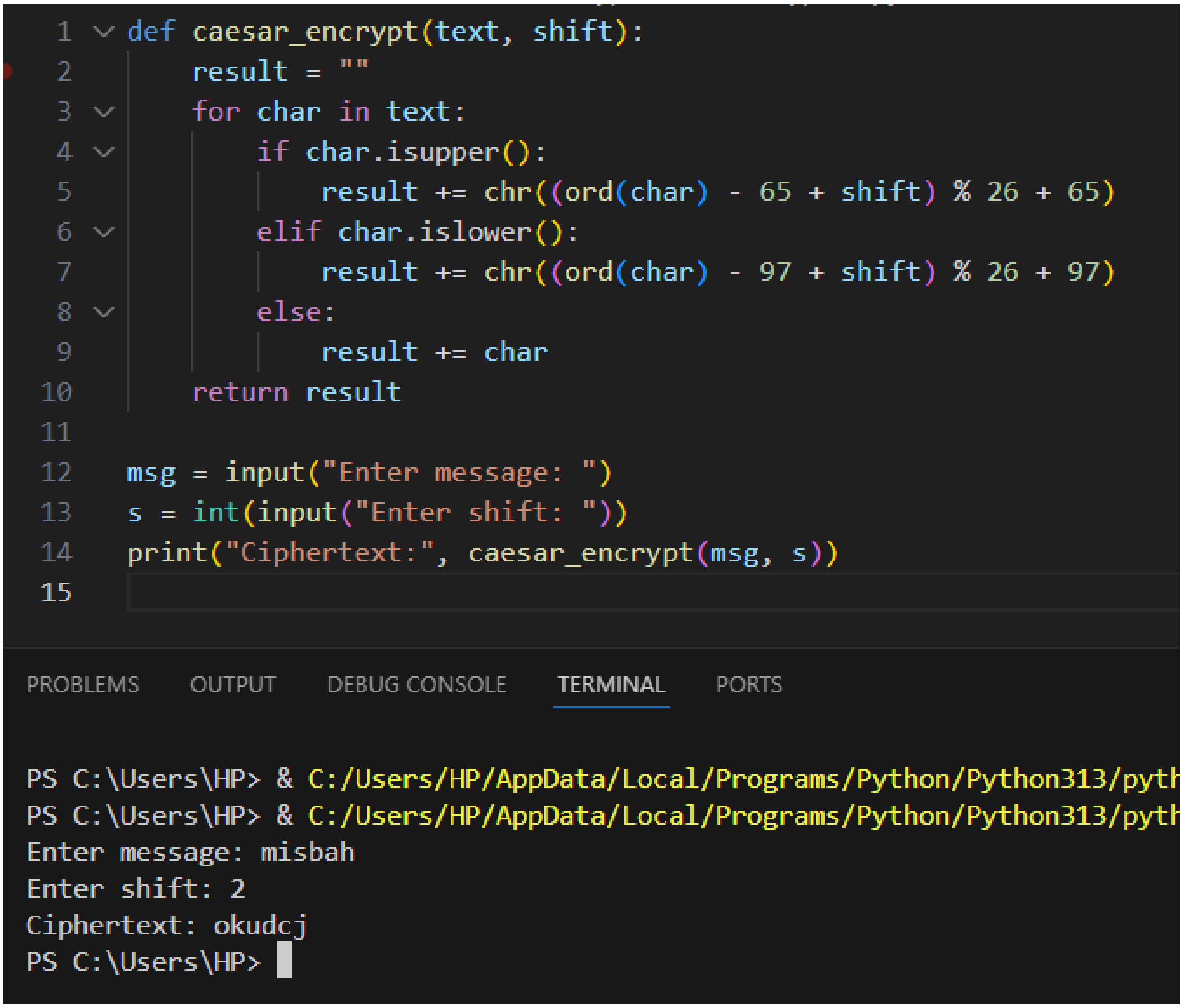
The given code didn’t wrap around alphabets when the shift went past ‘Z’ or ‘z’.

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



```
Enter message: z
Enter shift: 3
Ciphertext: }
PS C:\Users\HP>
```

Solution:



```python
def caesar_encrypt(text, shift):
    result = ""
    for char in text:
        if char.isupper():
            result += chr((ord(char) - 65 + shift) % 26 + 65)
        elif char.islower():
            result += chr((ord(char) - 97 + shift) % 26 + 97)
        else:
            result += char
    return result

msg = input("Enter message: ")
s = int(input("Enter shift: "))
print("Ciphertext:", caesar_encrypt(msg, s))

```

```
PS C:\Users\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python313/pyth
PS C:\Users\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python313/pyth
Enter message: misbah
Enter shift: 2
Ciphertext: okudcj
PS C:\Users\HP>
```

Question 5 – Conceptual: DES and AES

Answer:

a) **Write one similarity between DES and AES.**

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

b) **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.

c) **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.