

**LAB MIDTERM**

**INFORMATION SECURITY**

**WALEEJA ANSAR SP24\_ BSE\_ 061**

**MAM ANMBREEN**

QUESTION NO 1:

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.

ciphertext = input("Enter ciphertext: ").upper()

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

plaintext = ""

for char in ciphertext:

if char.isalpha():

decrypted = chr((ord(char) - 65 - shift) % 26 + 65)

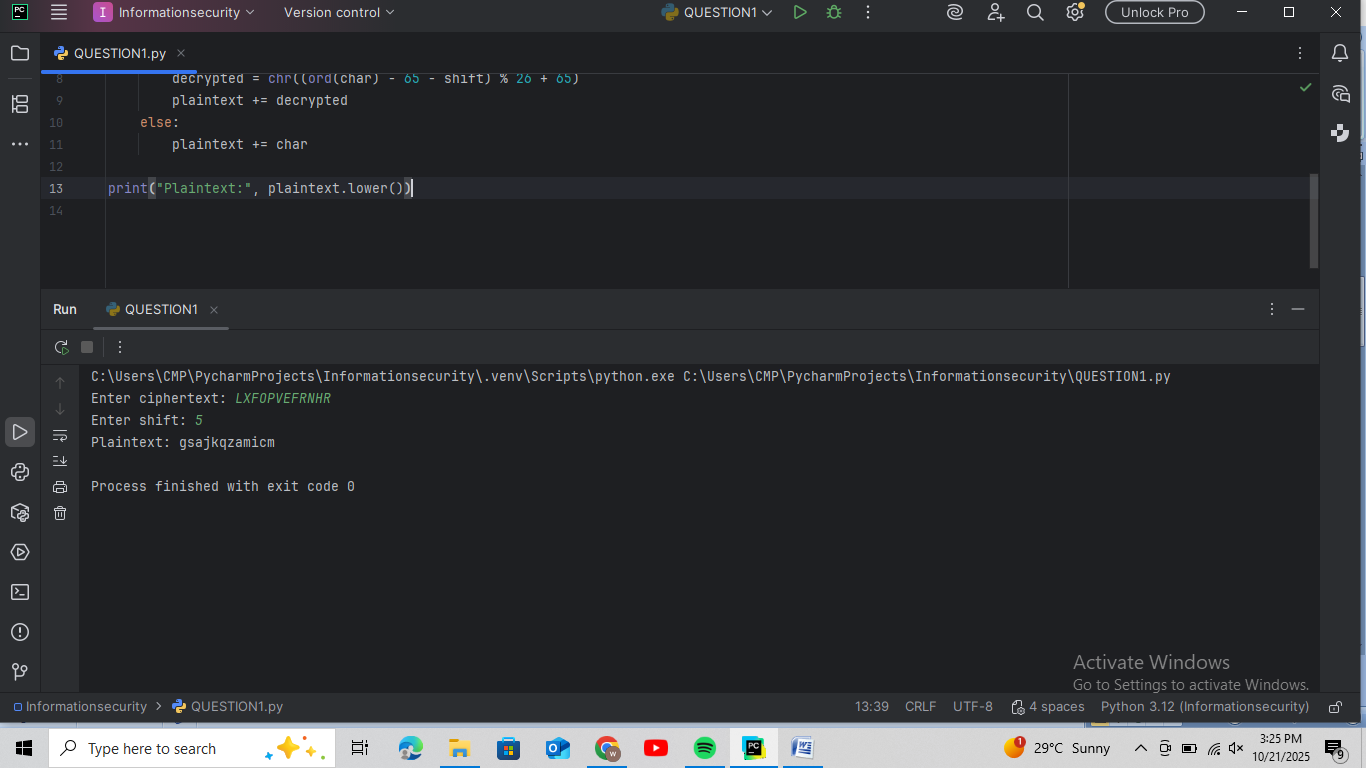
plaintext += decrypted

else:

plaintext += char

print("Plaintext:", plaintext.lower())

OUTPUT:



## **Question 2 – 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

ciphertext = input("Enter ciphertext: ").upper()

key = input("Enter key: ").upper()

plaintext = ""

key\_index = 0

for char in ciphertext:

if char.isalpha():

c\_val = ord(char) - 65

k\_val = ord(key[key\_index % len(key)]) - 65

p\_val = (c\_val - k\_val) % 26

# Convert back to letter

plaintext += chr(p\_val + 65)

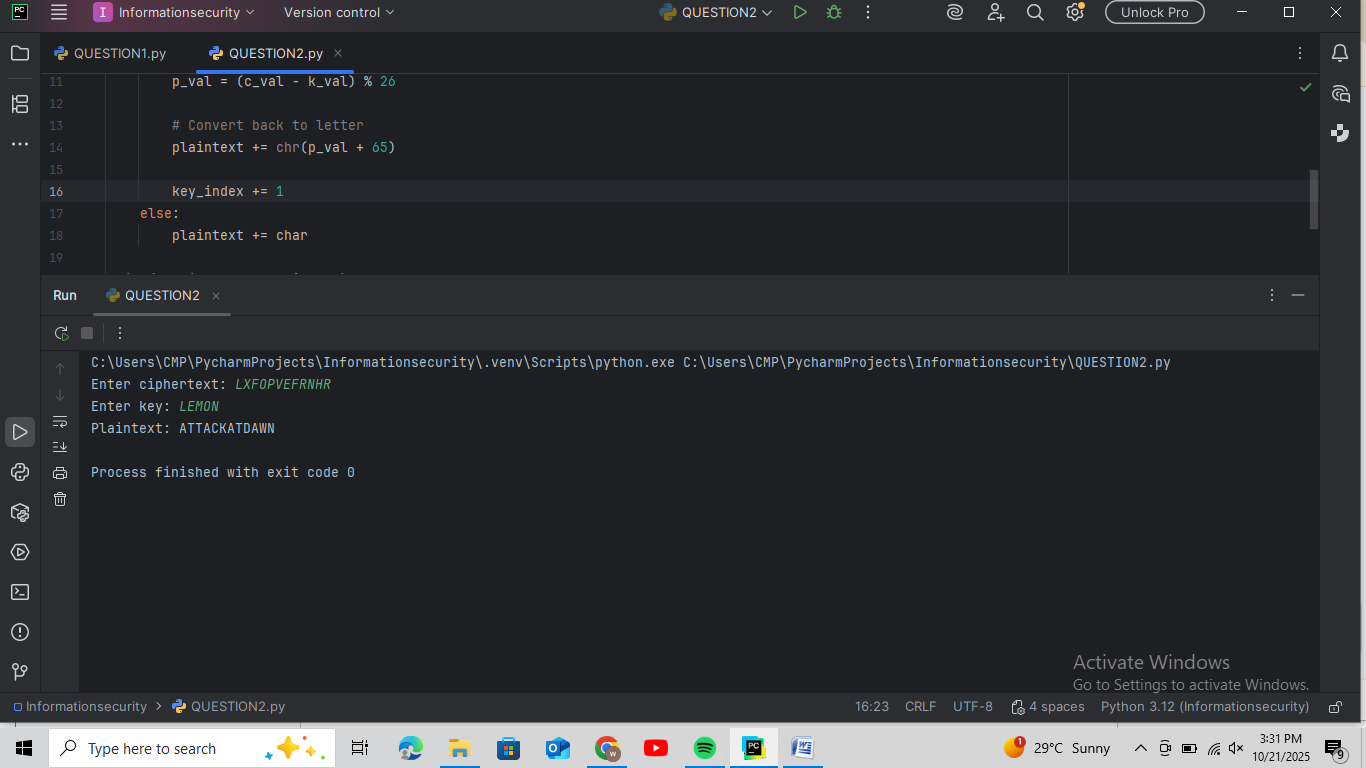
key\_index += 1

else:

plaintext += char

print("Plaintext:", plaintext)

OUTPUT:



QUESTION 3:

DEBUGGING TASK (CIESER CIPHER CODE)

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.

l 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.

def caesar\_encrypt(text, shift):

result = ""

for char in text:

if char.isalpha():

if char.isupper():

result += chr((ord(char) - 65 + shift) % 26 + 65)

else:

result += chr((ord(char) - 97 + shift) % 26 + 97)

else:

result += char

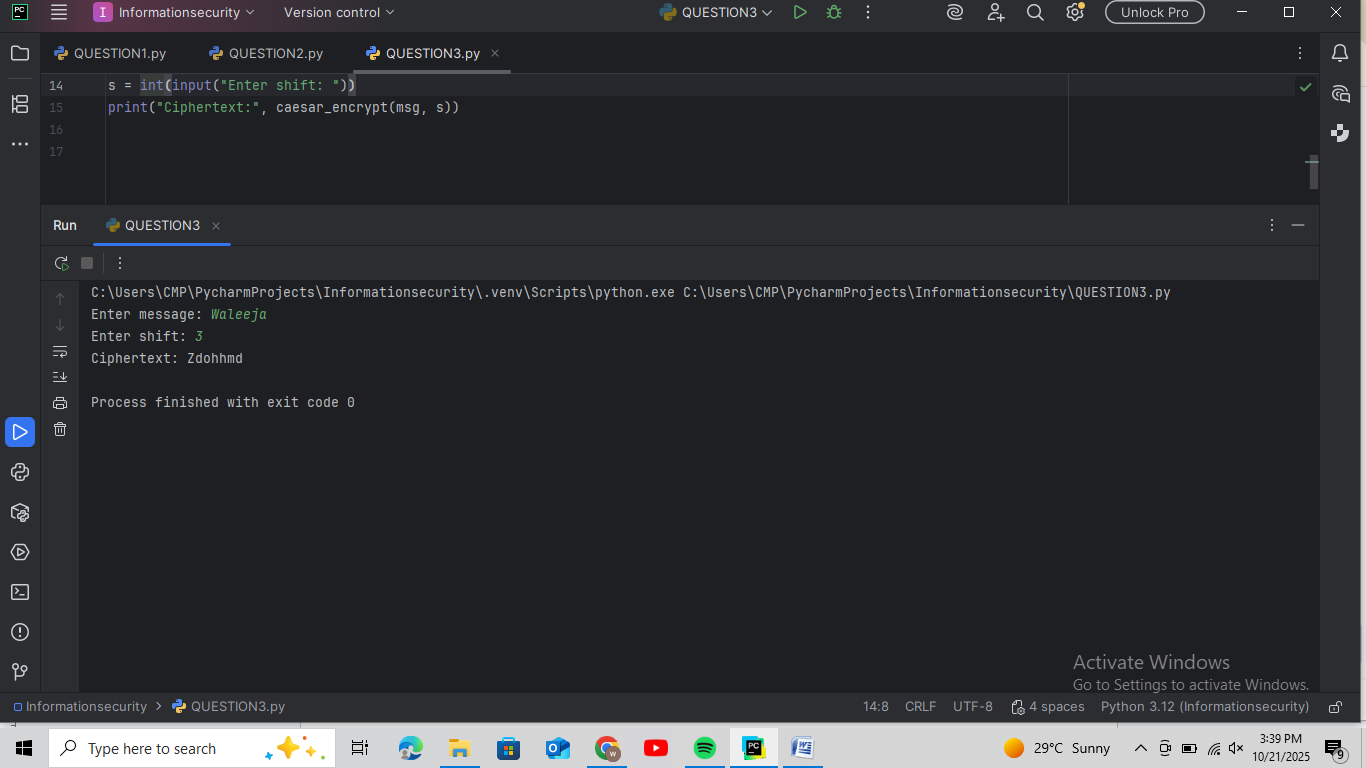
return result

msg = input("Enter message: ")

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

print("Ciphertext:", caesar\_encrypt(msg, s))

OUTPUT:



Question no4:

1. Write one similarity between DES and AES:

Both AES and DES use the same key for encryption and decryption therefore they are called symmetric key algorithms.

1. What does CBC mode stand for in block ciphers

CBC means cipher block chaining In this method,each new block of plaintext is XORed with the previous ciphertext block before encryption.

c) Why is AES faster than DES?

It is faster than DES because it works with bigger blocks of data that is 128 bits and use simpler steps than DES