

LAB MID

SUBMITTED BY:



SUBMITTED TO: MA’AM AMBREEN GUL

DATE: 21ST OCTOBER, 2025

COURSE: Information Security

**Q2**. **Caesar Cipher (Decryption)**

Write a Python program to decrypt a message that was encrypted using the Caesar Cipher.

ciphertext = input("Enter ciphertext: ")

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

plaintext = ""

for char in ciphertext:

    if char.isalpha():

        if char.isupper():

            plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

        else:

            plaintext += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))

    else:

        plaintext += char

print("Plaintext:", plaintext)

A screenshot of a computer

AI-generated content may be incorrect.

Q3. **Vigenère Cipher (Decryption Only)**

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

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

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

plaintext = ""

key\_index = 0

for char in ciphertext:

    if char.isalpha():

        shift = ord(key[key\_index % len(key)]) - ord('A')

        plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

        key\_index += 1

    else:

        plaintext += char

print("Plaintext:", plaintext)

**A screenshot of a computer

AI-generated content may be incorrect.**

Q4. **Debugging Task (Caesar 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.

def caesar\_encrypt(text, shift):

    result = ""

    for char in text:

        if char.isalpha():

            if char.isupper():

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

            else:

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

        else:

            result += char

    return result

msg = input("Enter message: ")

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

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

**A screenshot of a computer

AI-generated content may be incorrect.**

**Q4. Conceptual: DES and AES**

1. Write one similarity between DES and AES.

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

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

Cipher Block Chaining mode - where each block is XORed with the previous ciphertext block before encryption.

1. Why is AES faster than DES?

AES uses simpler mathematical operations and can be efficiently implemented in both software and hardware.