COMSATS UNIVERSITY ISLAMABAD ATTOCK CAMPUS

ASSIGNMENT # 01

NAME	**IQRA GUL**
REG NO	**FA24-BSE-059**
COURSE	**INFORMATION SECURITY LAB**

Submitted TO: MAM AMREEN GUL

Submission Date: 28-02-2026

Code Explanation

The Caesar Cipher program consists of two functions: `caesar_encrypt(text, shift)` and `caesar_decrypt(ciphertext, shift)`. The encryption function takes a message and a shift value, then loops through each character of the text. If the character is an uppercase letter, it converts it to its ASCII value using `ord()`, shifts it forward within the range of 0–25 using `(ord(char) - ord('A') + shift) % 26`, and converts it back to a letter using `chr()`. If the character is lowercase, the same logic is applied using `'a'` instead of `'A'` to preserve case sensitivity. Any spaces, numbers, or special characters remain unchanged. The decryption function works in the same way but subtracts the shift value instead of adding it, which restores the original message. The modulo operator `% 26` ensures the letters wrap around the alphabet correctly, making the algorithm simple, efficient, and suitable for understanding basic encryption concepts.

➢ Line-by-Line Explanation

You can copy this explanation into your PDF file.

1. def caesar_encrypt(text, shift):

Defines an encryption function that takes message and shift value.

2. result = ""

Creates an empty string to store encrypted characters.

3. for char in text:

Loops through each character in the message.

4. char.isupper()

Checks if character is uppercase.

5. ord(char)

Converts letter to ASCII value.

6. (ord(char) - ord('A') + shift) % 26

- Converts letter to 0–25 range
- Adds shift
- % 26 keeps result within alphabet range

7. chr(...)

Converts ASCII value back to letter.

8. char.islower()

Handles lowercase letters separately.

9. else: result += char

Keeps spaces and special characters unchanged.

10. Decryption Function

Same logic but subtracts shift instead of adding.

➢ Security Analysis

❖ **Strengths:**

- Simple to implement
- Easy to understand
- Good for learning basic encryption concepts

❖ **Weaknesses:**

- Only 25 possible keys (Very small key space)
- Easily breakable using brute force
- Vulnerable to frequency analysis attack
- Not secure for real-world communication

➢ Conclusion:

Caesar Cipher is a classical substitution cipher and is not secure for modern data security systems. It is mainly used for educational purposes

➢ Code:

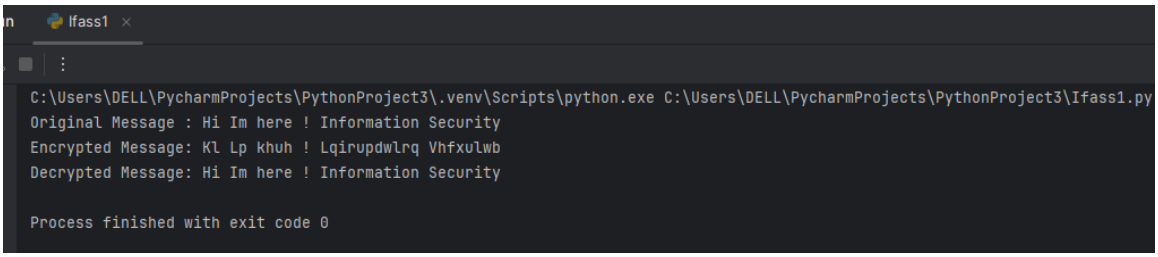
ab.py lfass1.py

```python
# Caesar Cipher Program
# Course: Information Security
# This program encrypts and decrypts a message using Caesar Cipher

# Function for Encryption
def caesar_encrypt(text, shift):  1 usage
    result = ""

    for char in text:
        # Check if character is uppercase letter
        if char.isupper():
            # Convert to ASCII, shift, and convert back
            result += chr((ord(char) - ord('A') + shift) % 26 + ord('A'))

        # Check if character is lowercase letter
        elif char.islower():
            result += chr((ord(char) - ord('a') + shift) % 26 + ord('a'))

        # Keep spaces and special characters unchanged
        else:
            result += char

    return result
```

```python
# Function for Decryption
def caesar_decrypt(ciphertext, shift):  1 usage
    result = ""

    for char in ciphertext:
        if char.isupper():
            result += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

        elif char.islower():
            result += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))

        else:
            result += char

    return result


# Example Usage
if __name__ == "__main__":
    message = "Hi Im here ! Information Security"
    shift_value = 3
```

```python
    encrypted = caesar_encrypt(message, shift_value)
    decrypted = caesar_decrypt(encrypted, shift_value)

    print("Original Message :", message)
    print("Encrypted Message:", encrypted)
    print("Decrypted Message:", decrypted)
```

➢ Output:


Ifass1
C:\Users\DELL\PycharmProjects\PythonProject3\.venv\Scripts\python.exe C:\Users\DELL\PycharmProjects\PythonProject3\Ifass1.py
Original Message : Hi Im here ! Information Security
Encrypted Message: Kl Lp khuh ! Lqirupdwlrq Vhfxulwb
Decrypted Message: Hi Im here ! Information Security
Process finished with exit code 0