**INFORMATION SECURITY LAB**

**BCA-VI SEMESTER**

**LAB SHEET 1**

**Name: Tanmay Dangat**

**PRN NO: 20220801070**

**Objective**

To implement the **Caesar Cipher** algorithm in Python for **encryption and decryption** of a given plaintext using a shift key.

**Caesar Cipher**

The Caesar Cipher is one of the simplest and oldest encryption techniques, attributed to Julius Caesar. It is a **substitution cipher** that replaces each letter in the plaintext with another letter at a fixed distance (known as the "shift") along the alphabet.

**Key Concept**

1. **Shift-Value(Key):**A number between 1 and 25 that determines how many positions each letter is shifted in the alphabet.
2. **Encryption Process:**
   * For each letter in the plaintext:
     + If the letter is uppercase or lowercase, shift it by the specified key value within its alphabet group (A-Z or a-z).
     + Wrap around the alphabet if the shift goes beyond 'Z' or 'z'.
   * Non-alphabetic characters, such as spaces, numbers, or punctuation, remain unchanged.
3. **Decryption Process:**

* Reverse the encryption by shifting each letter back by the same key value.
* **Alphabetic-wrapping:**When the shift moves beyond the end of the alphabet, it wraps around to the beginning.  
  For example, shifting "Z" by 1 results in "A."

**Tasks**

1. Run the Caesar Cipher Python program in your IDE.

2. Test the encryption & decryption with different shift values.

3. Paste your Python code & output below with the date & time of execution

**Python Code:**

import datetime

def caesar\_cipher(text, shift, encrypt=True):

    result = ""

    if not encrypt:

        shift = -shift

    for char in text:

        if char.isalpha():

            shift\_base = ord('A') if char.isupper() else ord('a')

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

        else:

            result += char

    return result

# User input

plaintext = input("Enter text to encrypt or decrypt: ")

shift\_value = int(input("Enter shift value (1-25): "))

operation = input("Enter e for encrypt and d for decrypt: ").lower()

if (operation == 'e'):

    encrypt = True

    result = caesar\_cipher(plaintext, shift\_value, encrypt)

    print("Encrypted Text:", result)

else:

    encrypt = False

    result = caesar\_cipher(plaintext, shift\_value, encrypt)

    print("Decrypted Text: ",result)

print("Execution Date & Time:", datetime.datetime.now().strftime("%Y-%m-%d %H:%M:%S"))

**OUTPUT:**

Enter text to encrypt or decrypt: Hello world lab

Enter shift value (1-25): 2

Enter e for encrypt and d for decrypt: e

Encrypted Text: Jgnnq yqtnf ncd

Execution Date & Time: 2025-02-12 22:53:44

Enter text to encrypt or decrypt: First lab

Enter shift value (1-25): 3

Enter e for encrypt and d for decrypt: d

Decrypted Text: Cfopq ixy

Execution Date & Time: 2025-02-12 22:55:06