**SCHOOL OF COMPUTER SCIENCE ENGINEERING AND APPLICATION**

**BCA TY SEM VI**

**SUBJECT NAME: INFORMATION SECURITY**

**LAB- ASSIGNMENT NO 1**

**AIM: IMPLEMENT CAESAR CIPHER ALGORITHM. (ENCRYPTION AND DECRYPTION)**

**CAESAR CIPHER:**

The Caesar cipher is among the simplest and most traditional encryption techniques. With this type of substitution cipher, each letter in the plaintext is moved by a preset amount up or down the alphabet.  
To give an example, think about a shift of 3:  
- A becomes D; - B becomes E; - C becomes F

-X becomes A, Y becomes B, and Z becomes C.

During the encryption process, each letter in the plaintext is replaced with a letter that is one number of positions lower in the alphabet.  
Simply put, decryption is the encryption process reversed, with the characters shifted in the opposite direction.

**ALGORITHM:**

Encryption Steps:

Suppose we want to encrypt the message "HELLO" with a shift of 3.

**Step-1: Input**:

Plaintext: "HELLO"

Shift: 3

**Step-2:Encryption:**

Iterate through each character in the plaintext:

H -> K (shifted by 3)

E -> H

L -> OL -> O

O -> R

So, the encrypted text is "KHOOR".

**Decryption Steps:**

Now, let's decrypt the ciphertext "KHOOR" back to the original plaintext using the same shift value of 3.

**Step-1: Input**:

Ciphertext: "KHOOR"

Shift: 3

**Step-2: Decryption:**

Iterate through each character in the ciphertext:

K -> H (shifted back by 3)

H -> E

O -> L

O -> L

R -> O

So, the decrypted text is "HELLO".

**PSUEDO CODE IN PYTHON FOR CAESAR CIPHER ENCRYPTION WITH OUTPUT:**

def caesar\_cipher\_encrypt(plaintext, shift):

    encrypted\_text = ""

    for char in plaintext:

        if char.isalpha():

            is\_upper = char.isupper()

            shifted\_char = chr((ord(char) - ord('A' if is\_upper else 'a') + shift) % 26 + ord('A' if is\_upper else 'a'))

            encrypted\_text += shifted\_char

        else:

            encrypted\_text += char

    return encrypted\_text

plaintext = input("Enter text want to encrypt :")

shift = 3

encrypted\_text = caesar\_cipher\_encrypt(plaintext, shift)

print("Encrypted text:", encrypted\_text)

PS C:\Users\T480> & C:/Users/T480/AppData/Local/Programs/Python/Python312/python.exe "c:/Users/T480/Desktop/sem\_6/IS/assignments/lab assignments/caeser-cipher-encryption.py"

Enter text want to encrypt :HELLO

Encrypted text: KHOOR

**PSUEDO CODE IN PYTHON FOR CAESAR CIPHER DECRYPTION WITH OUTPUT:**

def caesar\_cipher\_decrypt(ciphertext, shift):

    decrypted\_text = ""

    for char in ciphertext:

        if char.isalpha():

            is\_upper = char.isupper()

            shifted\_char = chr((ord(char) - ord('A' if is\_upper else 'a') - shift) % 26 + ord('A' if is\_upper else 'a'))

            decrypted\_text += shifted\_char

        else:

            decrypted\_text += char

    return decrypted\_text

ciphertext = input("Enter text want to decrypt :")

shift = 3

decrypted\_text = caesar\_cipher\_decrypt(ciphertext, shift)

print("Decrypted text:", decrypted\_text)

PS C:\Users\T480> & C:/Users/T480/AppData/Local/Programs/Python/Python312/python.exe "c:/Users/T480/Desktop/sem\_6/IS/assignments/lab assignments/caeser-cipher-decryption.py"

Enter text want to decrypt :KHOOR

Decrypted text: HELLO