**Name : Akash Babu Misal**

**PRN: 21520005**

**Class:** Final Year (Computer Science and Engineering)

**Course Name: Cryptography and Network Security**  **Lab**

**Assignment No – 1**

Aim - Implementation of Caesar Cypher in:

Part-A: Encrypt the given input.

Part-B: Decrypt the given input.

***Theory –***

**Caesar Cipher Overview:**

The Caesar Cipher is one of the simplest and most well-known encryption techniques. It is a substitution cipher that shifts each letter in the plaintext by a fixed number of positions down or up the alphabet. This fixed number is known as the "key" or "shift value."

**Part-A: Encryption**

In this part of the experiment, we will implement the Caesar Cipher encryption process. The encryption process involves the following steps:

**Input:** The user provides a plaintext message and a key (shift value), which determines how much each letter in the message will be shifted.

Encryption: For each letter in the plaintext message, we perform the following steps:

Identify the position of the letter in the alphabet.

Add the key (shift value) to the position to obtain a new position.

Wrap around the alphabet if the new position goes beyond 'Z' (for lowercase letters) or 'A' (for uppercase letters).

Replace the original letter with the letter at the new position.

**Output**: The encrypted message is produced, which is a ciphertext with the original message's characters shifted according to the key.

**Part-B: Decryption**

In this part of the experiment, we will implement the Caesar Cipher decryption process. The decryption process is essentially the reverse of encryption and involves the following steps:

**Input**: The user provides the ciphertext and the same key used for encryption.

Decryption: For each letter in the ciphertext, we perform the following steps:

Identify the position of the letter in the alphabet.

Subtract the key (shift value) from the position to obtain the original position.

Wrap around the alphabet if the original position is less than 'A' (for uppercase letters) or greater than 'Z' (for lowercase letters).

Replace the letter in the ciphertext with the letter at the original position.

**Output**: The decrypted message is produced, which should be identical to the original plaintext message if the correct key is used.

**Code**:

#include <bits/stdc++.h>

using namespace std;

string encrypt(string plain, int k)

{

    stringstream cipher;

    for (int i = 0; i < plain.length(); i++)

    {

        if (plain[i] != ' ')

        {

            cipher << char((plain[i] - 'a' + k) % 26 + 'a');

        }

        else

        {

            cipher << ' ';

        }

    }

    return cipher.str();

}

string decrypt(string cipher, int k)

{

    stringstream plain;

    for (int i = 0; i < cipher.length(); i++)

    {

        if (cipher[i] != ' ')

        {

            plain << char((cipher[i] - 'a' - k + 26) % 26 + 'a');

        }

    }

    return plain.str();

}

int main()

{

    int choice;

    cout << "Enter choice: \n1. Decrypt \n2. Encrypt\n";

    cin >> choice;

    cin.get();

    string plain, cipher;

    int k;

    if (choice == 1)

    {

        cout << "Enter Encrypted text: ";

        getline(cin, cipher);

        cout << "Enter K: ";

        cin >> k;

        string plain = decrypt(cipher, k);

        cout << "Decrypted text is: " << plain << endl;

    }

    else if (choice == 2)

    {

        cout << "Enter Plain text: ";

        getline(cin, plain);

        cout << "Enter K: ";

        cin >> k;

        string cipher = encrypt(plain, k);

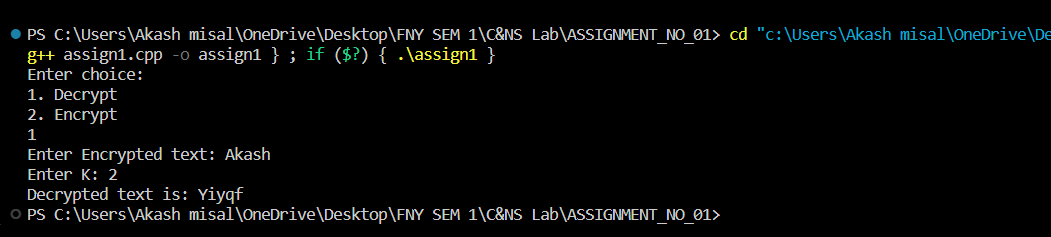
        cout << "\nEncrypted text is: " << cipher << endl;

    }

    return 0;

}

**Output:**

****

**Conclusion**:

The Caesar Cipher is a straightforward encryption technique that illustrates the concept of substitution ciphers. This experiment allows us to understand both the encryption and decryption processes of the Caesar Cipher and how the same key is used for both operations. It is essential to choose a suitable key value and ensure that both encryption and decryption are performed correctly to maintain the confidentiality of the message.