**Cryptography and Network Security Lab**

**Assignment No. 1**

**PRN : 2020BTECS00092**

**Name : Vishal Shrirang Madle**

**Batch : B8**

**Title:** Caesar Cipher Encryption

**Aim:** To implement Caesar Cipher Encryption using Console and file input

**Theory:**

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift

cipher, Caesar's code or Caesar shift, is one of the simplest and most widely

known encryption-decryption techniques. It is a type of substitution cipher in

which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.

**Procedure:**

En(x)=(x+n)% 26

(Encryption Phase where x is input character and n is given key)

 Traverse the given text one character at a time.

 For each character, transform the given character as per the rule and encrypt plain text using key.

 Return the new string generated.

**Code:Console Input Code:**

#include <iostream>

#include <fstream>

#include <string>

using namespace std;

string CaesarCipherEncryption(string text, int key)

{

    string ciphertext = "";

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

    {

        ciphertext += char(int(text[i] + key - 65) % 26 + 65);

    }

    return ciphertext;

}

int main()

{

    int Choice, key;

    string plain\_text;

    cout << "-----Caesar Cipher Encryption-----\n";

    cout << "Enter Choice:\n1) Console\n2) File\n";

    cin >> Choice;

    cout << "Enter key: ";

    cin >> key;

    switch (Choice)

    {

    case 1:

        cout << "Enter plain text: ";

        cin >> plain\_text;

        break;

    case 2:

        {

            ifstream inputFile("input.txt");

            if (!inputFile)

            {

                cerr << "Error opening input file." << endl;

                return 1;

            }

            getline(inputFile, plain\_text);

            inputFile.close();

        }

        break;

    default:

        cerr << "Invalid choice." << endl;

        return 1;

    }

    string ciphertext = CaesarCipherEncryption(plain\_text, key);

    // Open the "output.txt" file for writing

    ofstream outputFile("output.txt");

    if (!outputFile)

    {

        cerr << "Error opening output file." << endl;

        return 1;

    }

    // Write the cipher text to the output file

    outputFile << "Cipher Text: " << ciphertext << endl;

    // Close the output file

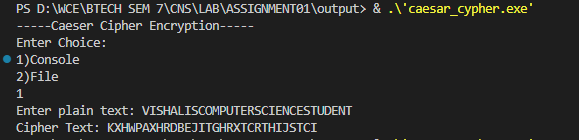
    outputFile.close();

    cout << "Cipher Text: " << ciphertext << endl;

    return 0;

}

**Output:**



**Conclusion:**

Caesar Cipher is simple substitution technique. It falls in category of

monoalphabetic cipher where each character is substituted by addition of that character with given key. The key can be deciphered easily, thus makes it less secure.