Cryptography and Network Security Lab

PRN: 2019BTECS00090

Name: Udaykumar Gadikar

Batch: B8

Assignment No. 1

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:

$$E_n(x)=(x+n)\%\ 26$$

(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.

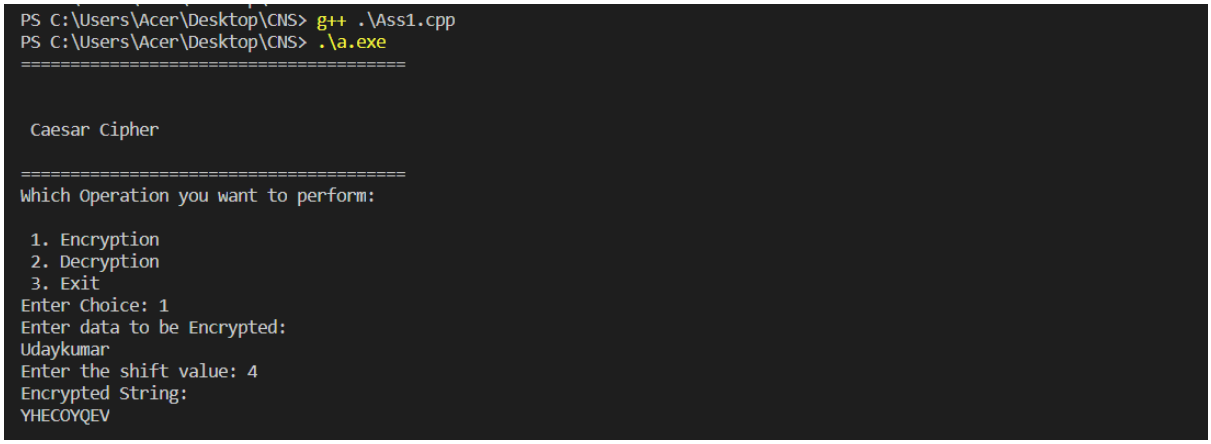
Code:

Console Input Code:

```
#include <bits/stdc++.h>
#include <string.h>
using namespace std;

string encrypt(string text, int s)
{
    string result = "";
    for (int i = 0; i < text.length(); i++)
    {
        if (text[i] == ' ' || text[i] == '\n')
            continue;
        else if (text[i] >= 65 && text[i] <= 90)
            result += char(int(text[i] + s - 65) % 26 + 65);
        else
            result += toupper(char(int(text[i] + s - 97) % 26 + 97));
    }
    return result;
}

string decrypt(string cipher, int s)
{
    string result = "";
    for (int i = 0; i < cipher.size(); i++)
    {
        if (cipher[i] == ' ' || cipher[i] == '\n')
            continue;
        else if (cipher[i] >= 65 && cipher[i] <= 90)
            result += char((int(cipher[i] - s - 65) + 26) % 26 + 65);
        else
            result += char((int(cipher[i] - s - 97) + 26) % 26 + 97);
    }
    return result;
}

int main()
{
    int choice;
    int datachoice;
    string sample;
    int shift;
    cout << "=====================================\n\n\n Caesar Cipher \n\n=
====================================";

    while (1)
    {
        cout << "\nWhich Operation you want to perform:\n ";
```

```
        // cout << "\n=======================================";
        cout << "\n 1. Encryption \n 2. Decryption\n 3. Exit\nEnter Choice: ";
        cin >> choice;
        if (choice > 2 || choice <= 0)
            break;
        switch (choice)
        {
        case 1:

            cout << "Enter data to be Encrypted:\n";
            cin.ignore();
            getline(cin, sample);
            cout << "Enter the shift value: ";
            cin >> shift;
            cout << "Encrypted String:\n";
            cout << encrypt(sample, shift) << endl;
            ;

            break;
        case 2:
            cout << "Enter data to be Decrypted:\n";
            cin.ignore();
            getline(cin, sample);
            cout << "Enter the shift value: ";
            cin >> shift;
            cout << "Decrypted String:\n";
            cout << decrypt(sample, shift) << endl;
            ;
            break;
        }
    }
    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.