Cryptography & Network Security

PRN - 2019BTECS00026

Name - Niraja Vasudev Kulkarni

Batch - B1

Assignment - 1

- **Title - Caeser Cipher**
- **Objective -**

Decrypting the cipher text encrypted using Caesar Cipher

- **Theory** -

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Procedure -

1. Take the plain text from user as an input

2. Apply the given shift & find the cipher text - For example with a shift of 3, A would be replaced by D, B would become E, and so on.

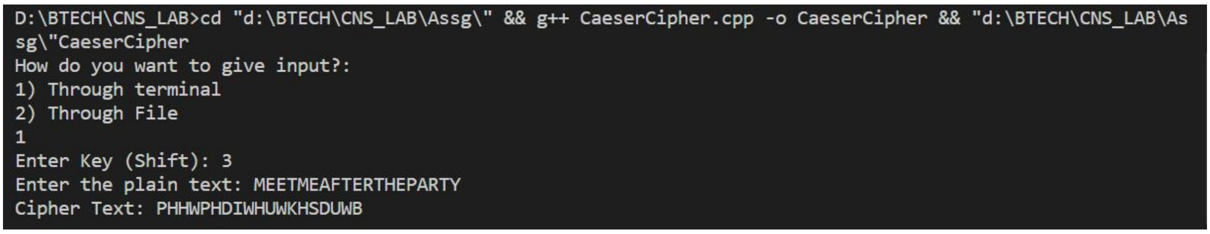
- **Code –**

```
#include <bits/stdc++.h>

using namespace std;


string encrypt(string plainText, int key)

{

    string ans = "";

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

    {

        ans += char(int(plainText[i] + key - 'A') % 26 + 'A');
    }
    return ans;
}
```

```
int main()
{
    int option;
    cout << "How do you want to give input?:\n1) Through terminal\n2) Through File\n";
    cin >> option;
    string plainText;
    int key;
    cout << "Enter Key (Shift): ";
    cin >> key;
    switch (option)
    {
    case 1:
        cout << "Enter the plain text: ";
        break;
    case 2:
        freopen("input.txt", "r", stdin);
        freopen("output.txt", "w", stdout);
        break;
    default:
        break;
    }
    cin >> plainText;
    cout << "Cipher Text: "
         << encrypt(plainText, key) << "\n";
    return 0;
}
```

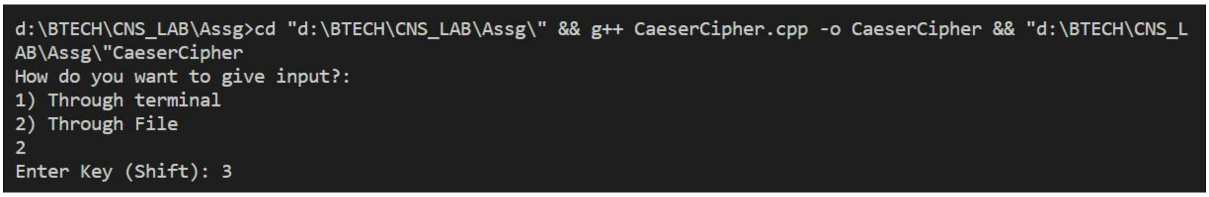
- **Outputs –**

Sample output 1 –



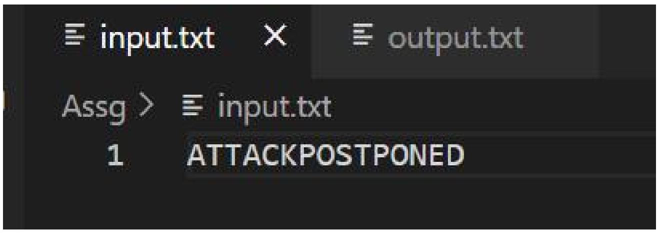
```
D:\BTECH\CNS_LAB>cd "d:\BTECH\CNS_LAB\Assg\" && g++ CaeserCipher.cpp -o CaeserCipher && "d:\BTECH\CNS_LAB\As
sg\"CaeserCipher
How do you want to give input?:
1) Through terminal
2) Through File
1
Enter Key (Shift): 3
Enter the plain text: MEETMEAFTERTHEPARTY
Cipher Text: PHHWPHDIWHUWKHSDUWB
```

Sample output 2 -



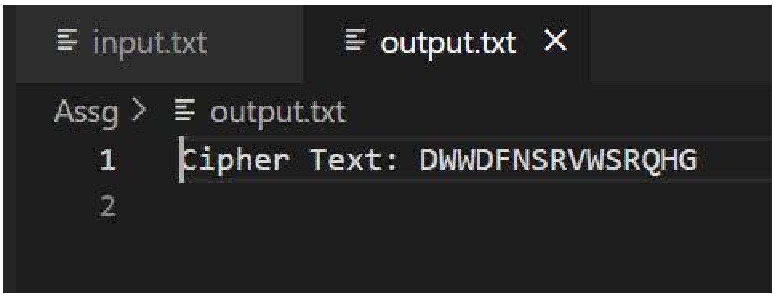
```
d:\BTECH\CNS_LAB\Assg>cd "d:\BTECH\CNS_LAB\Assg\" && g++ CaeserCipher.cpp -o CaeserCipher && "d:\BTECH\CNS_L
AB\Assg\"CaeserCipher
How do you want to give input?:
1) Through terminal
2) Through File
2
Enter Key (Shift): 3
```

Input file -



```
ATTACKPOSTPONED
```

Output file -



```
Cipher Text: DWWDFNSRVWSRQHG
```

- **Conclusion –**

Caesar Cipher is simple substitution (mono alphabetic) technique. The key can be deciphered easily. So, it is a classical way of cryptography which is not secure in modern era.