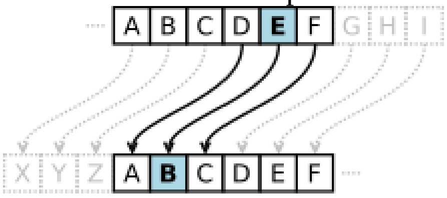
Experiment No: 2

Aim: Write a program for a Julius Caesar cipher.

Introduction: In cryptography, a Caesar cipher is one of the simplest and most widely known encryption technique. In this technique, each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a right shift of 7, A would be replaced by H, B would become I, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

This is how Caesar Cipher can be represented and understood.:



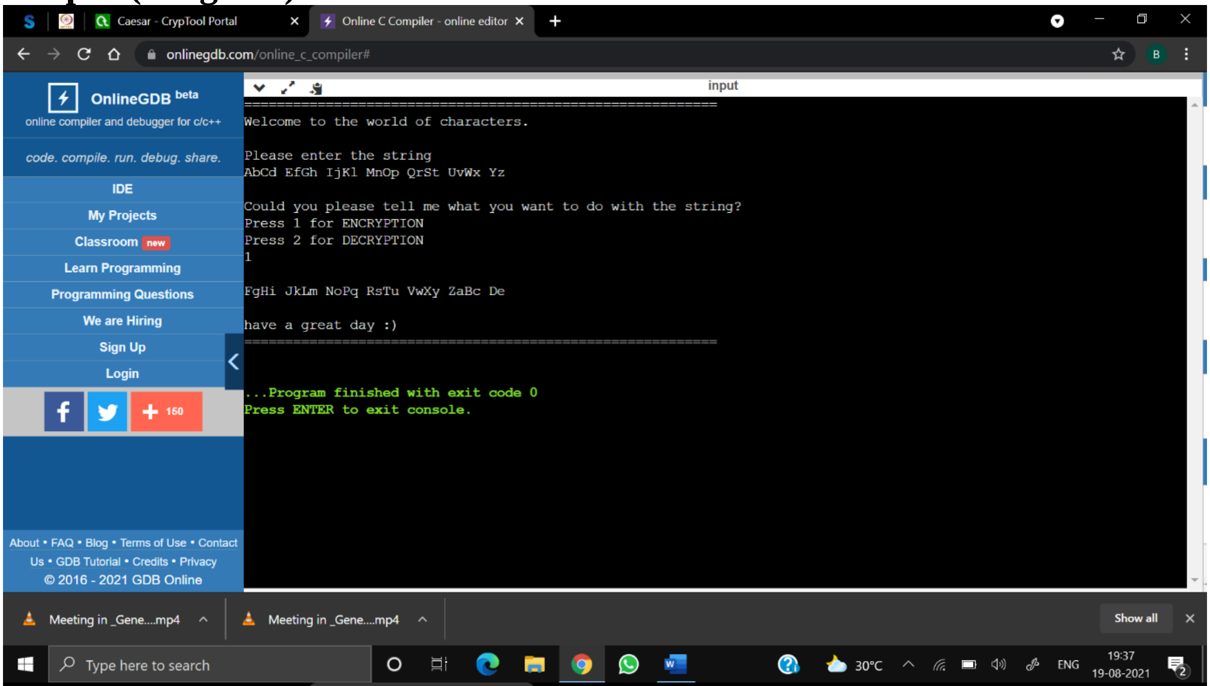
Program (Source Code):

```
#include<iostream>
#include<bits/stdc++.h>
using namespace std;
#define mm 250

string encry(string s)
{
   string op="";
   for(int i=0; i<s.size(); i++)
   {
      if(s[i]==' ')
         {op+= s[i];}

      else if((s[i]>='a' && s[i]<'v')||(s[i]>='A' && s[i]<'V'))
      {
         op+= (s[i]+5);
      }
      else if(s[i]>='v'|| s[i]>='V' )
      {
         op+= (s[i]-26+5);
      }
   }
   return op;
}

string decry(string s)
{
   string op="";
   for(int i=0; i<s.size(); i++)
```

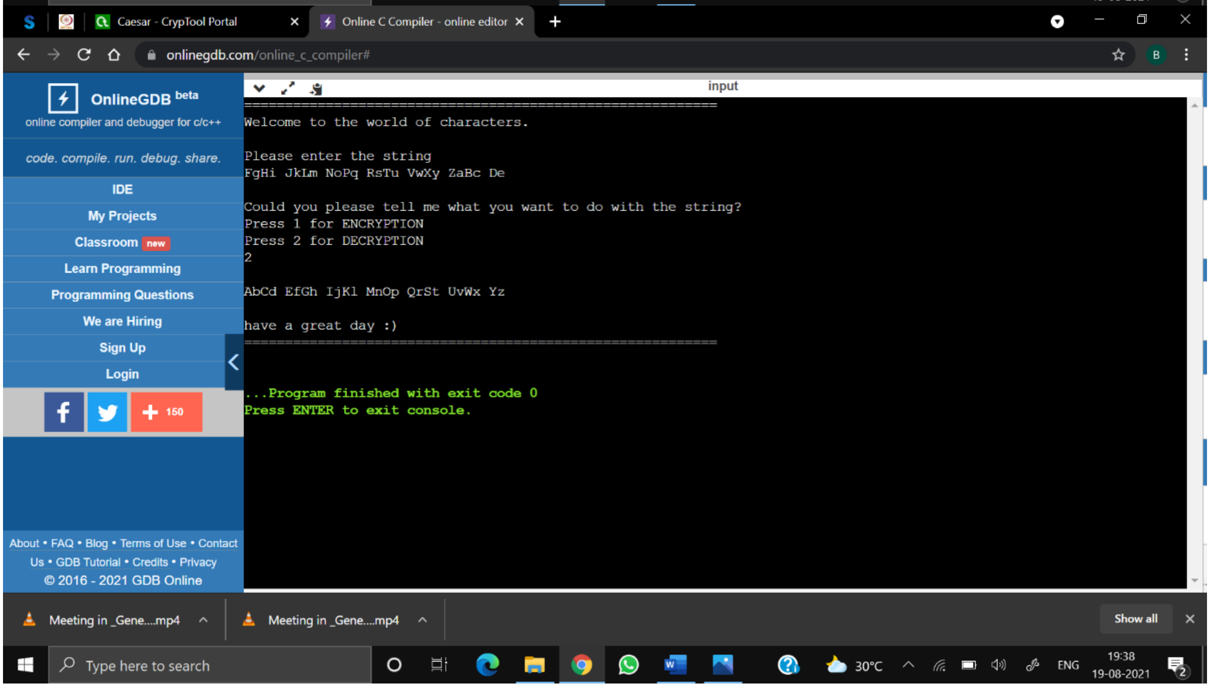
```
    {
        if(s[i]==' ')
            {op+= s[i];}

        else if((s[i]>'e' && s[i]<='z')||(s[i]>'E' && s[i]<='Z'))
        {
            op+= s[i]-5;
        }
        else if(s[i]<='e' || s[i]<='E')
        {
            op+= (s[i]+26-5);
        }
    }
    return op;
}

void doWork()
{

cout<<"=======================================================
==="<<endl;
    cout<<"Welcome to the world of characters."<<endl<<endl;
    string s;
    int x;
    cout<<"Please enter the string"<<endl;
    getline(cin,s);

    cout<<endl<<"Could you please tell me what you want to do with the
string?"<<endl;
    cout<<"Press 1 for ENCRYPTION"<<endl;
    cout<<"Press 2 for DECRYPTION"<<endl;
    // cout<<"Press 3 for EXIT"<<endl;
    cin>>x;
    switch(x)
    {
        case 1:
        {cout<<endl<<encry(s)<<endl;
        break;}

        case 2:
        {cout<<endl<<decry(s)<<endl;
        break;}

        default:
        cout<<"Please enter valid input next time."<<endl;
        break;
    }
    return;
}
```

```
int main()
{
    doWork();
    cout<<endl<<"have a great day :)"<<endl;

cout<<"=======================================================
==="<<endl;
    return 0;
}
```

Output (Program):

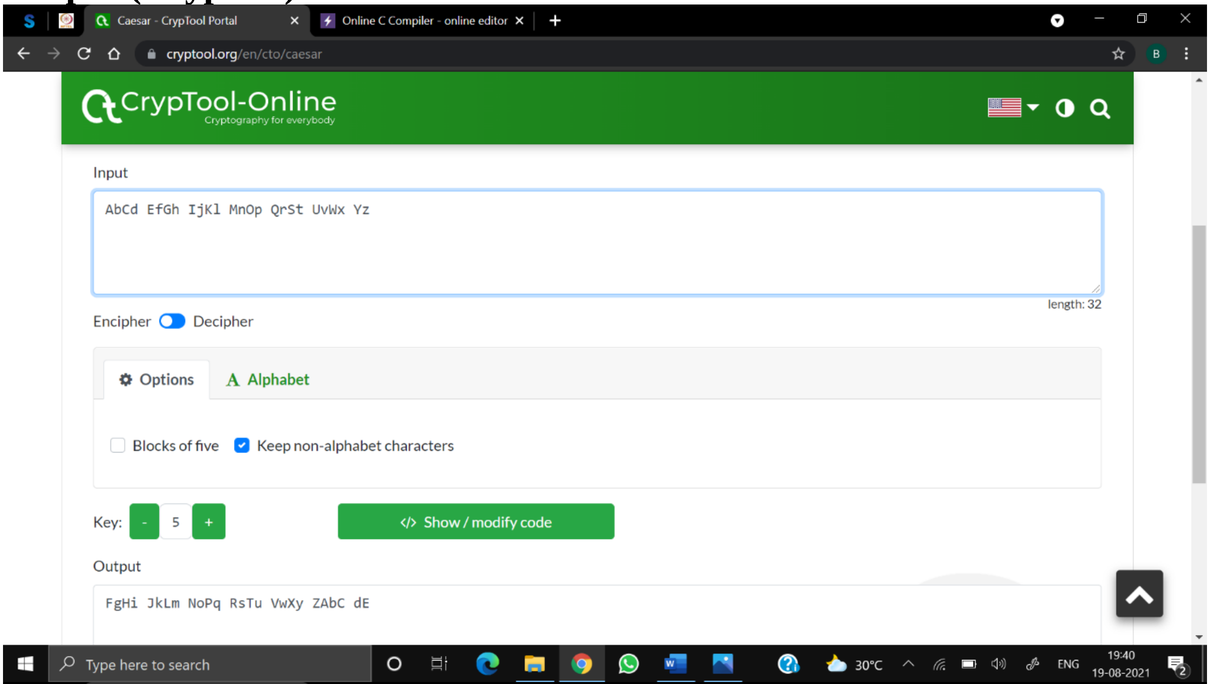


```
==========================================================
Welcome to the world of characters.

Please enter the string
AbCd EfGh IjKl MnOp QrSt UvWx Yz

Could you please tell me what you want to do with the string?
Press 1 for ENCRYPTION
Press 2 for DECRYPTION
1

FgHi JkLm NoPq RsTu VwXy ZaBc De

have a great day :)
==========================================================


...Program finished with exit code 0
Press ENTER to exit console.
```



```
==========================================================
Welcome to the world of characters.

Please enter the string
FgHi JkLm NoPq RsTu VwXy ZaBc De

Could you please tell me what you want to do with the string?
Press 1 for ENCRYPTION
Press 2 for DECRYPTION
2

AbCd EfGh IjKl MnOp QrSt UvWx Yz

have a great day :)
==========================================================


...Program finished with exit code 0
Press ENTER to exit console.
```

Output (Cryptool):



Caesar - CrypTool Portal
Online C Compiler - online editor
cryptool.org/en/cto/caesar
CrypTool-Online
Cryptography for everybody

Input

```
AbCd EfGh IjKl MnOp QrSt UvWx Yz
```

length: 32

Encipher ○ Decipher

Options | Alphabet

□ Blocks of five ☑ Keep non-alphabet characters

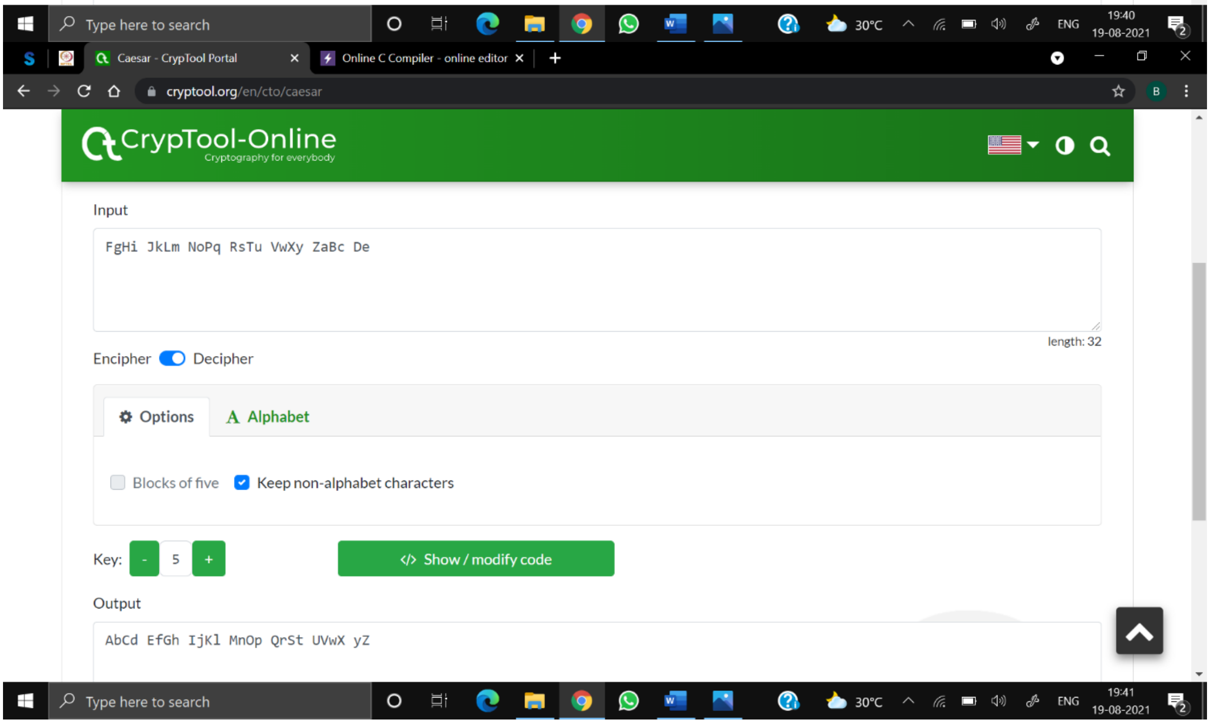
Key: - 5 +

Show / modify code

Output

```
FgHi JkLm NoPq RsTu VwXy ZAbC dE
```

Type here to search
30°C
ENG
19:40
19-08-2021



Caesar - CrypTool Portal
Online C Compiler - online editor
cryptool.org/en/cto/caesar
CrypTool-Online
Cryptography for everybody

Input

```
FgHi JkLm NoPq RsTu VwXy ZaBc De
```

length: 32

Encipher ● Decipher

Options | Alphabet

□ Blocks of five ☑ Keep non-alphabet characters

Key: - 5 +

Show / modify code

Output

```
AbCd EfGh IjKl MnOp QrSt UVwX yZ
```

Type here to search
30°C
ENG
19:41
19-08-2021

Cryptanalysis:

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plain text source, encryption key or the algorithm used to encrypt it. Cryptanalysts also target secure hashing, digital signatures and other cryptographic algorithms. While the objective of the cryptanalysts is to find weaknesses in or otherwise defeat cryptographic algorithms, cryptanalysis research results are used by cryptographers to improve the strengthen or replace flawed algorithms.

Applications:

The Cipher, in the current era, is very easy to break and hence is not in use. But Julius Caesar used it to encrypt military messages which means it proved to be effective in the past.

References:

1. https://www.cryptool.org/en/cto/caesar
2. https://en.wikipedia.org/wiki/Cryptanalysis
3. https://en.wikipedia.org/wiki/Caesar_cipher
4. https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/