

Practical-1

AIM: Implement Caesar cipher encryption-decryption.

1. encryption

Description:

- The Caesar Cipher technique is one of the earliest and simplest method of encryption technique.
- It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.
- For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.
- $En(x) = (x+n) \bmod 26$
(Encryption Phase with shift n)

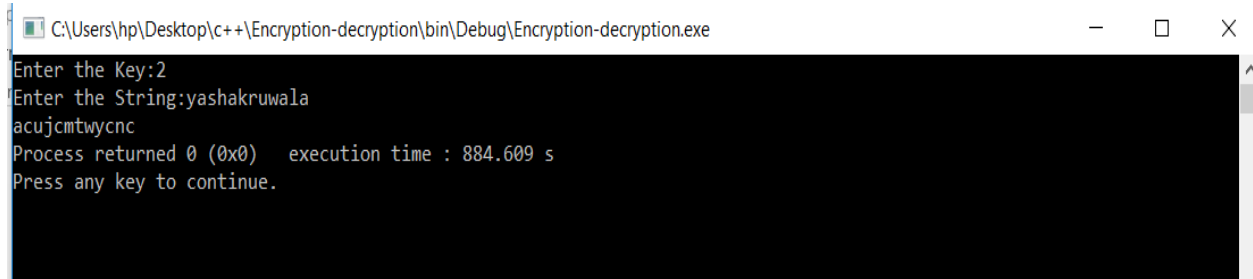
Code:

```
#include<iostream>
#include<string>
using namespace std;
int main()
{
    string a;
    int k;
    cout<<"Enter the Key:";
    cin>>k;
    cout<<"Enter the String:";
```

```
    cin>>a;

    for(int i=0;i<a.length();i++)
    {
        a[i]=a[i]+k;
        if(a[i]>'z')
            a[i]=a[i]-26;
    }
    cout<<a;
    return 0;
}
```

OUTPUT:



The screenshot shows a Windows command prompt window titled "C:\Users\hp\Desktop\c++\Encryption-decryption\bin\Debug\Encryption-decryption.exe". The window contains the following text:

```
Enter the Key:2
Enter the String:yashakruwala
acu jcmtwycnc
Process returned 0 (0x0)   execution time : 884.609 s
Press any key to continue.
```

2. decryption:

Description:

- We can either write another function decrypt similar to encrypt, that'll apply the given shift in the opposite direction to decrypt the original text.
- However we can use the cyclic property of the cipher under modulo , hence we can simply observe the logic is given below.
- $D_n(x) = (x-n) \bmod 26$

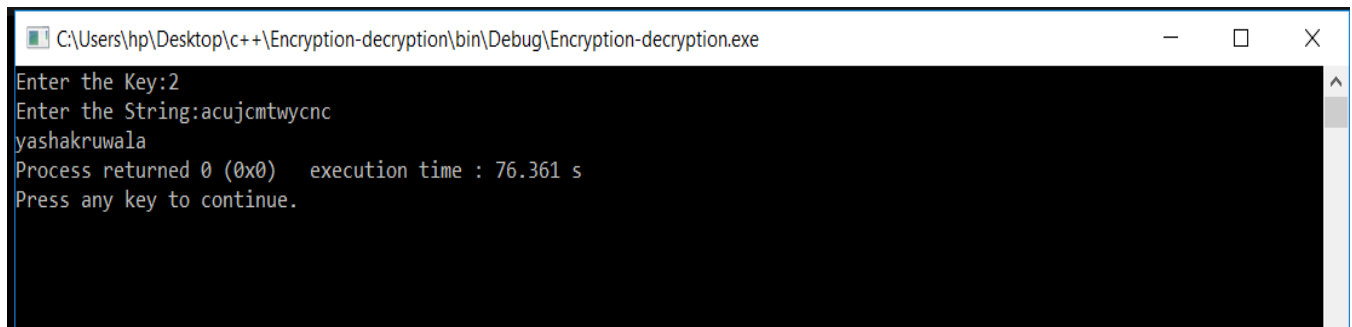
Code:

```
#include<iostream>
#include<string>
using namespace std;
int main()
{
    string a;
    int k;
    cout<<"Enter the Key:";
    cin>>k;
    cout<<"Enter the String:";
    cin>>a;

    for(int i=0;i<a.length();i++)
    {
        a[i]=a[i]-k;
        if(a[i]<'a')
            a[i]=a[i]+26;
    }
    cout<<a;
```

```
    return 0;  
  
}
```

OUTPUT:



The screenshot shows a Windows command prompt window titled "C:\Users\hp\Desktop\c++\Encryption-decryption\bin\Debug\Encryption-decryption.exe". The window has a black background with white text. The text inside the window is as follows:

```
Enter the Key:2  
Enter the String:acujcmtwycnc  
yashakruwala  
Process returned 0 (0x0)   execution time : 76.361 s  
Press any key to continue.
```