Assignment 2

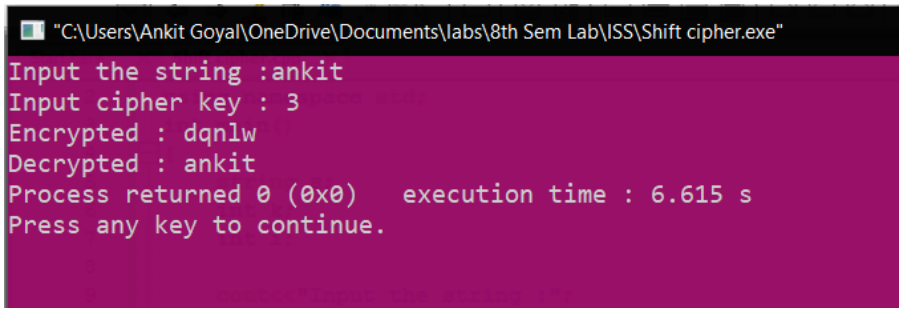
1. Shift cipher

In this cipher, the characters of the string is converted to encrypted form using shift cipher. This is one of the part of mono-alphabetic cipher, where each letter is substituted by another letter which is the encrypted form of the original character. The example of this type of cipher is Caeser cipher. In caeser cipher, a shift of three is used to encrypt the original data. Meanwhile, these type of ciphers are not very good at encrypting the data, and can be decrypted easily.

Code :

```
#include <bits/stdc++.h>
using namespace std;
int main()
{
    string s;
    int k;
    int i;

    cout<<"Input the string :";
    cin>>s;
    cout<<"Input cipher key : ";
    cin>>k;
    int n = s.length();

    /// Encryption ==>
    string encrypted = s;
    for(i=0;i<n;i++)
    {
        if(s[i]>='a' && s[i]<='z')
            encrypted[i] = (s[i]-'a'+k)%26 + 'a';
        else
            encrypted[i] = (s[i]-'A'+k)%26 + 'A';
    }

    cout<<"Encrypted : "<<encrypted<<"\n";


    /// Decryption ==>
    string decrypted = encrypted;
    for(i=0;i<n;i++)
    {
        if(s[i]>='a' && s[i]<='z')
            decrypted[i] = (encrypted[i]-'a'-k+26)%26 + 'a';
        else
            decrypted[i] = (encrypted[i]-'A'-k+26)%26 + 'A';
    }

    cout<<"Decrypted : "<<decrypted;
}
```

Result :



2. Mono-alphabetic cipher

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'D'. And it is different from Poly-alphabetic cipher, as it has fixed character for all occurrence. But in poly-alphabetic, there is different encrypted character for different occurrence of the same character.

Shift cipher is one of the way of mono-alphabetic cipher. However, here using a different approach to cipher the text.

Using a encryption string, and using that for decryption as well.

The Encryption string is : qwertyuioplkjhgfdsazxcvbnm

The Decryption string is : abcdefghijklmnopqrstuvwxyz

Code :

```
#include <bits/stdc++.h>
using namespace std;
int main()
{
    string EncryptionCipher = "qwertyuioplkjhgfdsazxcvbnm";
    string DecryptionCipher = "sxvqcponhmlkzyijadregwbuft";

    string s;
    int i;

    cout<<"Input the string :";
    cin>>s;
    int n = s.length();

    /// Encryption ==>
    string encrypted = s;
    for(i=0;i<n;i++)
    {
```

```
        if(s[i]>='a' && s[i]<='z')
            encrypted[i] = EncryptionCipher[s[i]-'a'];
        else
            encrypted[i] = EncryptionCipher[s[i]-'A']-'a'+'A';
    }

    cout<<"Encrypted : "<<encrypted<<"\n";


    /// Decryption ==>
    string decrypted = encrypted;
    for(i=0;i<n;i++)
    {
        if(s[i]>='a' && s[i]<='z')
            decrypted[i] = DecryptionCipher[encrypted[i]-'a'];
        else
            decrypted[i] = DecryptionCipher[encrypted[i]-'A']-'a'+'A';
    }

    cout<<"Decrypted : "<<decrypted;
}
```

Result :