Cryptography and Network Security

Name: Piyush Mhaske Batch: B3
PRN : 2019BTECS00089

Assignment 1

Objective :

Caesar Cipher Encryption

Theory:

Caesar Cipher is a substitution technique. The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. It consists of a input and Shift.
Input is the string or the sentence which is to be encrypted.
Shift is the number by which letter need to be shifted

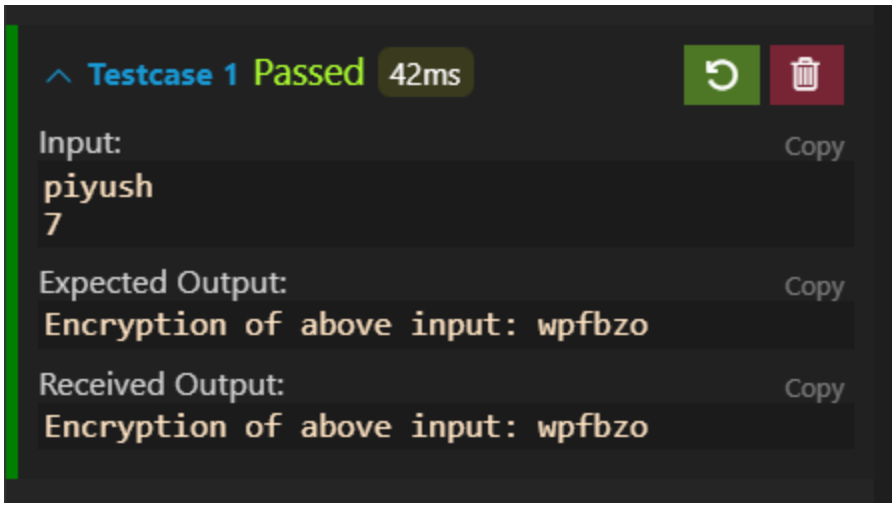
Code Snapshots :

```
// code by PiyushMhaske
#include <bits/stdc++.h>
#include <fstream>
#include <cstdlib>
#define ll long long
#define ul unsigned long long
#define pb emplace_back
#define po pop_back
#define vi vector<ll>
#define vii vector<vector<ll>>
using namespace std;
void file(){
     ios_base::sync_with_stdio(false);
     cin.tie(NULL);}
ll M = 1e9 + 7;
string caeserCipherEnc(string input, int shift){
```

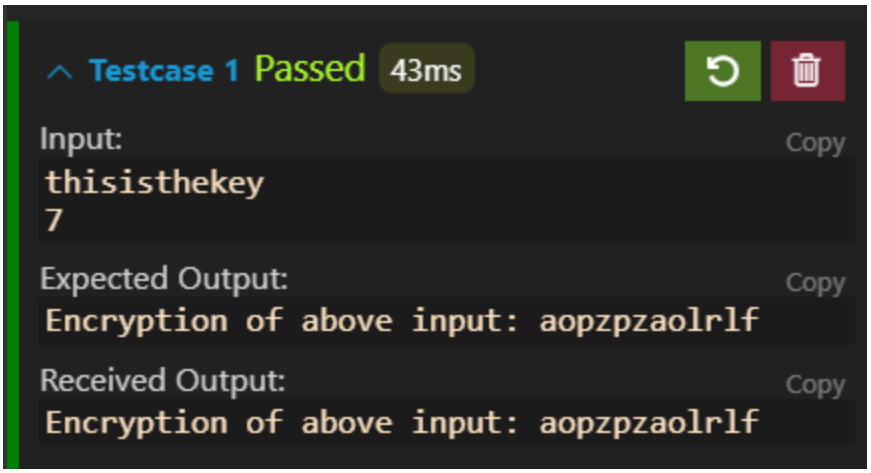
```
    for(int i=0;i<input.size();i++){
        char num = input[i] - 'a';

        input[i] = 'a' + (num + shift)%26;
    }
   return input;
}
int main()
{   file();
    string input;
    cin>>input;

    int shift;
    cin>>shift;

    // encrypt
    string ans = caeserCipherEnc(input,shift);
    cout<<"Encryption of above input: ";
    cout<<ans<<"\n";

    return 0;
}
```

Output:

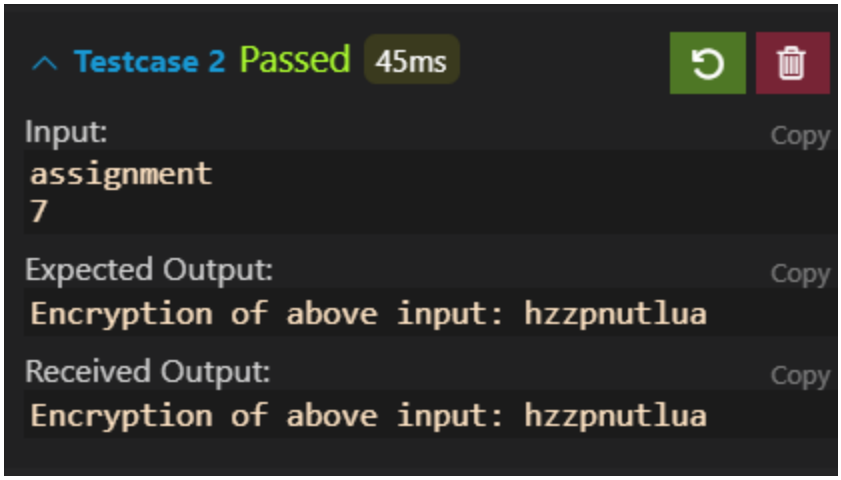
Testcase1:



Testcase 2:



Testcase 3:



Conclusion :

Caesar Cipher is simple substitution technique. The key can be deciphered easily, thus makes it less secure.