Final Year B. Tech. (CSE) – I: 2022-23

4CS451: Cryptography and Network Security Lab

Assignment No. 4

PRN: 2019BTECS00077 **Batch: B7**

Full name: Biradar Avinash Vishnu

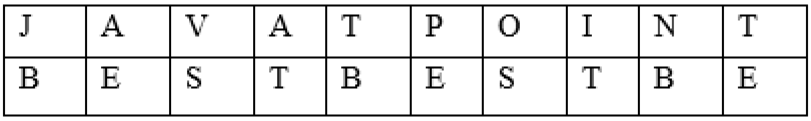
Title: Implementation of Vigenère cipher algorithm.

Objective: write a program to encrypt the plain text and decrypt the cipher text using Vigenère cipher algorithm.

Introduction & Theory:

- Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets

- To generate a new key, the given key is repeated in a circular manner, as long as the length of the plain text does not equal to the new key.



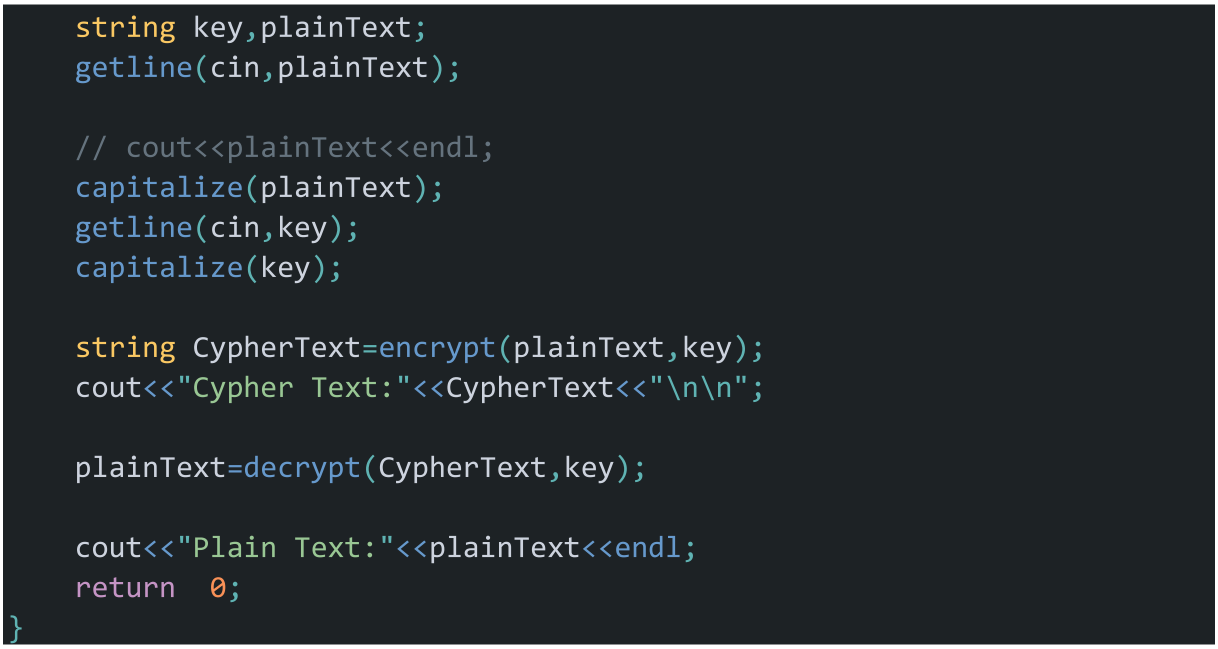
J	A	V	A	T	P	O	I	N	T
B	E	S	T	B	E	S	T	B	E

Encryption

- The first letter of the plaintext is combined with the first letter of the key. The column of plain text "J" and row of key "B" intersects the alphabet of "K" in the Vigenère table, so the first letter of ciphertext is "K".
- Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "A" and row of key "E" intersects the alphabet of "E" in the Vigenère table, so the second letter of ciphertext is "E".
- This process continues continuously until the plaintext is finished.
  Ciphertext = KENTUTGBOX

Code:

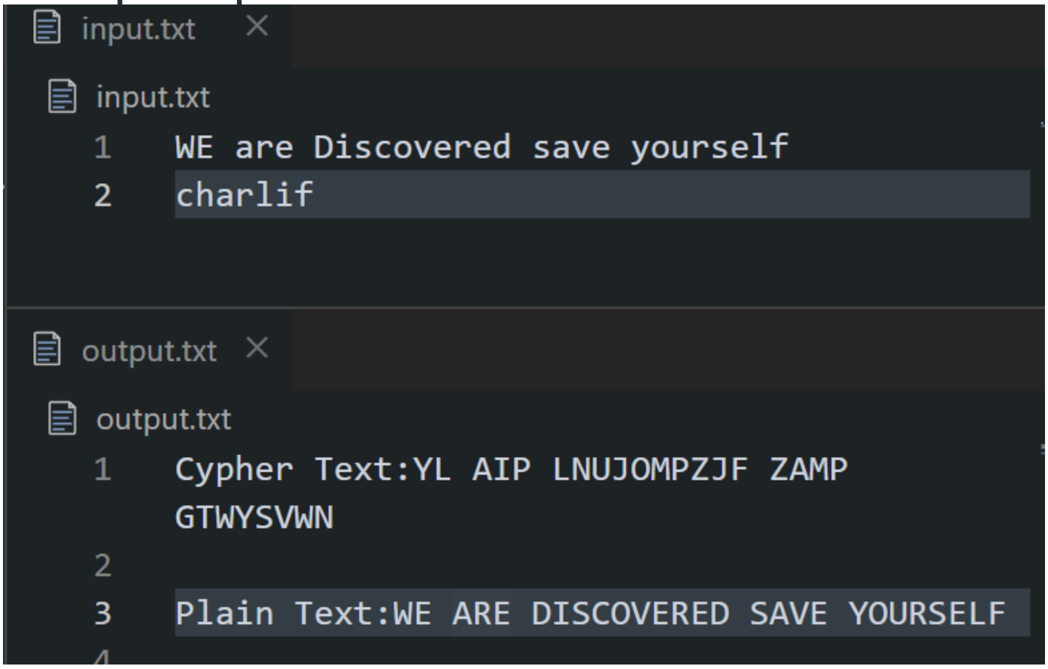
```
#include<bits/stdc++.h>
using namespace std;

// Capitalize the character
void capitalize(string &str){
    for(char &c:str){
      if(c>=97 && c<=122)
        c-=32;
    }
}

string encrypt(string &plainText,string &key){
   int n=key.size();
   int i=0;
   for(char &c:plainText){
       if(c>=65 && c<=90){
         int a=c-65;
         int b=key[i%n]-65;
         c=((a+b)%26+65);
         i++;
       }
   }
   return plainText;
}

string decrypt(string &cypherText,string &key){

   int n=key.size();
   int i=0;
   for(char &c:cypherText){
       if(c>=65 && c<=90){
         int a=c-65;
         int b=key[i%n]-65;
         c=(a-b+26)%26+65;
         i++;
       }
   }
   return cypherText;
}

int main(){

    freopen("input.txt", "r", stdin);
    freopen("output.txt", "w", stdout);

```



```
    string key,plainText;
    getline(cin,plainText);

    // cout<<plainText<<endl;
    capitalize(plainText);
    getline(cin,key);
    capitalize(key);

    string CypherText=encrypt(plainText,key);
    cout<<"Cypher Text:"<<CypherText<<"\n\n";

    plainText=decrypt(CypherText,key);

    cout<<"Plain Text:"<<plainText<<endl;
    return  0;
}
```

Result:

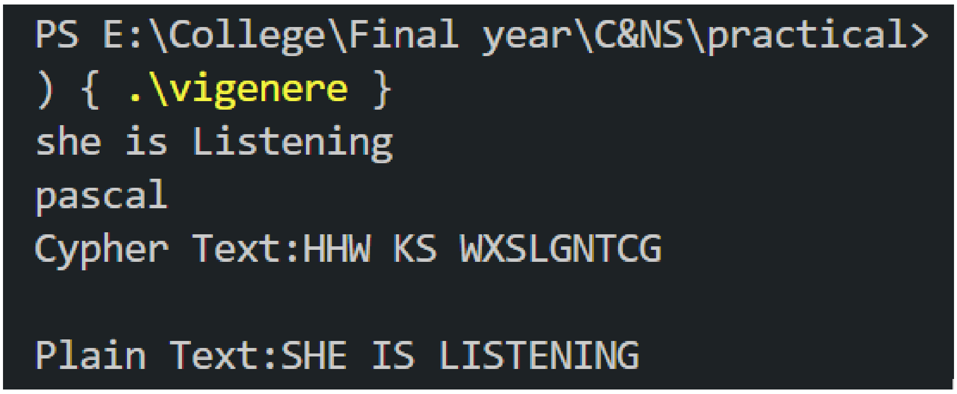
File input output:



```
WE are Discovered save yourself
charlif
```

```
Cypher Text:YL AIP LNUJOMPZJF ZAMP
GTWYSVWN

Plain Text:WE ARE DISCOVERED SAVE YOURSELF
```

Console Input Output:



```
PS E:\College\Final year\C&NS\practical>
) { .\vigenere }
she is Listening
pascal
Cypher Text:HHW KS WXSLGNTCG

Plain Text:SHE IS LISTENING
```