

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

4CS451: Cryptography and Network Security Lab

Assignment No. 1

PRN: 2019BTECS00077

Batch: B7

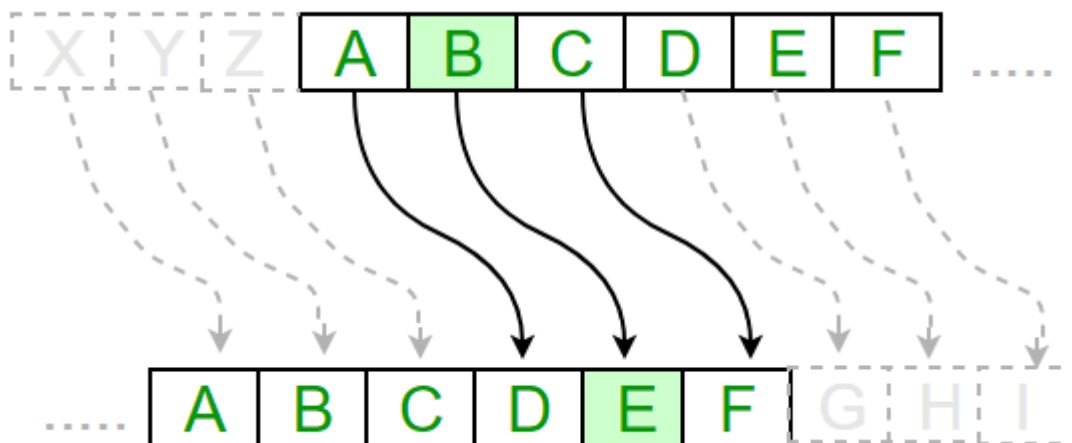
Full name: Biradar Avinash Vishnu

Title: Implementation of Caser Cipher algorithm.

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

Introduction & Theory:

- The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique.
- It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a 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..



Code:

```
// Implementation of Ceasor Cypher
#include<iostream>
using namespace std;
```

```

string encrypt(string plainText,int pos){

    int n=plainText.size();
    for(int i=0;i<n;i++){
        if(plainText[i]==32)
            continue;
        if(plainText[i]>96 && plainText[i]<=122)
            plainText[i]-=32;
        plainText[i]=(plainText[i]-'A'+pos)%26+'A';
    }
    cout<<"\nCypher Text :"<<plainText<<endl;
    return plainText;
}

void decrypt(string cypherText,int pos){
    int n=cypherText.size();
    for(int i=0;i<n;i++){
        if(cypherText[i]==32)
            continue;
        cypherText[i]=(cypherText[i]-'A'-pos+26)%26+'A';
    }
    cout<<"\nPlain Text :"<<cypherText<<endl;
}

int main(){
    int pos;
    freopen("input.txt", "r", stdin);
    freopen("output.txt", "w", stdout);

    string plain_text;
    getline(cin,plain_text);

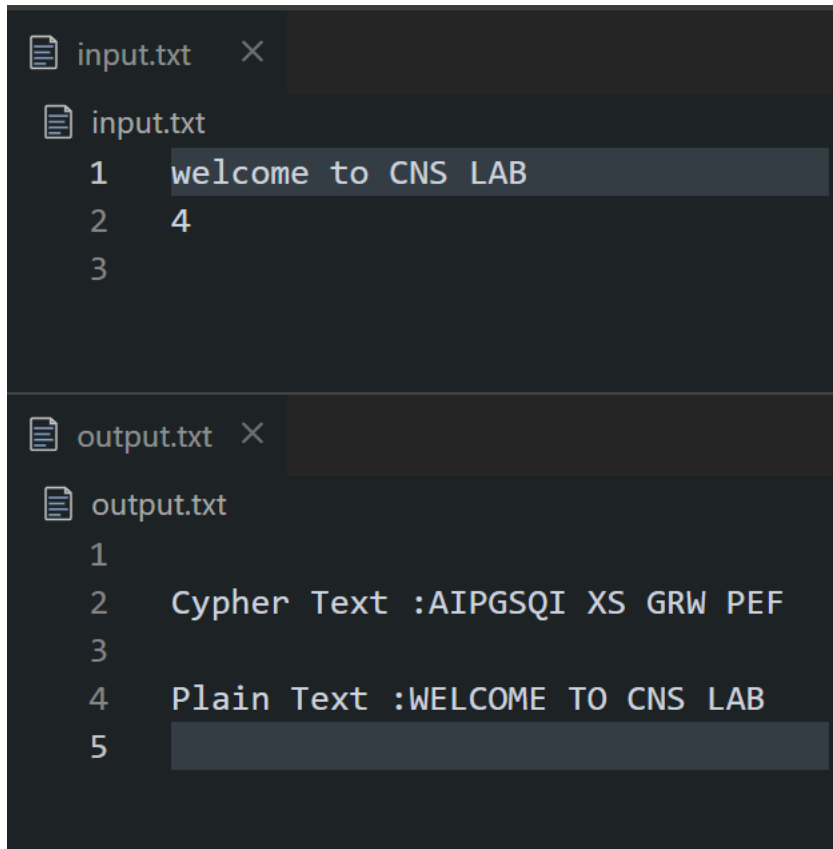
    // cout<<"Plain text:"<<plain_text<<endl;
    cin>>pos;

    string cypher_text=encrypt(plain_text,pos);
    decrypt(cypher_text,pos);
}

```

Result:

File input output:

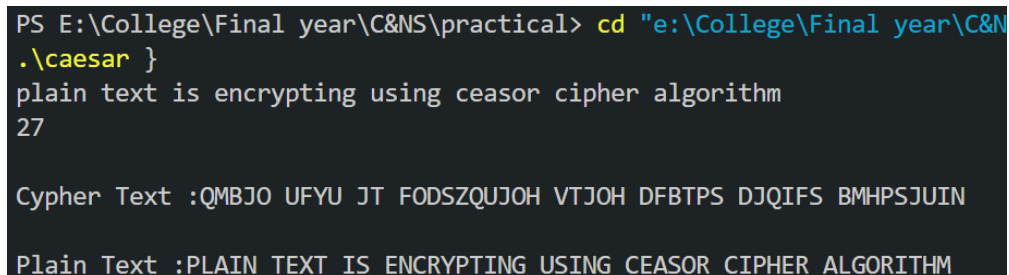


The screenshot shows a text editor with two tabs: 'input.txt' and 'output.txt'. The 'input.txt' tab is active, showing three lines of text: '1 welcome to CNS LAB', '2 4', and '3'. The 'output.txt' tab is also visible, showing five lines of text: '1', '2 Cypher Text :AIPGSQI XS GRW PEF', '3', '4 Plain Text :WELCOME TO CNS LAB', and '5'.

```
input.txt  X
1 welcome to CNS LAB
2 4
3

output.txt  X
1
2 Cypher Text :AIPGSQI XS GRW PEF
3
4 Plain Text :WELCOME TO CNS LAB
5
```

Console input output:



The screenshot shows a command prompt window with the following text: 'PS E:\College\Final year\C&NS\practical> cd "e:\College\Final year\C&N', '.\caesar }', 'plain text is encrypting using ceasor cipher algorithm', '27', 'Cypher Text :QMBJO UFYU JT FODSZQUJOH VTJOH DFBTPS DJQIFS BMHPSJUIN', and 'Plain Text :PLAIN TEXT IS ENCRYPTING USING CEASOR CIPHER ALGORITHM'.

```
PS E:\College\Final year\C&NS\practical> cd "e:\College\Final year\C&N
.\caesar }
plain text is encrypting using ceasor cipher algorithm
27
Cypher Text :QMBJO UFYU JT FODSZQUJOH VTJOH DFBTPS DJQIFS BMHPSJUIN
Plain Text :PLAIN TEXT IS ENCRYPTING USING CEASOR CIPHER ALGORITHM
```