

**Final Year B. Tech., Sem VII 2022-23**

## **Cryptography And Network Security**

**PRN: 2020BTECS00206**

**Full Name: SAYALI YOGESH DESAI**

**Batch: B4**

### **Assignment No. 1**

---

**1. Aim:**

To encrypt the given plain text using Caesar Cipher and then decrypt it to get the plain text again.

**2. Theory:**

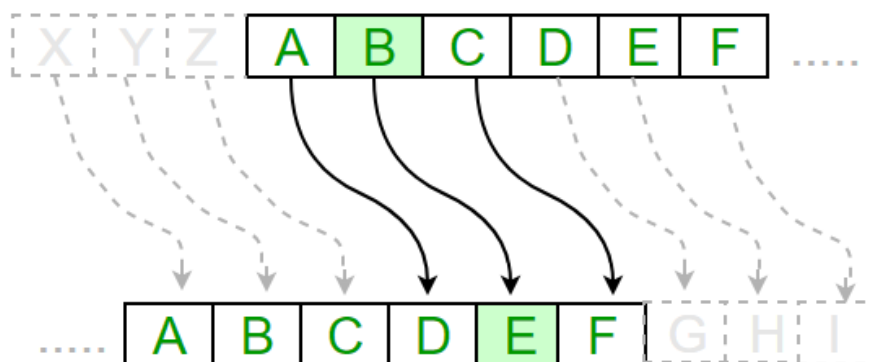
It's a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus, to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.

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.



**Examples:**

**Text:** ABCDEFGHIJKLMNOPQRSTUVWXYZ

**Shift:** 23

**Cipher:** XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

**3. Code:**

```
// Implementation of Caesar Cipher
#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<<"\nCipher 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;
}

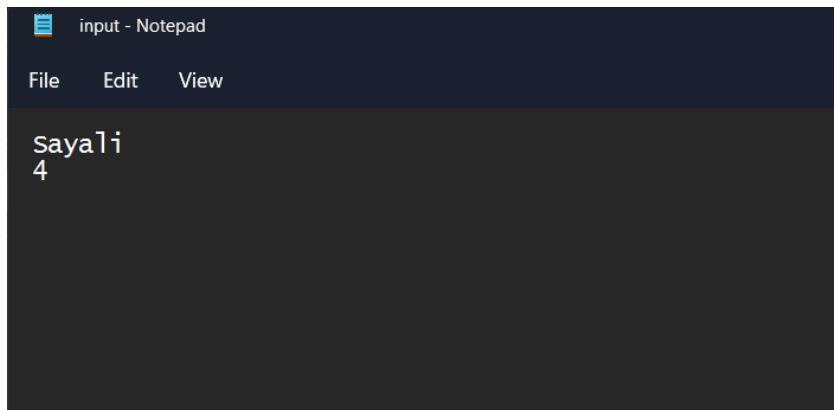
int main(){
    int pos;
    freopen("input.txt", "r", stdin);
    freopen("output.txt", "w", stdout);

    string plain_text;
    getline(cin,plain_text);

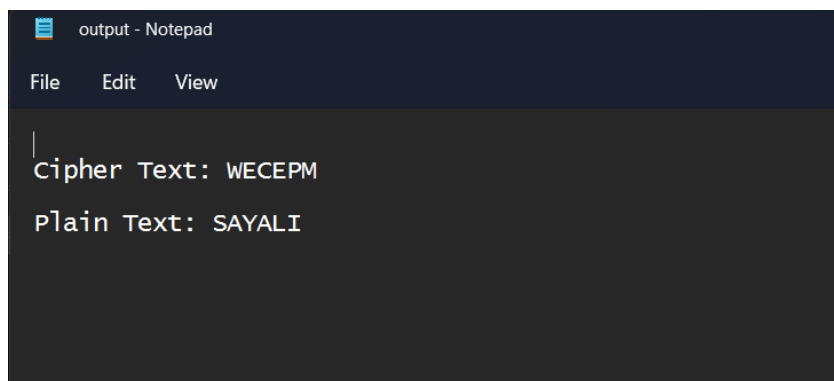
    // cout<<"Plain text:"<<plain_text<<endl;
    cin>>pos;

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

#### 4. Input:



#### 5. Output:



#### 6. Conclusion:

I have successfully encrypted and decrypted the plain text using Caesar cipher algorithm.