

Final Year B. Tech, Sem VII 2022-23
PRN – 2020BTECS00211
Name – Aashita Narendra Gupta
Cryptography And Network Security Lab
Batch: B4

Practical No – 1

Title: To implement Ceaser Cipher.

Theory:

The Caesar cipher method is based on a mono-alphabetic cipher and is also called a shift cipher or additive cipher. Julius Caesar used the shift cipher (additive cipher) technique to communicate with his officers. For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter.

The formula of encryption is:

$$En(x) = (x + n) \bmod 26$$

The formula of decryption is:

$$Dn(x) = (xi - n) \bmod 26$$

If any case (Dn) value becomes negative (-ve), in this case, we will add 26 in the negative value.

E denotes the encryption

D denotes the decryption

x denotes the letters value

n denotes the key value (shift value)

Example:

Encryption:

Message - The sky is pink

Key - 5

Plaintext: T \rightarrow 20 En: $(20 + 5) \bmod 26$ Ciphertext: 25 \rightarrow Y

Likewise,

Encrypted message - Ymj xpd nx unsp

Decryption:

Message - Ymj xpd nx unsp

Key – 5

Plaintext: Y \rightarrow 25 Dn: $(25 - 5) \bmod 26$ Ciphertext: 20 \rightarrow T

Likewise,
Decrypted message - The sky is pink

Code Snapshots:

```
#include<iostream>

#include<string.h>
using namespace std;
int main()
{
    cout<<"Enter the message:\n";
    char msg[100];
    cin.getline(msg,100); //take the message as input
    int i, j, length,choice,key;
    cout << "Enter key: ";
    cin >> key; //take the key as input
    length = strlen(msg);
    cout<<"Enter your choice \n1. Encryption \n2. Decryption \n";
    cout<<"Your Choice: ";
    cin>>choice;
    if (choice==1) //for encryption
    {
        char ch;
        for(int i = 0; msg[i] != '\0'; ++i)
        {
            ch = msg[i];
            //encrypt for lowercase letter
            if(ch >= 'a' && ch <= 'z')
            {
                ch = ch + key;
                if (ch > 'z') {
                    ch = ch - 'z' + 'a' - 1;
                }
                msg[i] = ch;
            }
            //encrypt for uppercase letter
            else if (ch >= 'A' && ch <= 'Z'){
                ch = ch + key;
                if (ch > 'Z'){
                    ch = ch - 'Z' + 'A' - 1;
                }
                msg[i] = ch;
            }
        }
        printf("Encrypted message: %s", msg);
    }
    else
```

```

    if (choice == 2) { //for decryption
        char ch;
        for(int i = 0; msg[i] != '\0'; ++i) {
            ch = msg[i];
            //decrypt for lowercase letter
            if(ch >= 'a' && ch <= 'z') {
                ch = ch - key;
                if(ch < 'a'){
                    ch = ch + 'z' - 'a' + 1;
                }
                msg[i] = ch;
            }
            //decrypt for uppercase letter
            else if(ch >= 'A' && ch <= 'Z') {
                ch = ch - key;
                if(ch < 'A') {
                    ch = ch + 'Z' - 'A' + 1;
                }
                msg[i] = ch;
            }
        }
        cout << "Decrypted message: " << msg;
    }
}

```

Output Snapshots:

Encryption:

```

PROBLEMS  OUTPUT  TERMINAL  DEBUG CONSOLE

PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs> cd "c:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs\" ; if ($?) { g++ CeaserCipherED.cpp -o CeaserCipherED } ; if ($?) { .\CeaserCipherED }
Enter the message:
The sky is pink
Enter key: 5
Enter your choice
1. Encryption
2. Decryption
Your Choice: 1
Encrypted message: Ymj xpd nx unsp
PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs> 

```

Decryption:

```

PROBLEMS  OUTPUT  TERMINAL  DEBUG CONSOLE

PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs> cd "c:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs\" ; if ($?) { g++ CeaserCipherED.cpp -o CeaserCipherED } ; if ($?) { .\CeaserCipherED }
Enter the message:
Ymj xpd nx unsp
Enter key: 5
Enter your choice
1. Encryption
2. Decryption
Your Choice: 2
Decrypted message: The sky is pink
PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs> 

```

Conclusion:

1. Caesar cipher algorithm can be implemented in many encryption projects to make data secure and better.
2. Implementation of Caesar Cipher Algorithm is easy in comparison with other algorithms.
3. Caesar cipher is not that strong in terms of providing security.