C&NS Lab Assignment 1

Onkar Santosh Gavali (2019BTECS00037)

Batch B2

Index

Caesar cipher

The Caesar cipher is one of the simplest and most widely known encryption techniques. It is also popular as one of the earliest known substitution ciphers. It had been used by Julius Caesar to communicate with his army. It requires one integer key to encrypt plain text and decrypt the cipher text. It encrypts one letter of plain text each time so the decryption.

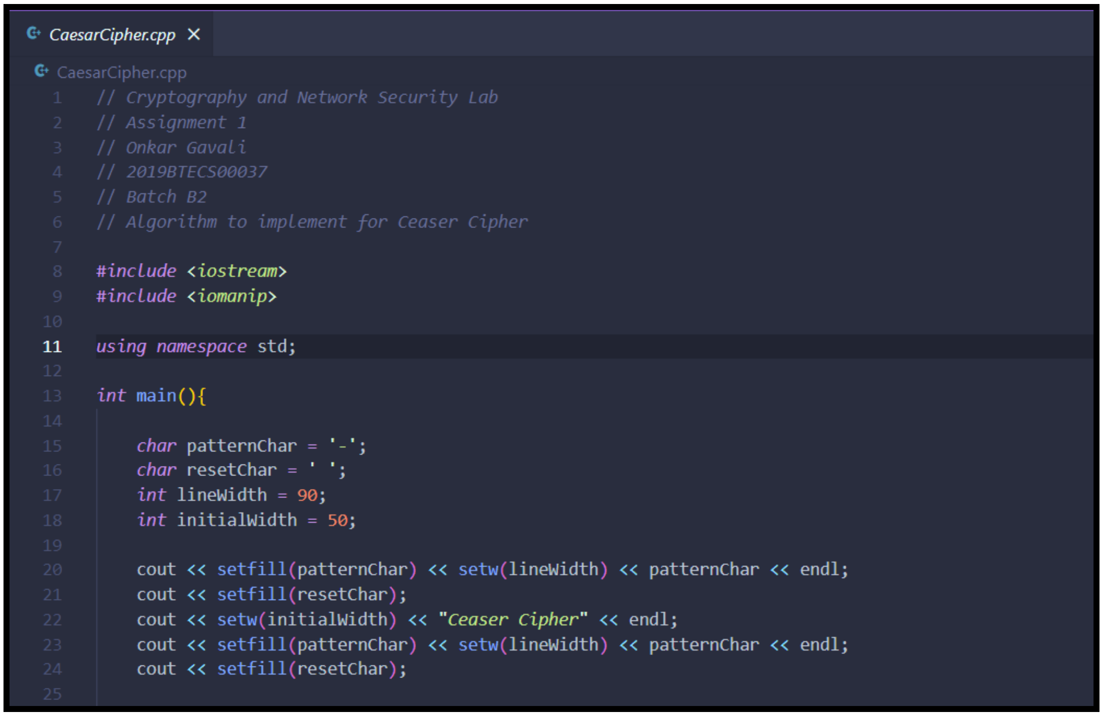
Eg. let's suppose the given letter is **‘char_$’** and the key is **“INT_KEY”**

Then the encrypted letter will be **“encryted_char_$”=** ***“(char_$+INT_KEY)”.***

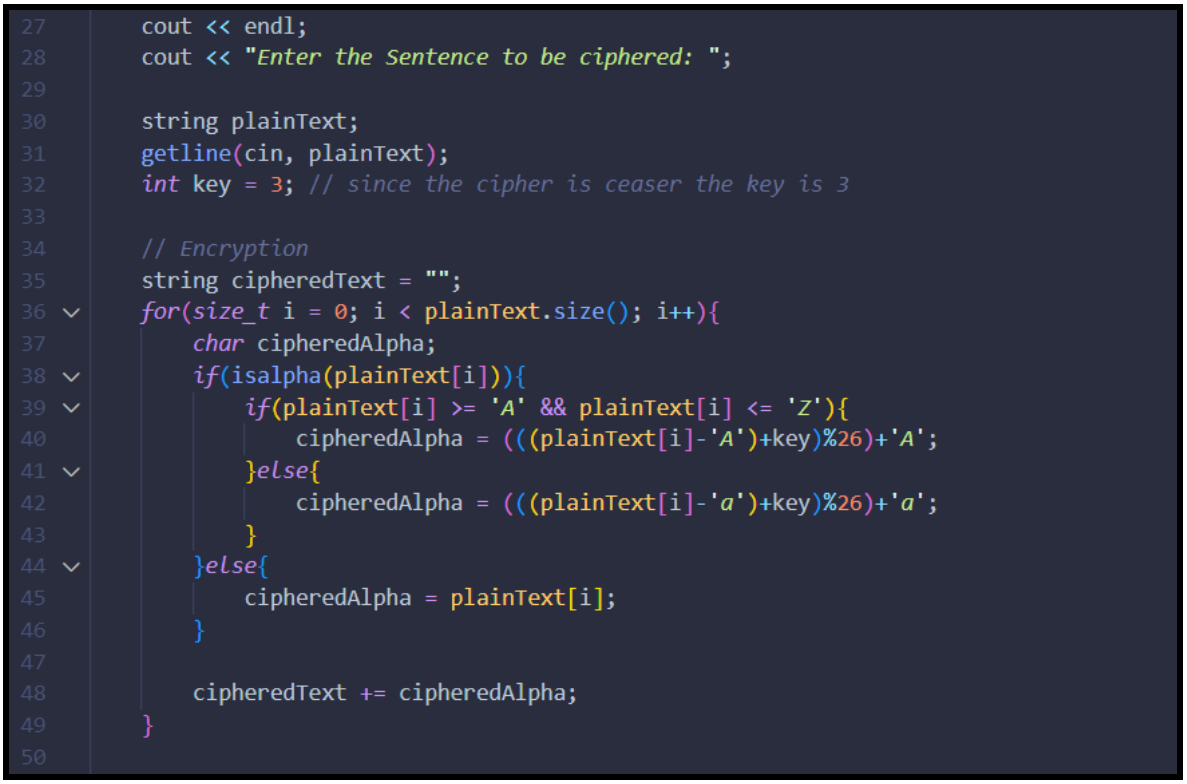
We use the same key to decrypt the letter where plain text can be required by performing option ***“(*****encryted_char_*****$-INT_KEY)”.***

key	**A**	**a**	**B**	**b**	**…..**	**x**	**y**	**Z**	**z**
1	*B*	*b*	*C*	*c*	….	*y*	*z*	*A*	*a*
2	*C*	*c*	*D*	*d*	….	*z*	*a*	*B*	*b*
25	*Z*	*z*	*A*	*a*	….	*w*	*x*	*Y*	*y*
26	*A*	*a*	*B*	*b*	….	*x*	*y*	*Z*	*z*
27	*B*	*b*	*C*	*c*	….	*y*	*z*	*A*	*a*

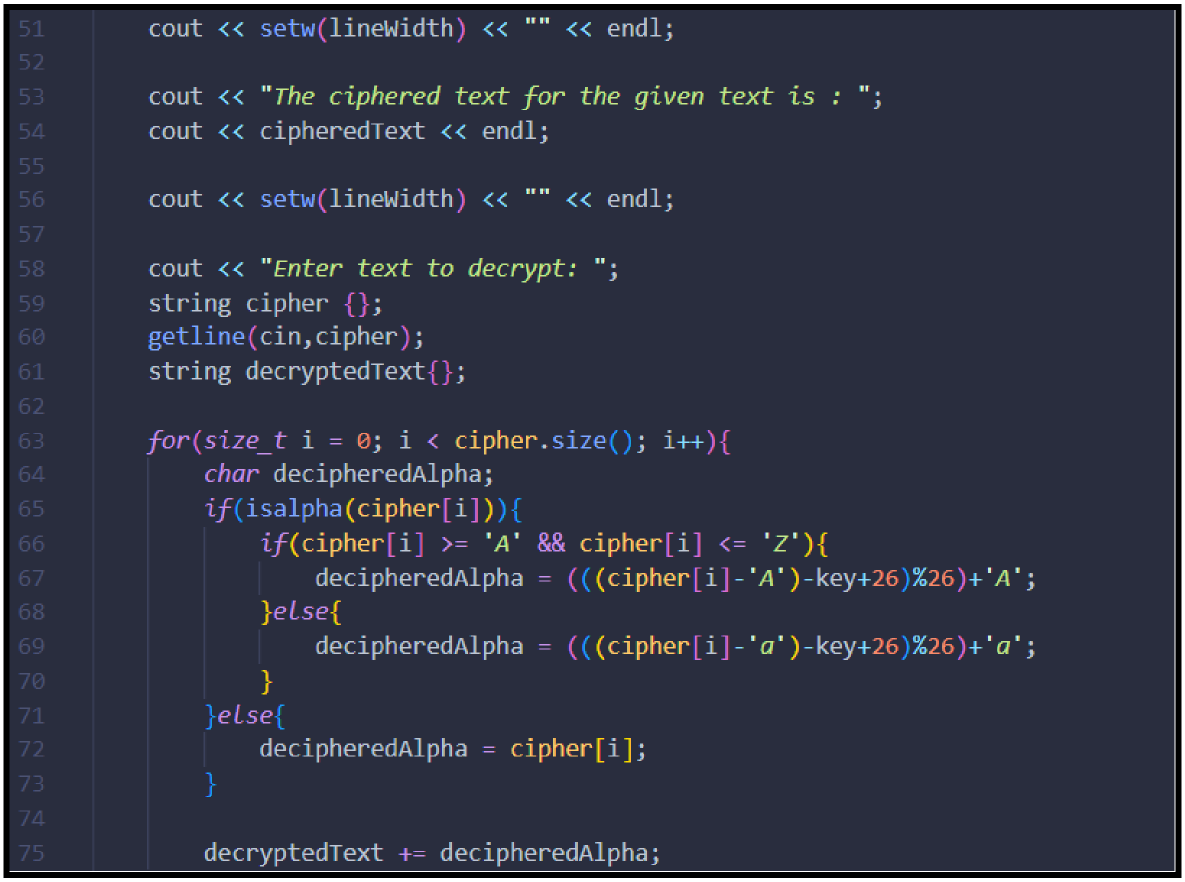
Code



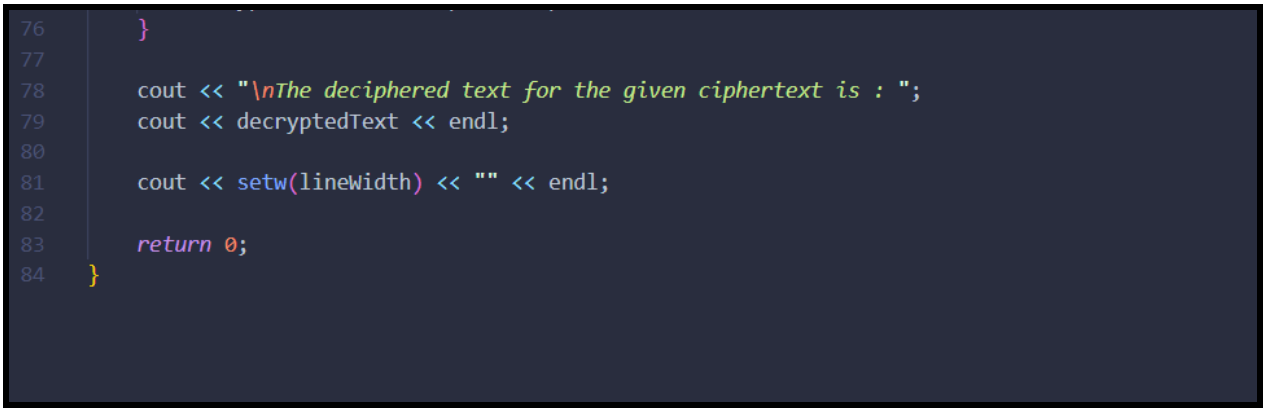
```cpp
// Cryptography and Network Security Lab
// Assignment 1
// Onkar Gavali
// 2019BTECS00037
// Batch B2
// Algorithm to implement for Ceaser Cipher

#include <iostream>
#include <iomanip>

using namespace std;

int main(){

    char patternChar = '-';
    char resetChar = ' ';
    int lineWidth = 90;
    int initialWidth = 50;

    cout << setfill(patternChar) << setw(lineWidth) << patternChar << endl;
    cout << setfill(resetChar);
    cout << setw(initialWidth) << "Ceaser Cipher" << endl;
    cout << setfill(patternChar) << setw(lineWidth) << patternChar << endl;
    cout << setfill(resetChar);

```



```cpp
    cout << endl;
    cout << "Enter the Sentence to be ciphered: ";

    string plainText;
    getline(cin, plainText);
    int key = 3; // since the cipher is ceaser the key is 3

    // Encryption
    string cipheredText = "";
    for(size_t i = 0; i < plainText.size(); i++){
        char cipheredAlpha;
        if(isalpha(plainText[i])){
            if(plainText[i] >= 'A' && plainText[i] <= 'Z'){
                cipheredAlpha = (((plainText[i]-'A')+key)%26)+'A';
            }else{
                cipheredAlpha = (((plainText[i]-'a')+key)%26)+'a';
            }
        }else{
            cipheredAlpha = plainText[i];
        }

        cipheredText += cipheredAlpha;
    }

```

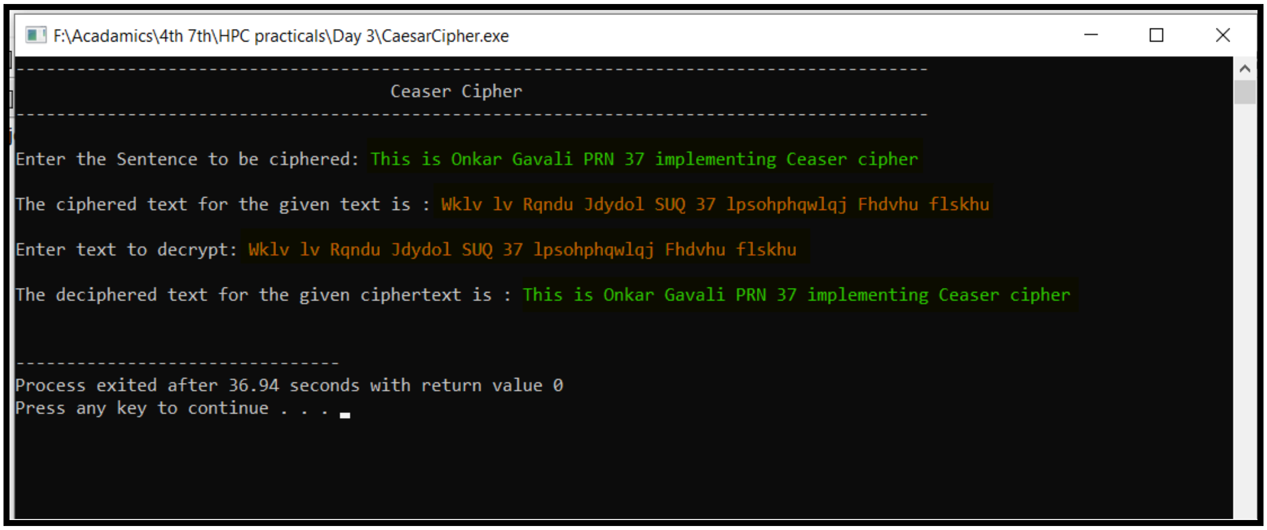


```
    cout << setw(lineWidth) << "" << endl;

    cout << "The ciphered text for the given text is : ";
    cout << cipheredText << endl;

    cout << setw(lineWidth) << "" << endl;

    cout << "Enter text to decrypt: ";
    string cipher {};
    getline(cin,cipher);
    string decryptedText{};

    for(size_t i = 0; i < cipher.size(); i++){
        char decipheredAlpha;
        if(isalpha(cipher[i])){
            if(cipher[i] >= 'A' && cipher[i] <= 'Z'){
                decipheredAlpha = (((cipher[i]-'A')-key+26)%26)+'A';
            }else{
                decipheredAlpha = (((cipher[i]-'a')-key+26)%26)+'a';
            }
        }else{
            decipheredAlpha = cipher[i];
        }

        decryptedText += decipheredAlpha;
```



```
    }

    cout << "\nThe deciphered text for the given ciphertext is : ";
    cout << decryptedText << endl;

    cout << setw(lineWidth) << "" << endl;

    return 0;
}
```

Output:



```
------------------------------------------------------------------------------------------
                                     Ceaser Cipher
------------------------------------------------------------------------------------------

Enter the Sentence to be ciphered: This is Onkar Gavali PRN 37 implementing Ceaser cipher

The ciphered text for the given text is : Wklv lv Rqndu Jdydol SUQ 37 lpsohphqwlqj Fhdvhu flskhu

Enter text to decrypt: Wklv lv Rqndu Jdydol SUQ 37 lpsohphqwlqj Fhdvhu flskhu

The deciphered text for the given ciphertext is : This is Onkar Gavali PRN 37 implementing Ceaser cipher


--------------------------------
Process exited after 36.94 seconds with return value 0
Press any key to continue . . .
```

Conclusion

It was one of the simplest encryption algorithms. It is easy to learn and substitution based. It shifted letters by definite alphabets.

Pros:

- Simple and easy to learn
- Easy to implement

Cons:

- Limited sample space (only 26)
- Easy to decrypt code
- Failed because of the high computing power of Today's computers.

References

- https://en.wikipedia.org/wiki/Caesar_cipher