Cryptography and Network Security Lab

PRN: 2019BTECS00090

Name: Udaykumar Gadikar

Batch: B8

Assignment No. 2

Title:

Caesar Cipher Decryption (Cryptanalysis)

Aim:

To implement Caesar Cipher Decryption using Console and file input for cryptanalysis.

Theory:

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption-decryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.

Procedure:

$$D_n(x)=(x-n+26)\%\ 26$$

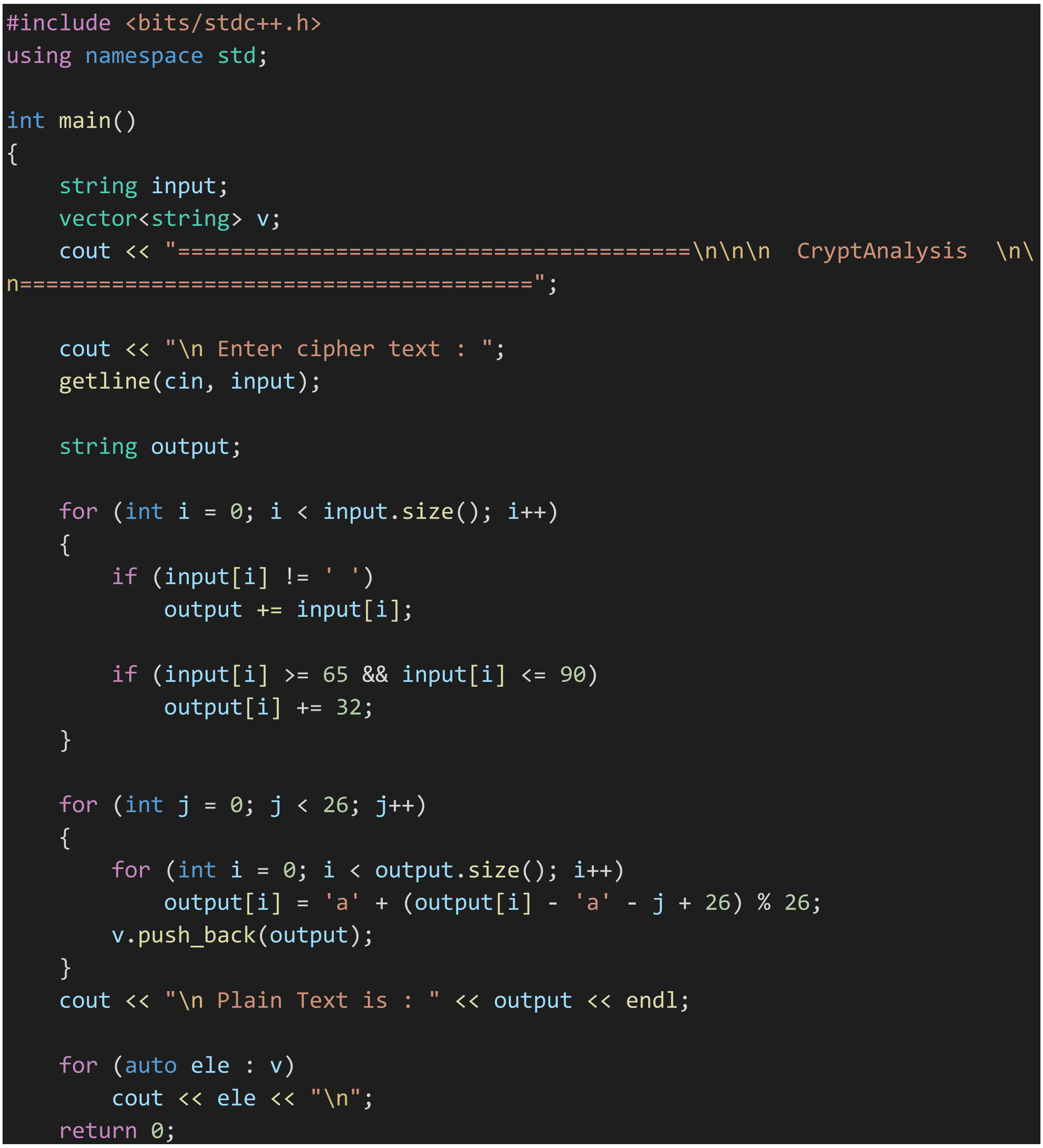
(Decryption Phase where x is input character and n is given key)

- Traverse the given text one character at a time.
- For each character, transform the given character as per the rule and encrypt plain text using key.
- Return the new string generated.

Code:

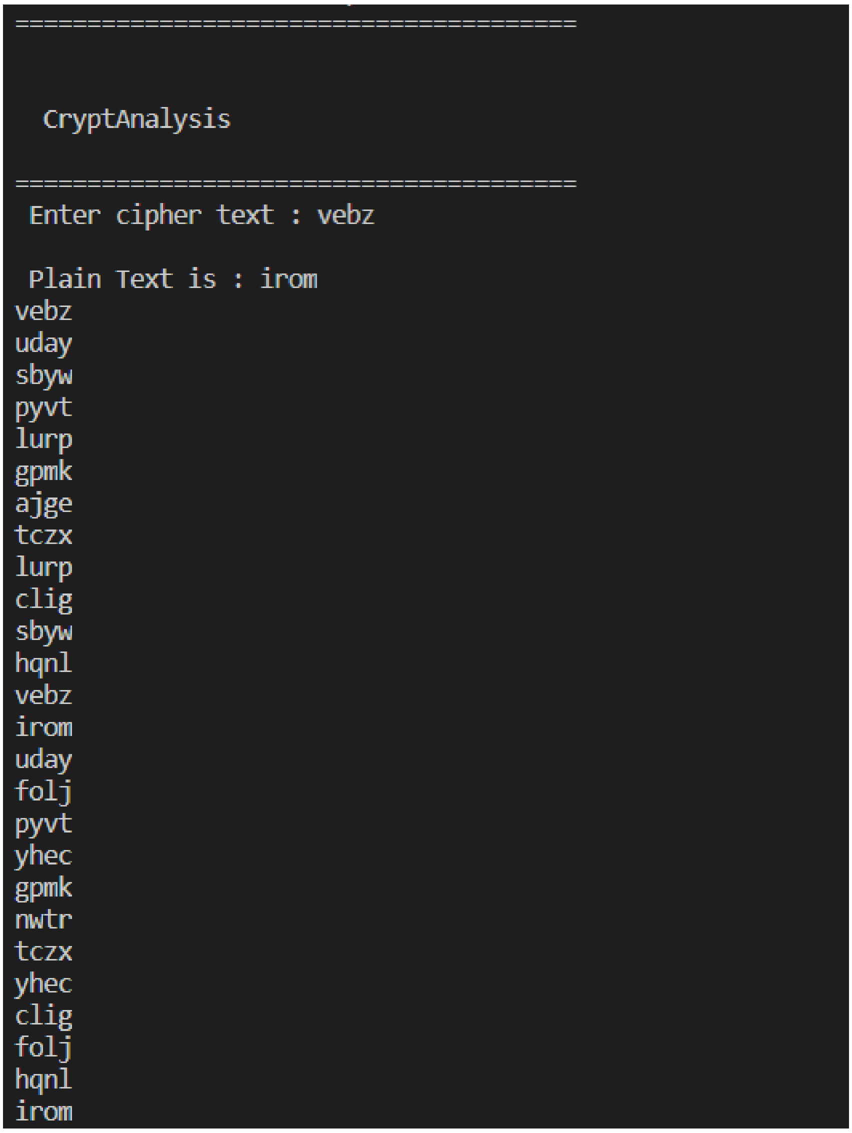
Console Input Code:

File Input Code:



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

int main()
{
    string input;
    vector<string> v;
    cout << "=======================================\n\n\n  CryptAnalysis  \n\
n=======================================";

    cout << "\n Enter cipher text : ";
    getline(cin, input);

    string output;

    for (int i = 0; i < input.size(); i++)
    {
        if (input[i] != ' ')
            output += input[i];

        if (input[i] >= 65 && input[i] <= 90)
            output[i] += 32;
    }

    for (int j = 0; j < 26; j++)
    {
        for (int i = 0; i < output.size(); i++)
            output[i] = 'a' + (output[i] - 'a' - j + 26) % 26;
        v.push_back(output);
    }
    cout << "\n Plain Text is : " << output << endl;

    for (auto ele : v)
        cout << ele << "\n";
    return 0;
}
```

Output:



```
=========================================


  CryptAnalysis

=========================================
 Enter cipher text : vebz

 Plain Text is : irom
vebz
uday
sbyw
pyvt
lurp
gpmk
ajge
tczx
lurp
clig
sbyw
hqnl
vebz
irom
uday
folj
pyvt
yhec
gpmk
nwtr
tczx
yhec
clig
folj
hqnl
irom
```

Conclusion:

Caesar Cipher is simple substitution technique. It falls in category of monoalphabetic cipher where each character is substituted by addition of that character with given key. The key can be deciphered easily, thus makes it less secure.