**Assignment No 3**

**Name-Aniket Tatoba Mane**

**PRN-2020BTECS00020**

**Batch-B7**

**Subject - CNS LAB**

**Aim**: To implement Vigenere cipher

**Theory**: The Vigenère Cipher is a polyalphabetic substitution cipher that uses a keyword to shift letters in the plaintext. The keyword is repeated to match the length of the message, and each letter of the keyword determines the shift value.

Code:

#include <bits/stdc++.h>

using namespace std;

string alpah\_lower(string str)

{

    for (char c : str)

    {

        if (isalpha(c))

        {

            c += tolower(c);

        }

    }

    return str;

}

string encrypt(string text, string key)

{

    string cipher;

    for (int i = 0; i < text.size(); i++)

    {

        int val = text[i] - 'a' + key[i % (key.size())] - 'a';

        cipher += ('a' + (val % 26));

    }

    return cipher;

}

string decrypt(string cipher, string key)

{

    string text;

    for (int i = 0; i < cipher.size(); i++)

    {

        int val = cipher[i] - 'a' - (key[i % (key.size())] - 'a');

        text += ('a' + (val + 26) % 26);

    }

    return text;

}

int main()

{

    int choice;

    cout << "1. Encrypt\n2. Decrypt\nEnter your choice: ";

    cin >> choice;

    cin.get();

    if (choice == 1)

    {

        string plain, key;

        cout << "\nEnter plain text: ";

        getline(cin, plain);

        plain = alpah\_lower(plain);

        cout << "\nEnter key: ";

        getline(cin, key);

        string cipher = encrypt(plain, key);

        cout << "\nEncrypted text is : " << cipher << endl;

    }

    else if (choice == 2)

    {

        string cipher, key;

        cout << "\nEnter cipher text: ";

        getline(cin, cipher);

        cipher = alpah\_lower(cipher);

        cout << "\nEnter key: ";

        getline(cin, key);

        string plain = decrypt(cipher, key);

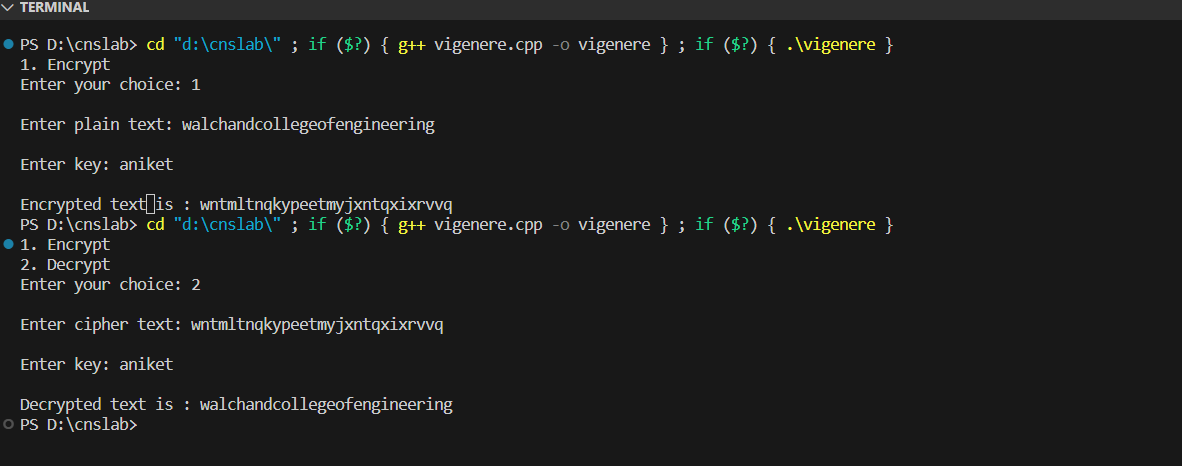
        cout << "\nDecrypted text is : " << plain << endl;

    }

    return 0;

}

Output:



Advantages:

Polyalphabetic Substitution: Unlike the Caesar cipher, which uses a single fixed shift value for all characters, the Vigenère cipher uses a keyword to determine different shift values for each character in the plaintext. This makes it more complex and less susceptible to simple frequency analysis attacks.

Resistance to Brute Force: With a sufficiently long and random keyword, the Vigenère cipher can be resistant to brute force attacks. The number of possible keys grows significantly with the length of the keyword, making it computationally infeasible to try all combinations.

Limitations:

Repeating nature of the key (largest weakness that leads to other weaknesses).

Because the key repeats it makes it much easier to guess the length of the key. Using Kasiski examination and the Friedman test the length of the key can be found much faster than brute force methods