**Final Year B.Tech. (CSE) – II [ 2021-22 ]**

**Cryptograpy and Network Security Lab**

**PRN: 2019BTECS00015**

**Full name: Shraddha Sanjay Kharat**

**Batch: B1**

**Assignment no -4**

**Date: 23-08-2022**

**Que )** **Vigenere Cipher implementation**

**Objective :**

To implement Vigenere Cipher in C

**Theory:**

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table* .The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers .At different points in the encryption process, the cipher uses a different alphabet from one of the rows.The alphabet used at each point depends on a repeating keyword.

**Code Snapshots:**

#include <bits/stdc++.h>

using namespace std;

string GenerateKey(string text, string key)

{

    int i = 0;

    while (key.size() != text.size())

    {

        key.push\_back(key[i]);

        i++;

    }

    return key;

}

string VigenreCipherEncrypt(string text, string key)

{

    string ciphertext;

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

    {

        char x = (text[i] + key[i]) % 26;

        x += 'A';

        ciphertext.push\_back(x);

    }

    return ciphertext;

}

string VigenreCipherDecrypt(string ciphertext, string key)

{

    string text;

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

    {

        char x = (ciphertext[i] - key[i] + 26) % 26;

        x += 'A';

        text.push\_back(x);

    }

    return text;

}

int main()

{

    int option;

    string key, text, ciphertext;

    cout << "Enter option:\n1)Console\n2)File\n";

    cin >> option;

    cout << "Enter key: ";

    cin >> key;

    switch (option)

    {

    case 1:

        cout << "Enter text: ";

        break;

    case 2:

        freopen("input.txt", "r", stdin);

        freopen("output.txt", "w", stdout);

        break;

    }

    cin >> text;

    key = GenerateKey(text, key);

    ciphertext = VigenreCipherEncrypt(text, key);

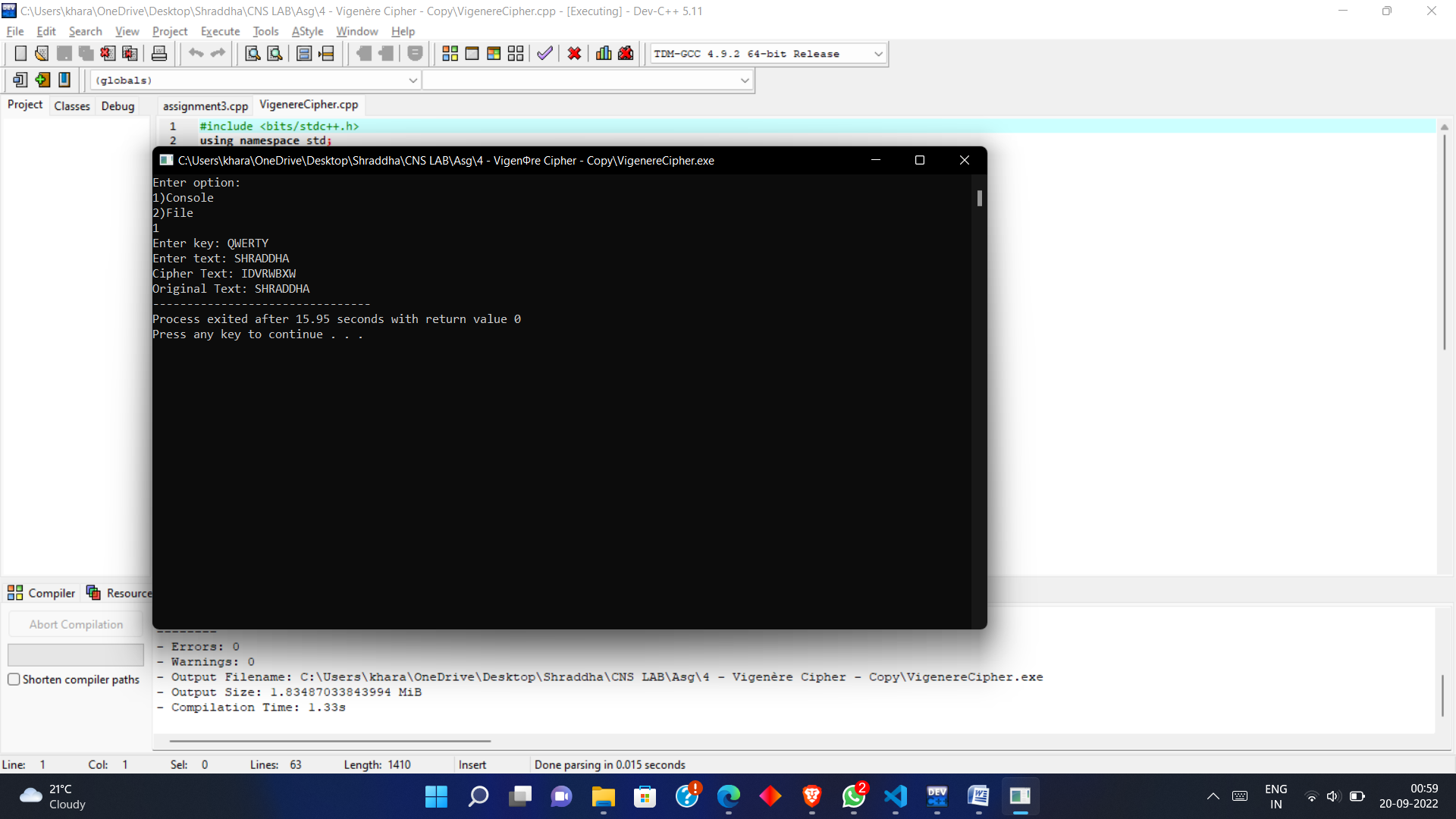
    cout << "Cipher Text: " << ciphertext << endl;

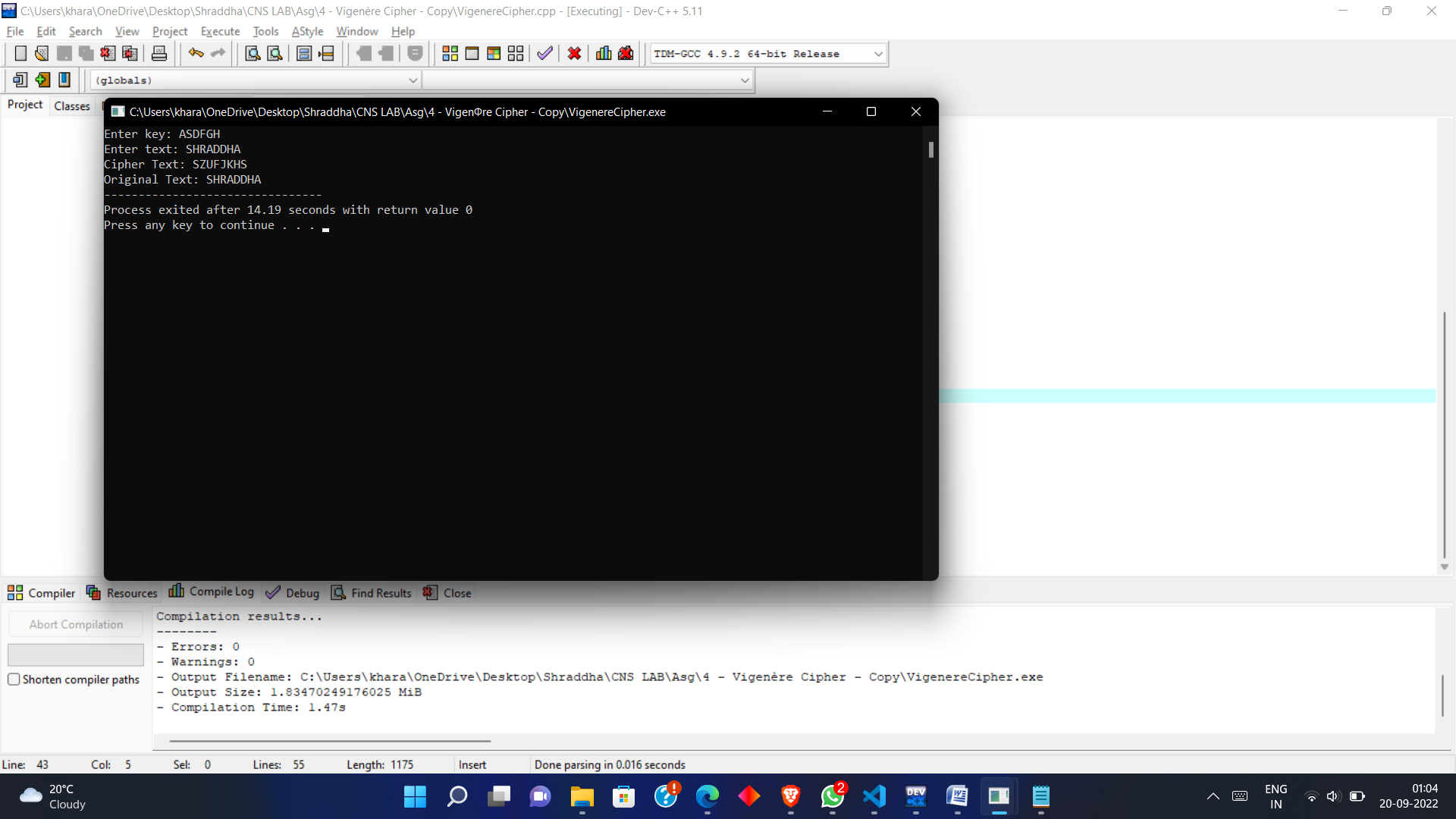
    cout << "Original Text: " << VigenreCipherDecrypt(ciphertext, key);

    return 0;

}

**Output:**





* **Conclusion** :

Vigenere Cipher is polyalphabetic substition cipher , in which a single alphabet can be encrypted with different alphabets when its occurrence is repeated.