C&NS Lab Assignment 3

Onkar Santosh Gavali (2019BTECS00037)

Batch B2

Index

Vigenere cipher

Vigener Cipher is another simple polyalphabetic substitution cipher. It is the same as the caesar cipher instead of an integer key it has a string key.

Plain text	z	a	e	a	d	d
key(abc)	a	b	c	a	b	c
Cipher text	z	b	g	a	e	f

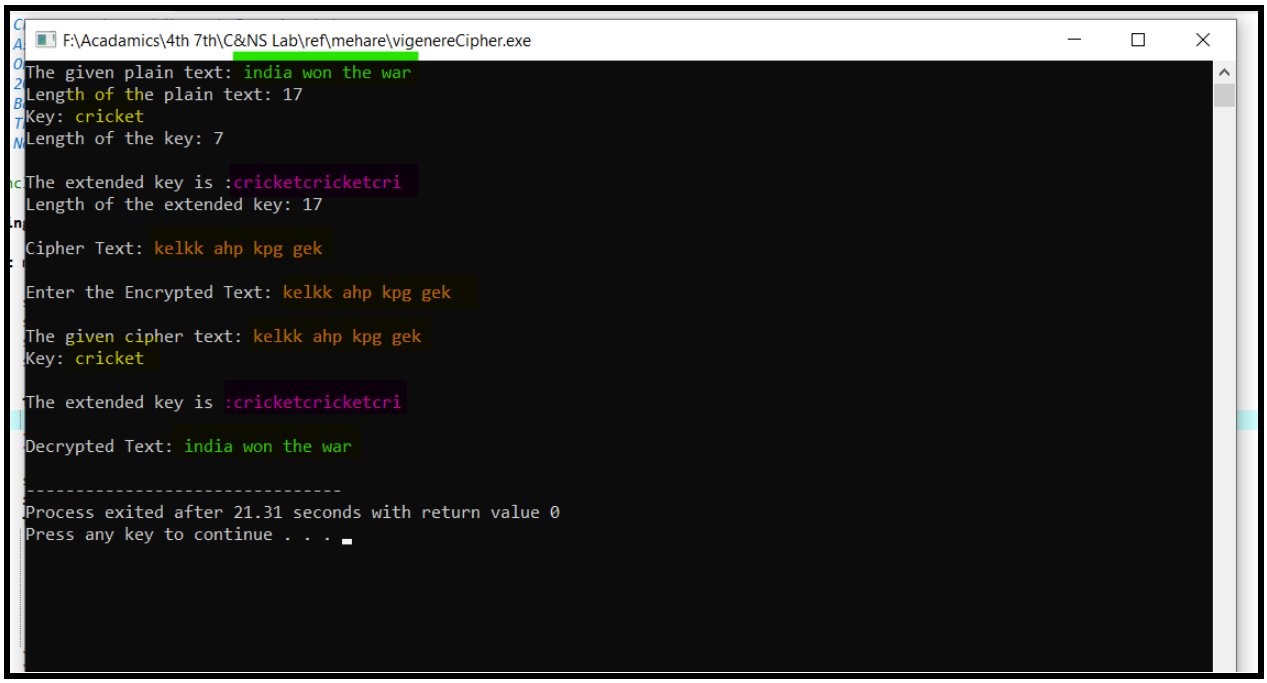
Code

vigenereCipher.cpp

```cpp
// Cryptography and Network Security Lab
// Assignment 3
// Onkar Gavali
// 2019BTECS00037
// Batch B2
// This programs demonstrates the vigenere cipher
// Note: length of key in vigenere cipher should be lesser than or equal to plain text

#include <iostream>

using namespace std;

int main() {

    string plainText = "india won the war";
    string key = "cricket";
    size_t keyLength = key.size();
    string extendedKey {};

    for(size_t i = 0; i < plainText.size(); i++){
        extendedKey += key[i%keyLength];
    }

    string cipherText{};
    int j = 0;
```

```
    for(size_t i = 0; i < plainText.size(); i++){
        if(plainText[i] == ' '){
            cipherText += ' ';
        }else{
            cipherText += (((plainText[i]-'a')+(extendedKey[j]-'a'))%26)+'a';
            j++;
        }
    }

    cout << "The given plain text: " << plainText << endl;
    cout << "Length of the plain text: " << plainText.length() << endl;
    cout << "Key: " << key << endl;
    cout << "Length of the key: " << key.length() << endl;
    cout << "\nThe extended key is :" << extendedKey << endl;
    cout << "Length of the extended key: " << extendedKey.length() << endl;
    cout << "\nCipher Text: " << cipherText << endl;

    string encryptedText{};
    string decryptedText{};
    cout << "\nEnter the Encrypted Text: ";
    getline(cin, encryptedText);

    j = 0;
    for(size_t i = 0; i < encryptedText.size(); i++){
        if(encryptedText[i] == ' '){
            decryptedText += ' ';
        }else{
            decryptedText += (((encryptedText[i] - 'a')-(extendedKey[j]-'a')+26)%26)+'a';
            j++;
        }
    }

    cout << "\nThe given cipher text: " << encryptedText << endl;
    cout << "Key: " << key << endl;
    cout << "\nThe extended key is :" << extendedKey << endl;
    cout << "\nDecrypted Text: " << decryptedText << endl;

    return 0;
}
```

Output



Conclusion

- Vigenere cipher is better than other early substitution ciphers. Brute force attacks were difficult to decode Vigenere cipher.
- Because the same characters in plaintext ciphered with the same character for each instance that character are quite rare makes it difficult to decrypt its code without the key.