

C&NS Lab Assignment 3

Onkar Santosh Gavali (2019BTECS00037)

Batch B2

Index

Vigenere cipher

- Explain the Vigenere cipher.
- Implement the Vigenere cipher algorithm using any programming language.

### 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

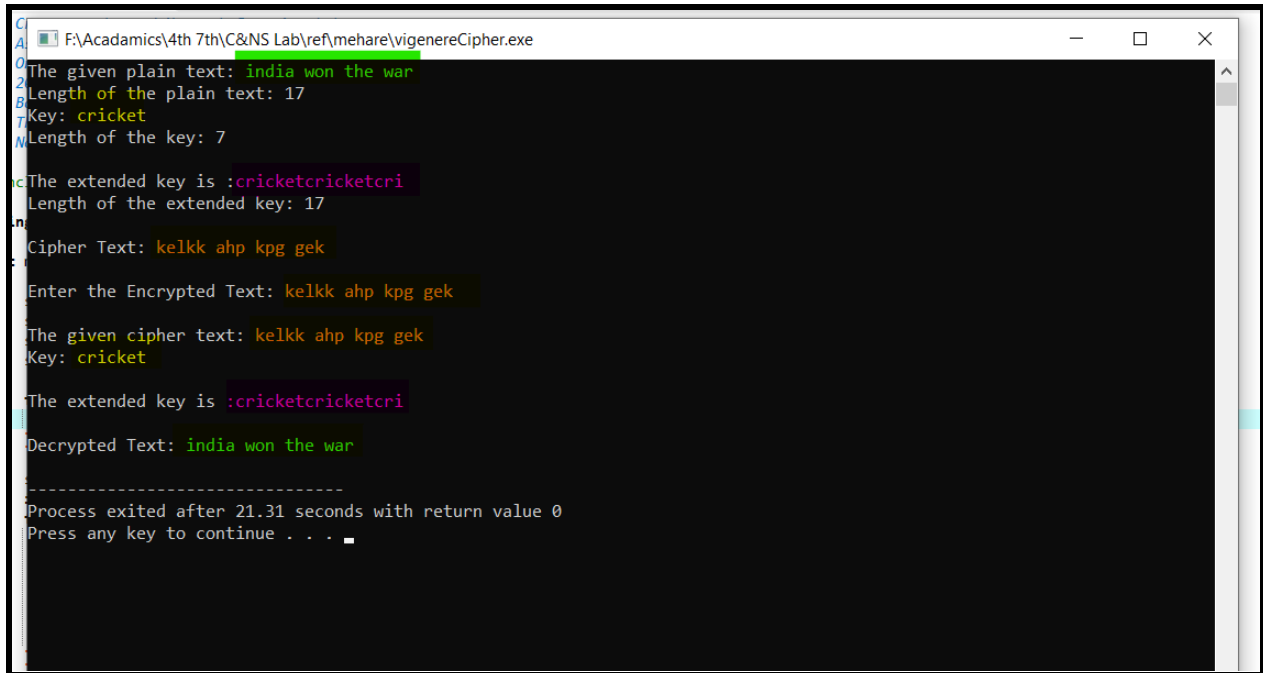
### Code

```
vigenereCipher.cpp ×
vigenereCipher.cpp
1 // Cryptography and Network Security Lab
2 // Assignment 3
3 // Onkar Gavali
4 // 2019BTECS00037
5 // Batch B2
6 // This programs demonstrates the vigenere cipher
7 // Note: Length of key in vigenere cipher should be Lesser than or equal to plain text
8
9 #include <iostream>
10
11 using namespace std;
12
13 int main() {
14     string plainText = "india won the war";
15     string key = "cricket";
16     size_t keyLength = key.size();
17     string extendedKey {};
18
19     for(size_t i = 0; i < plainText.size(); i++){
20         extendedKey += key[i%keyLength];
21     }
22
23     string cipherText{};
24     int j = 0;
```

```
26     for(size_t i = 0; i < plainText.size(); i++){
27         if(plainText[i] == ' '){
28             cipherText += ' ';
29         }else{
30             cipherText += (((plainText[i]-'a')+(extendedKey[j]-'a'))%26)+'a';
31             j++;
32         }
33     }
34
35     cout << "The given plain text: " << plainText << endl;
36     cout << "Length of the plain text: " << plainText.length() << endl;
37     cout << "Key: " << key << endl;
38     cout << "Length of the key: " << key.length() << endl;
39     cout << "\nThe extended key is : " << extendedKey << endl;
40     cout << "Length of the extended key: " << extendedKey.length() << endl;
41     cout << "\nCipher Text: " << cipherText << endl;
42
43     string encryptedText{};
44     string decryptedText{};
45     cout << "\nEnter the Encrypted Text: ";
46     getline(cin, encryptedText);
47
48     j = 0;
49     for(size_t i = 0; i < encryptedText.size(); i++){
50         if(encryptedText[i] == ' '){
```

```
51             decryptedText += ' ';
52         }else{
53             decryptedText += (((encryptedText[i] - 'a')-(extendedKey[j]-'a')+26)%26)+'a';
54             j++;
55         }
56     }
57
58     cout << "\nThe given cipher text: " << encryptedText << endl;
59     cout << "Key: " << key << endl;
60     cout << "\nThe extended key is : " << extendedKey << endl;
61     cout << "\nDecrypted Text: " << decryptedText << endl;
62
63     return 0;
64 }
```

## Output



```
F:\Academics\4th 7th\C&NS Lab\ref\mebare\vigenereCipher.exe
0 The given plain text: india won the war
2 Length of the plain text: 17
4 Key: cricket
6 Length of the key: 7
8 The extended key is :cricketcricketcri
10 Length of the extended key: 17
12 Cipher Text: kelkk ahp kpg gek
14 Enter the Encrypted Text: kelkk ahp kpg gek
16 The given cipher text: kelkk ahp kpg gek
18 Key: cricket
20 The extended key is :cricketcricketcri
22 Decrypted Text: india won the war
24 -----
26 Process exited after 21.31 seconds with return value 0
28 Press any key to continue . . .
```

## 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.