

Walchand College Of Engineering, Sangli
Department of Computer Science and Engineering
Subject: C&NS Lab

Batch: B4

Name: Gayatri Sopan Gade

PRN:2020BTECS00210

Assignment 4

Title: Implementation of Vigenere Cipher.

Introduction:

- 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 ceaser cipher.
- 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.

Encryption

The plaintext(P) and key(K) are added modulo 26.

$$E_i = (P_i + K_i) \bmod 26$$

Decryption

$$D_i = (E_i - K_i + 26) \bmod 26$$

Code Screenshot:

```
C:\Users\lenevo\Downloads\C&NS Assignments\C&NS Assignments\Experiment - 4\Vigenere.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
(globals)
Project Classes Debug [!] caesar.cpp cryptanalysis.cpp PlayFair.cpp Vigenere.cpp RailFence.cpp Columnar.cpp

1 #include<bits/stdc++.h>
2
3 using namespace std;
4 class Vigenere
5 {
6     public:
7     string key;
8     void createkey(string k) {
9         key.clear();
10        for (int i = 0; i < k.size(); ++i)
11        {
12            if (k[i] >= 'A' && k[i] <= 'Z')
13                key += k[i];
14            else if (k[i] >= 'a' && k[i] <= 'z')
15                key += k[i] + 'A' - 'a';
16        }
17    }
18    string encryption(string t)
19    {
20        string output;
21        for (int i = 0, j = 0; i < t.length(); ++i)
22        {
23            char c = t[i];
24            if(c == ' ')
25                continue;
26            if (c >= 'a' && c <= 'z')
27                c += 'A' - 'a';
28            else if (c < 'A' || c > 'Z')
29                continue;
30            output += (c + key[j] - 2 * 'A') % 26 + 'A';
31            //added 'A' to bring it in range of ASCII alphabet [ 65-90 | A-Z ]
32            j = (j + 1) % key.length();
33        }
34        return output;
35    }
36    string decryption(string t)
```

```
C:\Users\lenevo\Downloads\C&NS Assignments\C&NS Assignments\Experiment - 4\Vigenere.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
(globals)
Project Classes Debug [!] caesar.cpp cryptanalysis.cpp PlayFair.cpp Vigenere.cpp RailFence.cpp Columnar.cpp

31 //added 'A' to bring it in range of ASCII alphabet [ 65-90 | A-Z ]
32 j = (j + 1) % key.length();
33 }
34 return output;
35 }
36 string decryption(string t)
37 {
38     string output;
39     for (int i = 0, j = 0; i < t.length(); ++i)
40     {
41         char c = t[i];
42         if (c >= 'a' && c <= 'z')
43             c += 'A' - 'a';
44         else if (c < 'A' || c > 'Z')
45             continue;
46         output += (c - key[j] + 26) % 26 + 'A';
47         //added 'A' to bring it in range of ASCII alphabet [ 65-90 | A-Z ]
48         j = (j + 1) % key.length();
49     }
50     return output;
51 };
52 };
53
54 int main()
55 {
56     Vigenere v;
57
58     int choice;
59     int datachoice;
60     string sample,key;
61     int shift;
62     while(1)
63     {
64         cout << "Vigenere Cipher\n 1. Encryption \n 2. Decryption\n 3. Exit\nEnter Choice: ";
65         cin>>choice;
66         if(choice>2)
```

```
C:\Users\lenevo\Downloads\C&NS Assignments\C&NS Assignments\Experiment - 4\Vigenere.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
[globals]
Project Classes Debug [!] caesar.cpp cryptanalysis.cpp PlayFair.cpp Vigenere.cpp RailFence.cpp Columnar.cpp

114 cin.ignore();
115 getline(cin,sample);
116 cout<<"Enter the key: ";
117 getline(cin,key);
118 v.createkey(key);
119 cout<<"Decrypted String:\n";
120 cout<<v.decryption(sample)<<endl;;
121 }
122 else
123 {
124 cout<<"Enter File Name:\n";
125 cin.ignore();
126 getline(cin,sample);
127 cout<<"Enter the key: ";
128 getline(cin,key);
129 v.createkey(key);
130 fstream myfile;
131 myfile.open(sample.c_str());
132 string str,s;
133 if(!myfile.is_open())
134 cout << "Error while Opening File";
135 while(getline(myfile,str))
136 s+=str;
137 myfile.close();
138 s=v.decryption(s);
139 myfile.open("PlainText.txt",ios_base::out);
140 if(myfile.is_open())
141 myfile.write(s.data(),s.size());
142 cout<<"File Decrypted\n";
143 myfile.close();
144 }
145 break;
146 }
147 }
148 return 0;
149 }
```

Output:

```
C:\Users\lenevo\Downloads\C&NS Assignments\C&NS Assignments\Experiment - 4\Vigenere.exe
Vigenere Cipher
1. Encryption
2. Decryption
3. Exit
Enter Choice: 1
Data is from
1. Manual Entering
2. File
Enter Choice: 1
Enter data to be Encrypted:
Gayatri
Enter the key: good
Encrypted String:
MOMDZFW
Vigenere Cipher
1. Encryption
2. Decryption
3. Exit
Enter Choice: 2
Data is from
1. Manual Entering
2. File
Enter Choice: 1
Enter data to be Decrypted:
MOMDZFW
Enter the key: good
Decrypted String:
GAYATRI
Vigenere Cipher
1. Encryption
2. Decryption
3. Exit
Enter Choice:
```