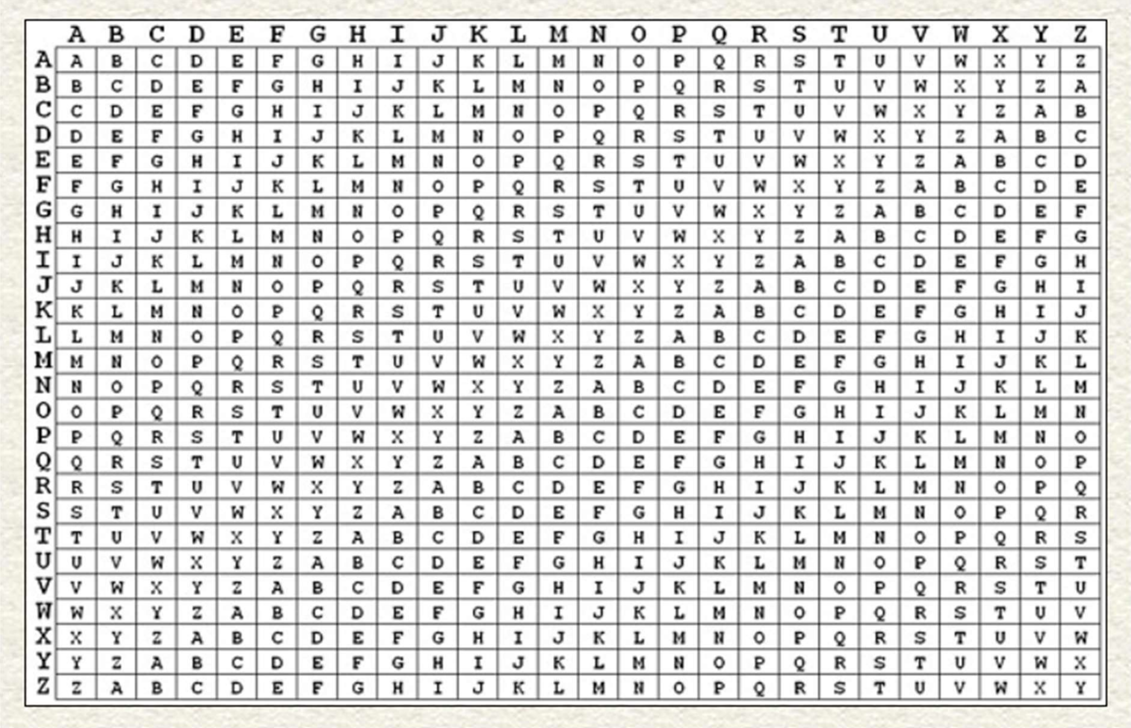
Final Year B. Tech, Sem VII 2022-23
PRN – 2020BTECS00211
Name – Aashita Narendra Gupta
Cryptography And Network Security Lab
Batch: B4

Practical No – 4

Title: To implement vigener cipher.

Theory:
The vigenere cipher is an algorithm that is used to encrypting and decrypting the text. The vigenere cipher is an algorithm of encrypting an alphabetic text that uses a series of interwoven caesar ciphers. It is based on a keyword's letters. It is an example of a polyalphabetic substitution cipher. This algorithm is easy to understand and implement. This algorithm was first described in 1553 by Giovan Battista Bellaso. It uses a Vigenere table or Vigenere square for encryption and decryption of the text. The vigenere table is also called the tabula recta.



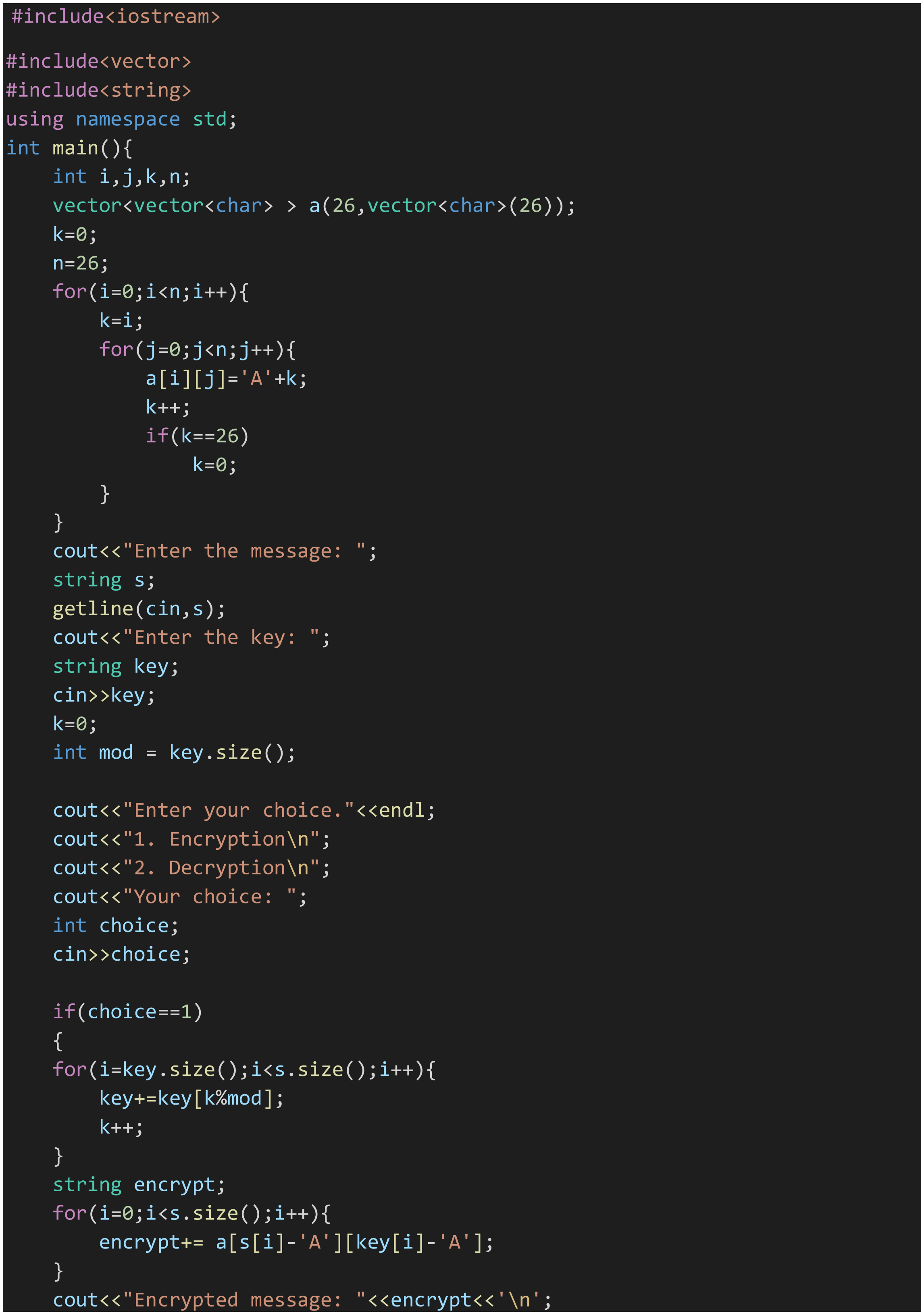
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Example:
Suppose the plaintext is COMMUNICATION and the keyword is COMPUTER.

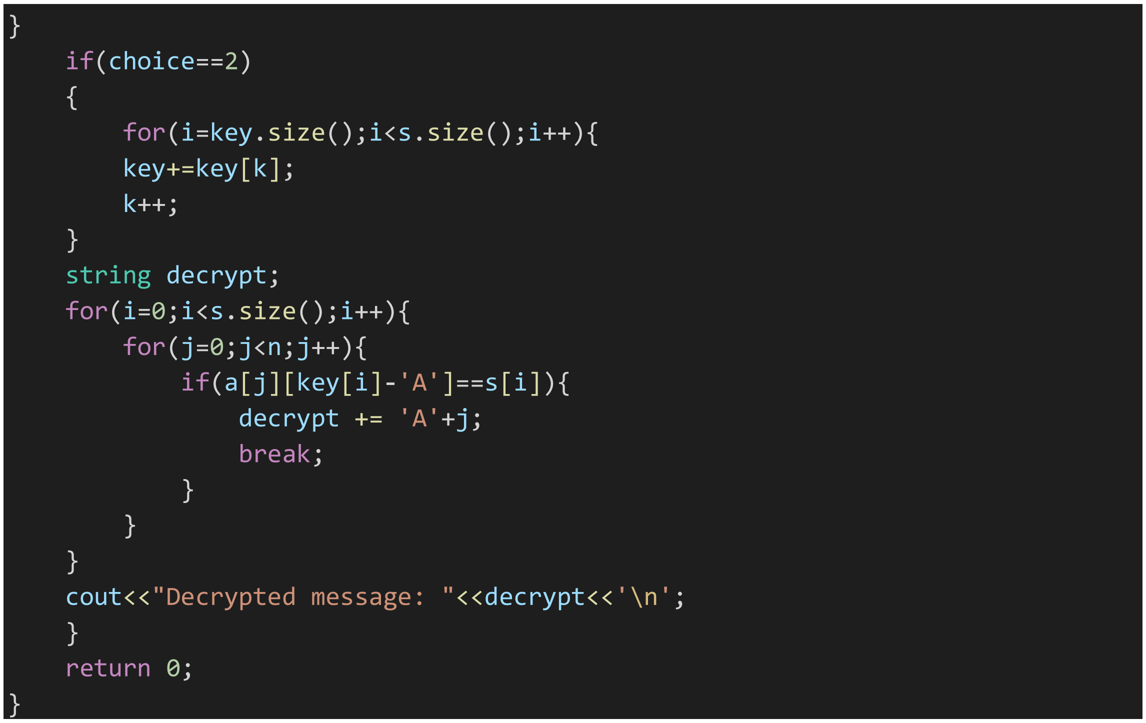
Encrypted text – ECYBOGMTCHUDH

Decrypted text - COMMUNICATION

Code Snapshots:



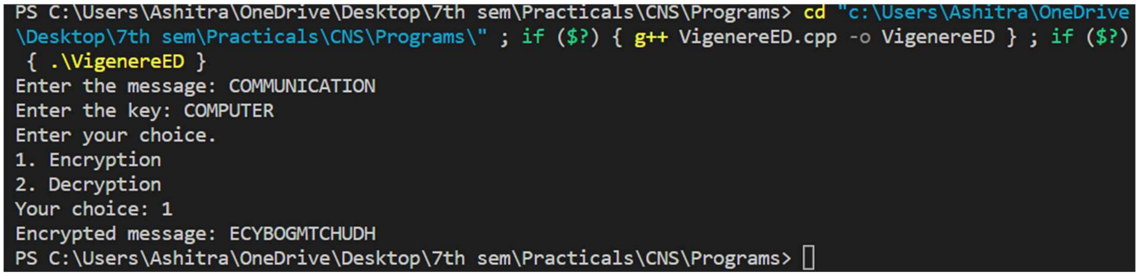
```
 #include<iostream>

#include<vector>
#include<string>
using namespace std;
int main(){
    int i,j,k,n;
    vector<vector<char> > a(26,vector<char>(26));
    k=0;
    n=26;
    for(i=0;i<n;i++){
        k=i;
        for(j=0;j<n;j++){
            a[i][j]='A'+k;
            k++;
            if(k==26)
                k=0;
        }
    }
    cout<<"Enter the message: ";
    string s;
    getline(cin,s);
    cout<<"Enter the key: ";
    string key;
    cin>>key;
    k=0;
    int mod = key.size();

    cout<<"Enter your choice."<<endl;
    cout<<"1. Encryption\n";
    cout<<"2. Decryption\n";
    cout<<"Your choice: ";
    int choice;
    cin>>choice;

    if(choice==1)
    {
    for(i=key.size();i<s.size();i++){
        key+=key[k%mod];
        k++;
    }
    string encrypt;
    for(i=0;i<s.size();i++){
        encrypt+= a[s[i]-'A'][key[i]-'A'];
    }
    cout<<"Encrypted message: "<<encrypt<<'\n';
```



```
}
    if(choice==2)
    {
        for(i=key.size();i<s.size();i++){
        key+=key[k];
        k++;
    }
    string decrypt;
    for(i=0;i<s.size();i++){
        for(j=0;j<n;j++){
            if(a[j][key[i]-'A']==s[i]){
                decrypt += 'A'+j;
                break;
            }
        }
    }
    cout<<"Decrypted message: "<<decrypt<<'\n';
    }
    return 0;
}
```

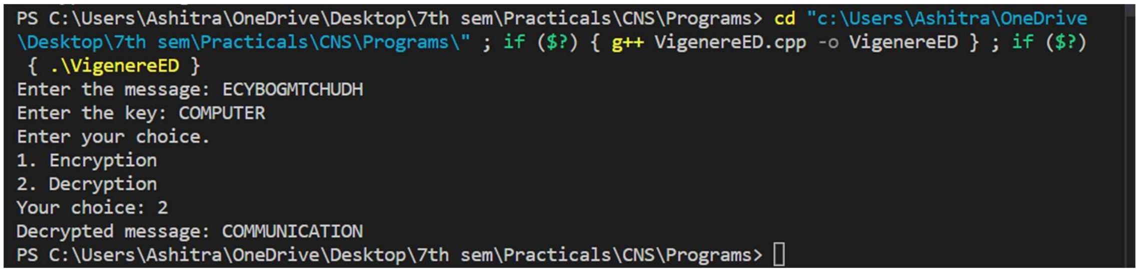
Output Snapshots:

Encryption:



```
PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs> cd "c:\Users\Ashitra\OneDrive
\Desktop\7th sem\Practicals\CNS\Programs\" ; if ($?) { g++ VigenereED.cpp -o VigenereED } ; if ($?)
 { .\VigenereED }
Enter the message: COMMUNICATION
Enter the key: COMPUTER
Enter your choice.
1. Encryption
2. Decryption
Your choice: 1
Encrypted message: ECYBOGMTCHUDH
PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs>
```

Decryption:



```
PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs> cd "c:\Users\Ashitra\OneDrive
\Desktop\7th sem\Practicals\CNS\Programs\" ; if ($?) { g++ VigenereED.cpp -o VigenereED } ; if ($?)
 { .\VigenereED }
Enter the message: ECYBOGMTCHUDH
Enter the key: COMPUTER
Enter your choice.
1. Encryption
2. Decryption
Your choice: 2
Decrypted message: COMMUNICATION
PS C:\Users\Ashitra\OneDrive\Desktop\7th sem\Practicals\CNS\Programs>
```

Conclusion:

1. Vigenere Cipher is a simple polyalphabetic substitution method that goes from a simple to advanced method.

2. The Vigenere Square or Table is an important tool used in this Cipher. You can use this cipher in three different ways as per your needs. All the three methods involve different steps.
3. The autokey method is the least secure method. Even though the keyword method has its vulnerabilities, it is more secure than the autokey method. The Python Code method is relatively the most secure method.