Final Year B. Tech., Sem VII 2022-23

Cryptography And Network Security

PRN: 2020BTECS00206

Full Name: SAYALI YOGESH DESAI

Batch: B4

Assignment No. 4

---

1. **Aim:**
   Encrypt the given plain text using Vigenere Cipher.

2. **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.
   - It uses a Vigenere table or Vigenere square for encryption and decryption of the text.

Two methods of Vigenere Cipher:

Method 1-

When the vigenere table is not given, the encryption and decryption are done by Vigenar algebraically formula in this method (convert the letters (A-Z) into the numbers (0-25)).

Formula of encryption is,

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

Formula of decryption is,

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

If any case (D_i) value becomes negative (-ve), in this case, we will add 26 in the negative value.

where,

E denotes the encryption.

D denotes the decryption.

P denotes the plaintext.

K denotes the key.

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Method 2-

When the vigenere table is given, the encryption and decryption are done using the vigenere table (26 * 26 matrix) in this method.

Plaintext

Key

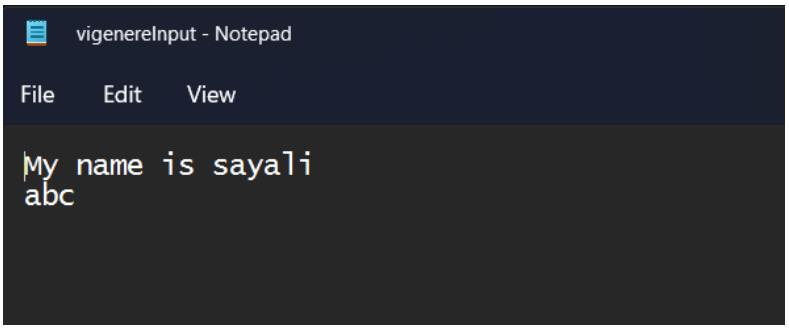
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

3. Code:

```
#include<bits/stdc++.h>
using namespace std;

// Capitalize the character
void capitalize(string &str){
    for(char &c:str){
      if(c>=97 && c<=122)
        c-=32;
    }
}

string encrypt(string &plainText,string &key){
   int n=key.size();
   int i=0;
   for(char &c:plainText){
       if(c>=65 && c<=90){
         int a=c-65;
         int b=key[i%n]-65;
         c=((a+b)%26+65);
         i++;
       }
   }
   return plainText;
}

string decrypt(string &cypherText,string &key){

   int n=key.size();
   int i=0;
   for(char &c:cypherText){
       if(c>=65 && c<=90){
         int a=c-65;
         int b=key[i%n]-65;
         c=(a-b+26)%26+65;
         i++;
       }
   }
   return cypherText;
}

int main(){

    freopen("vigenereInput.txt", "r", stdin);
```

```
    freopen("vigenereOutput.txt", "w", stdout);


    string key,plainText;
    getline(cin,plainText);

    // cout<<plainText<<endl;
    capitalize(plainText);
    getline(cin,key);
    capitalize(key);

    string CypherText=encrypt(plainText,key);
    cout<<"Cipher Text: "<<CypherText<<"\n\n";

    plainText=decrypt(CypherText,key);

    cout<<"Plain Text: "<<plainText<<endl;
    return  0;
}
```

4. Input:



5. Output: