**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.

1. **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,**

Ei = (Pi + Ki) mod 26

**Formula of decryption is,**

Di = (Ei - Ki) mod 26

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

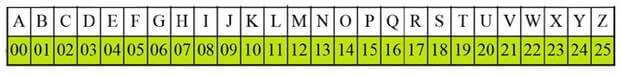
**where,**

E denotes the encryption.

D denotes the decryption.

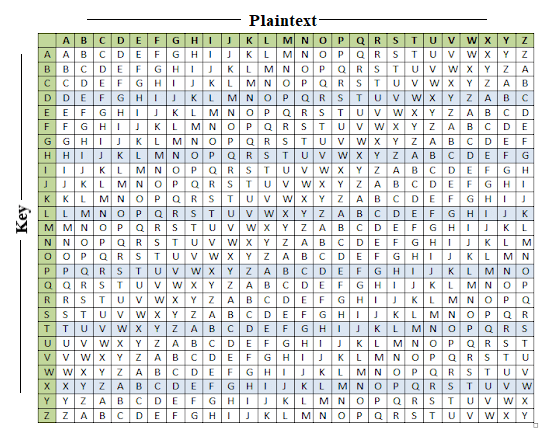
P denotes the plaintext.

K denotes the key.



**Method 2-**

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



1. **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";

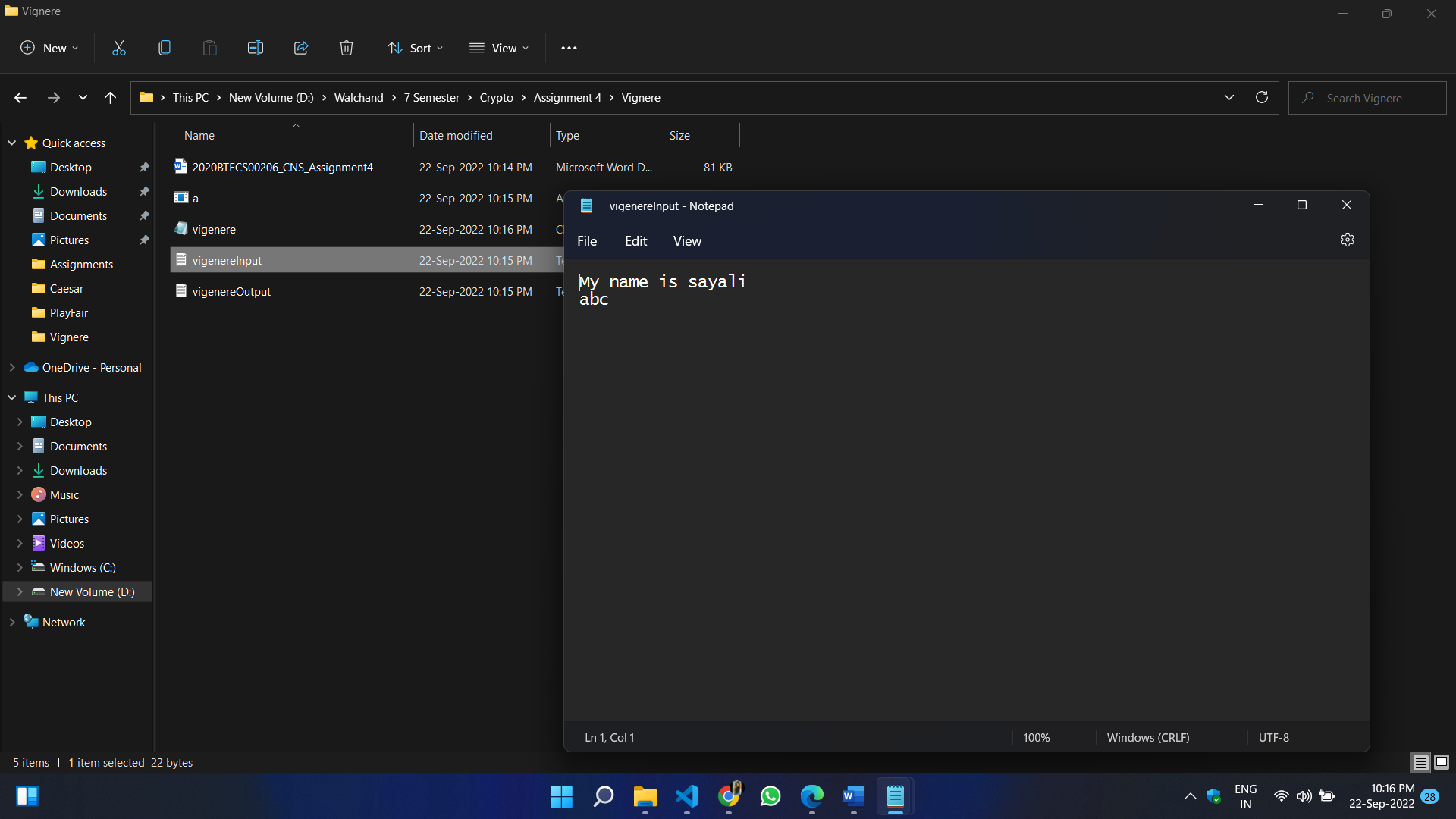
plainText=decrypt(CypherText,key);

cout<<"Plain Text: "<<plainText<<endl;

return 0;

}

1. **Input:**



1. **Output:**

