One Page Report Classical_Ciphers

CSE436, Computer and Networks Security

Name: Manal Ahmed Mahamed ID: 1601449

Date: 3 /2 /2021

This report consists of:

1) Code explanation

2) How to run the exe with screenshots provided for example

- **Code explanation**

1) Caesar Cipher :

This cipher uses 1 function which is `Caesar_Cipher(plaintext,key)` it takes the plaintext and the desired key and returns the encrypted message. The main operation is getting the order of the character then adding the key to this order (mod26 as we have 26 char) then getting the character of the new order.

2) Playfair Cipher:

This cipher uses 1 helper function `find_position(playfair_matrix,character)` it takes the playfair_matrix after creating it and the character which it will return its row and column numbers in the playfair_matrix.

The main function of it is `Play_Fair_Cipher(plaintext,keyword)` it takes the plaintext and the keyword first we create the playfair_matrix using the keyword, then we format the plaintext in the correct shape (adding x if it needs and so on) then we call the helper function and uses the row and column number of each 2 characters to get the new 2 characters

3) **Hell Cipher:**

This cipher uses 1 helper function `getKeyMatrix(key)`it takes the key as array of integers and return it in a matrix shape so we can multiply it with the characters matrix.

The min function of it is `Hill_Cipher(message,key)` it takes the plaintext and the key then it calls the helper function to get the key matrix, and format the message the split it to the correct shape 2x1 or 3x1 depends on the mode chosen, then it multiply the matrices to get the cipher text and return it

4) **Vigenere Cipher:**

This cipher 1 helper function `generateKey(string,key,mode)` which will return the key depending on the mode chosen (false for repeating, true for auto).

The main function of it is `Vigenere_Cipher(string,key,mode)` it calls the helper function first then it uses the order of the corresponding key character to the string character to get the cipher character then append them to get the cipher text

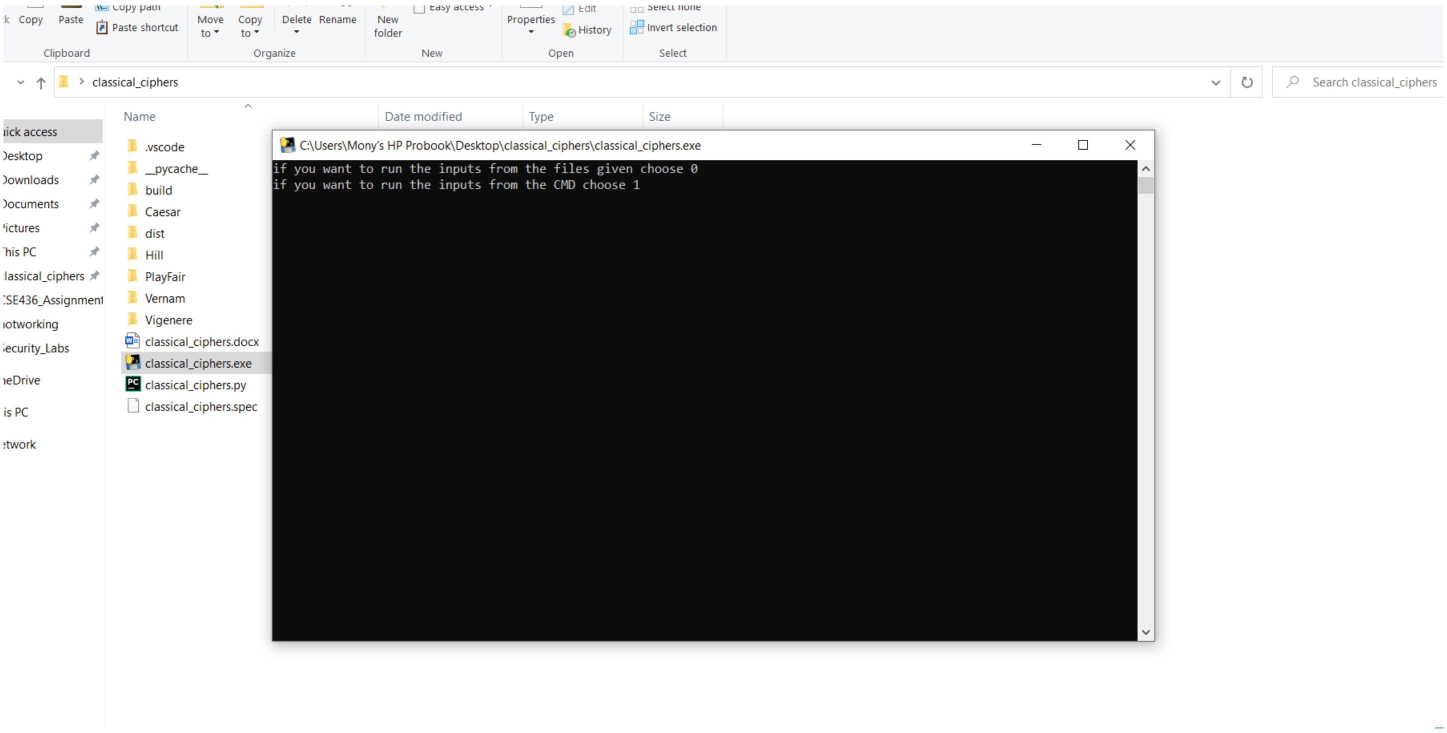
5) **Vernam Cipher:**

This cipher uses one function which is `Vernam_Cipher(plaintext,key)` which will use the order of the corresponding key character to the plaintext character to get the cipher character

- **How to run the exe with screenshots provided for example**

First of all we have 2 modes, 1 mode for the input to be taken from the files and you write the parameters for each cipher in the console, second mode is to take the input from the console, let's see the screenshot

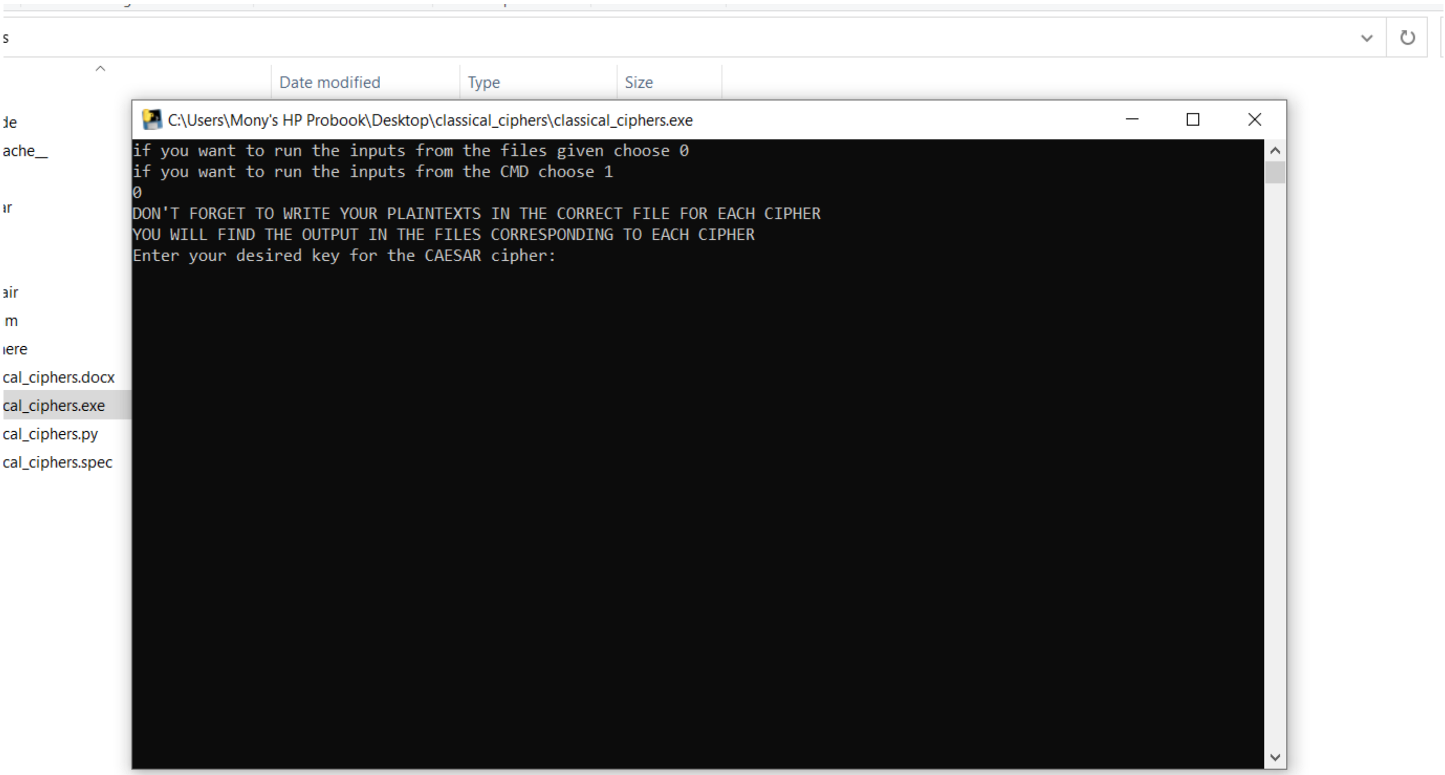
Running the classical_cipher.exe:



```
if you want to run the inputs from the files given choose 0
if you want to run the inputs from the CMD choose 1
```

Example1 (Input form the files)

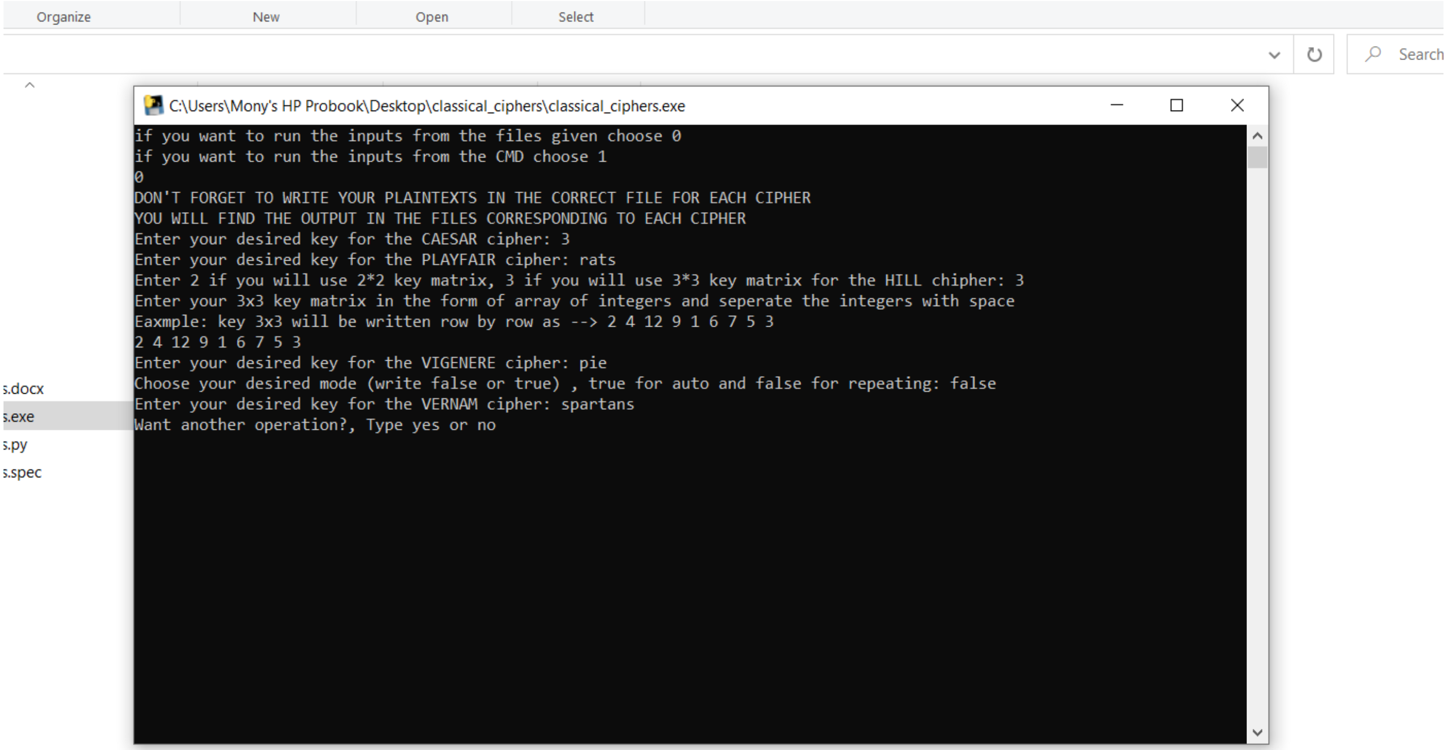
-First choose you desired mode, for example we choose 0


Date modified
Type
Size
C:\Users\Mony's HP Probook\Desktop\classical_ciphers\classical_ciphers.exe

```
if you want to run the inputs from the files given choose 0
if you want to run the inputs from the CMD choose 1
0
DON'T FORGET TO WRITE YOUR PLAINTEXTS IN THE CORRECT FILE FOR EACH CIPHER
YOU WILL FIND THE OUTPUT IN THE FILES CORRESPONDING TO EACH CIPHER
Enter your desired key for the CAESAR cipher:
```

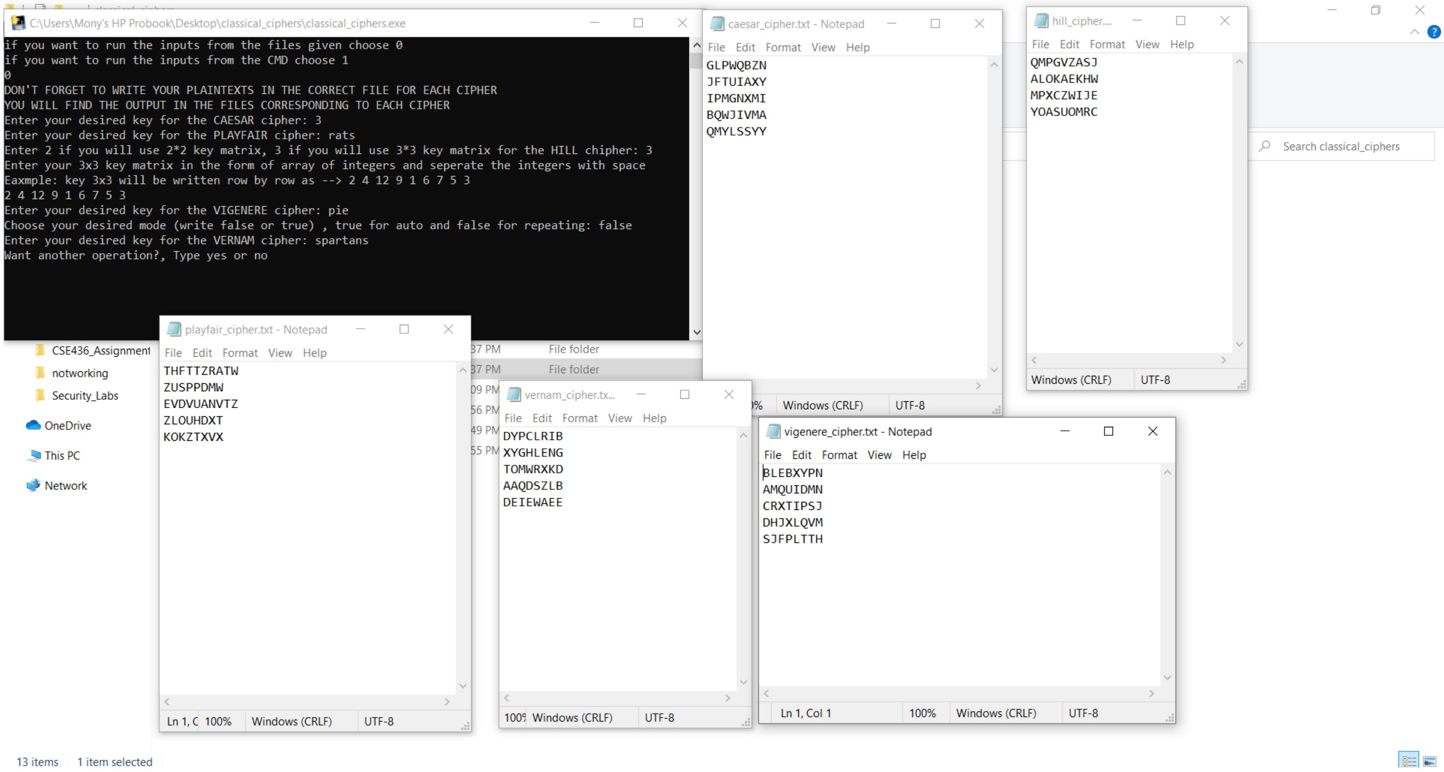
-you will be asked about all the keys and the parameters for all the ciphers, lets try the document example, the highlighted greens are the user inputs

Enter your desired key for the CAESAR cipher: 3
Enter your desired key for the PLAYFAIR cipher: rats
Enter 2 if you will use 2*2 key matrix, 3 if you will use 3*3 key matrix for the HILL chipher: 3
Enter your 3x3 key matrix in the form of array of integers and seperate the integers with space
Eaxmple: key 3x3 will be written row by row as --> 2 4 12 9 1 6 7 5 3
2 4 12 9 1 6 7 5 3
Enter your desired key for the VIGENERE cipher: pie
Choose your desired mode (write false or true) , true for auto and false for repeating: false
Enter your desired key for the VERNAM cipher: spartans


Organize
New
Open
Select
Search
s.docx
s.exe
s.py
s.spec
C:\Users\Mony's HP Probook\Desktop\classical_ciphers\classical_ciphers.exe

```
if you want to run the inputs from the files given choose 0
if you want to run the inputs from the CMD choose 1
0
DON'T FORGET TO WRITE YOUR PLAINTEXTS IN THE CORRECT FILE FOR EACH CIPHER
YOU WILL FIND THE OUTPUT IN THE FILES CORRESPONDING TO EACH CIPHER
Enter your desired key for the CAESAR cipher: 3
Enter your desired key for the PLAYFAIR cipher: rats
Enter 2 if you will use 2*2 key matrix, 3 if you will use 3*3 key matrix for the HILL chipher: 3
Enter your 3x3 key matrix in the form of array of integers and seperate the integers with space
Eaxmple: key 3x3 will be written row by row as --> 2 4 12 9 1 6 7 5 3
2 4 12 9 1 6 7 5 3
Enter your desired key for the VIGENERE cipher: pie
Choose your desired mode (write false or true) , true for auto and false for repeating: false
Enter your desired key for the VERNAM cipher: spartans
Want another operation?, Type yes or no
```

-the output will be in the files, let's see them:



```
if you want to run the inputs from the files given choose 0
if you want to run the inputs from the CMD choose 1
0
DON'T FORGET TO WRITE YOUR PLAINTEXTS IN THE CORRECT FILE FOR EACH CIPHER
YOU WILL FIND THE OUTPUT IN THE FILES CORRESPONDING TO EACH CIPHER
Enter your desired key for the CAESAR cipher: 3
Enter your desired key for the PLAYFAIR cipher: rats
Enter 2 if you will use 2*2 key matrix, 3 if you will use 3*3 key matrix for the HILL chipher: 3
Enter your 3x3 key matrix in the form of array of integers and seperate the integers with space
Eaxmple: key 3x3 will be written row by row as --> 2 4 12 9 1 6 7 5 3
2 4 12 9 1 6 7 5 3
Enter your desired key for the VIGENERE cipher: pie
Choose your desired mode (write false or true) , true for auto and false for repeating: false
Enter your desired key for the VERNAM cipher: spartans
Want another operation?, Type yes or no
```

caesar_cipher.txt

```
GLPWQBZN
JFTUIAXY
IPMGNXMI
BQWJIVMA
QMYLSSYY
```

hill_cipher

```
QMPGVZASJ
ALOKAEKHW
MPXCZWIJE
YOASUOMRC
```

playfair_cipher.txt

```
THFTTZRATW
ZUSPPDMW
EVDVUANVTZ
ZLOUHDXT
KOKZTXVX
```

vernam_cipher

```
DYPCLRIB
XYGHLENG
TOMWRXKD
AAQDSZLB
DEIEWAEE
```

vigenere_cipher.txt

```
BLEBXYPN
AMQUIDMN
CRXTIPSJ
DHJXLQVM
SJFPLTTH
```

Then you are asked if you want another operation, let's try the console input example:

- **Example2 (Input plaintext form the console):**

  -First type yes

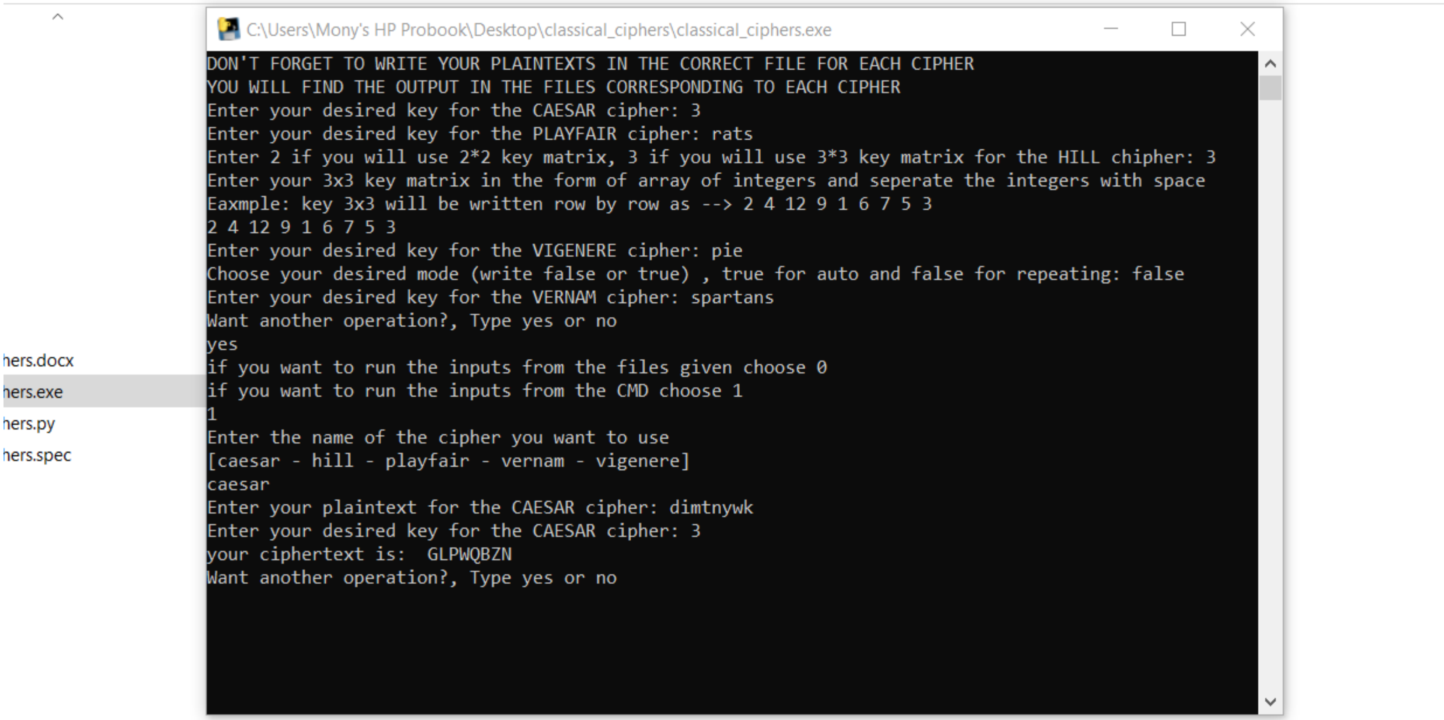
  -then type 1 to take the input from console

  -enter the name of the cipher you want to use, for example Caesar

  -enter the plaintext you want to encrypt, for example dimtnywk

  -enter the key you want, for example 3

  -the output cipher text will be printed for you in the console


C:\Users\Mony's HP Probook\Desktop\classical_ciphers\classical_ciphers.exe
hers.docx
hers.exe
hers.py
hers.spec

```
DON'T FORGET TO WRITE YOUR PLAINTEXTS IN THE CORRECT FILE FOR EACH CIPHER
YOU WILL FIND THE OUTPUT IN THE FILES CORRESPONDING TO EACH CIPHER
Enter your desired key for the CAESAR cipher: 3
Enter your desired key for the PLAYFAIR cipher: rats
Enter 2 if you will use 2*2 key matrix, 3 if you will use 3*3 key matrix for the HILL chipher: 3
Enter your 3x3 key matrix in the form of array of integers and seperate the integers with space
Eaxmple: key 3x3 will be written row by row as --> 2 4 12 9 1 6 7 5 3
2 4 12 9 1 6 7 5 3
Enter your desired key for the VIGENERE cipher: pie
Choose your desired mode (write false or true) , true for auto and false for repeating: false
Enter your desired key for the VERNAM cipher: spartans
Want another operation?, Type yes or no
yes
if you want to run the inputs from the files given choose 0
if you want to run the inputs from the CMD choose 1
1
Enter the name of the cipher you want to use
[caesar - hill - playfair - vernam - vigenere]
caesar
Enter your plaintext for the CAESAR cipher: dimtnywk
Enter your desired key for the CAESAR cipher: 3
your ciphertext is:  GLPWQBZN
Want another operation?, Type yes or no
```

-if you want another operation type yes and it will repeat asking you about the mode of input and so on, if you do not want another operation type no and the exe will close