Assignment Answer

CSExxx, Course Name

Name: Hala Mohamed Ahmed ID: 1601655

Assignment No: (1)

Date: 3 / 2 /2021

Classical ciphers Implementation functions:

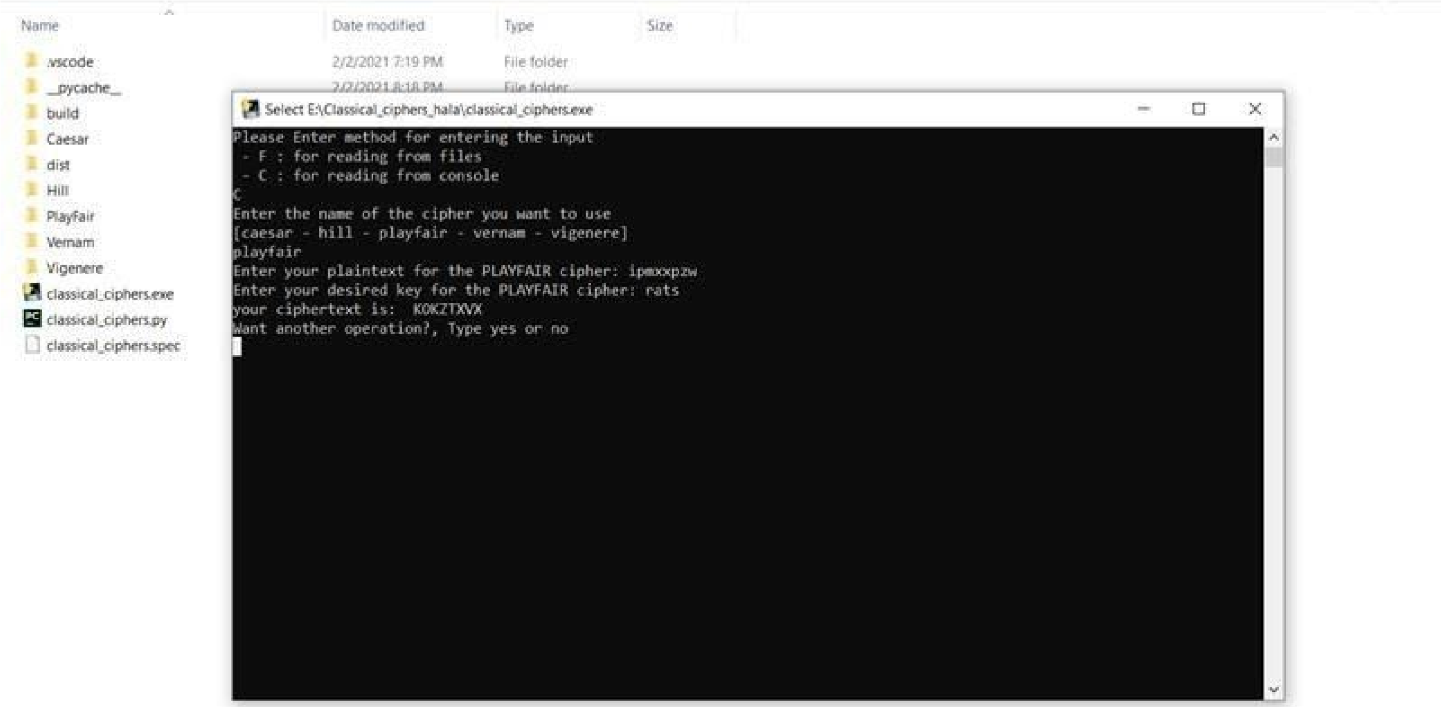
- **Caesar_Cipher(plaintext,key):** Caesar_Cipher Function :
  input : plaintext,key
  output : ciphertext after applying the algorithm
  explanation : The main operation is getting the order of the character then adding the key to this order(mod26 as we have 26 char) then getting the character of the new order.
- **find_position(playfair_matrix,character):**
  input : playfair_matrix,character
  output : the row and column numbers of the character given
  explanation : helper function for the playfair cipher
- **Play_Fair_Cipher(plaintext,keyword):**
  input : plaintext,keyword
  output : the ciphertext after applying the algorithm
  explanation : 1.The Algorithm consistes of 2 steps:
  Generate the key Square(5×5)
  2.Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters.
  If there is an odd number of letters, a X is added to the last letter.
- **getKeyMatrix(key):**
  input : key as an array of integers
  output : returns the key in the matrix form
  explanation : helper function for the hill cipher algorithm, it does reshaping of the key depending on the length of the key
- **Hill_Cipher(message, K):**
  input : message,K
  output : the ciphertext after applying the algorithm
  explanation : To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26.
  The matrix used for encryption is the cipher key.

- **generateKey(string,key,mode):**
  input : string,key,mode
  output : the correct key depending on the mode and the size of the message
  explanation : there is 2 modes in generating the key in vigenere cipher, if the key size equal to the message size there is no need for this function, auto key mode repeates the key until its the same size of the message ,while repeating mode appends the message to the key until the key is the same size as the message
- **Vigenere_Cipher(string, key,mode):**
  input : string,key,mode
  output : the ciphertext after applying the algorithm
  explanation : it is the same as the caesar Cipher but it uses different moves for each character depending on the character corresponding to it in the key.
- **Vernam_Cipher(plaintext, key):**
  input : plaintext,key,key
  output : the ciphertext after applying the algorithm
  explanation : Assign a number to each character of the plain-text and the key according to alphabetical order. Add both the number (Corresponding plain-text character number and Key character number). Subtract the number from 26 if the added number is greater than 26, if it isn’t then leave it.
- **main_files():**
  this function to take the input in a text file and the output will also be in a text file.
- **main_console_input():**
  this function to take the input text from the console and the output cipher text will be in the console.
- **main():**
  this function asks the user about the method of entering the input text.

Examples:

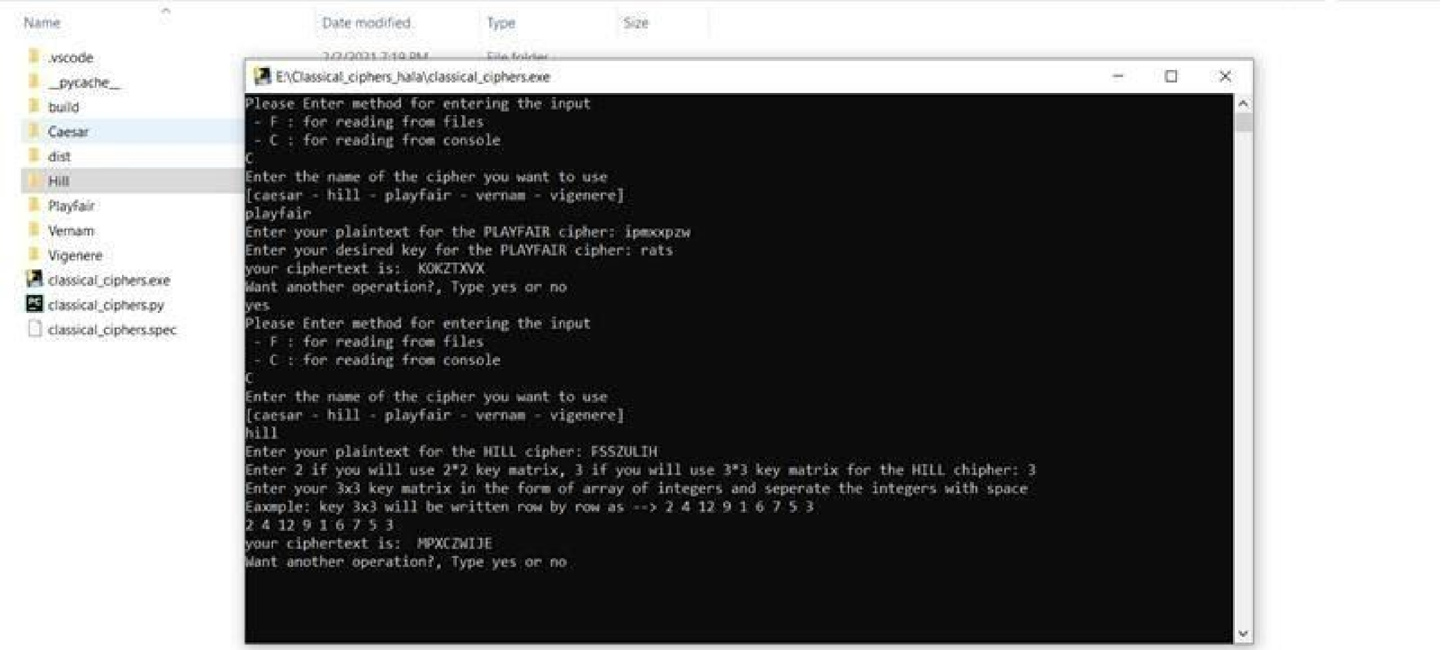
1. reading from the console:

- Play fair cipher



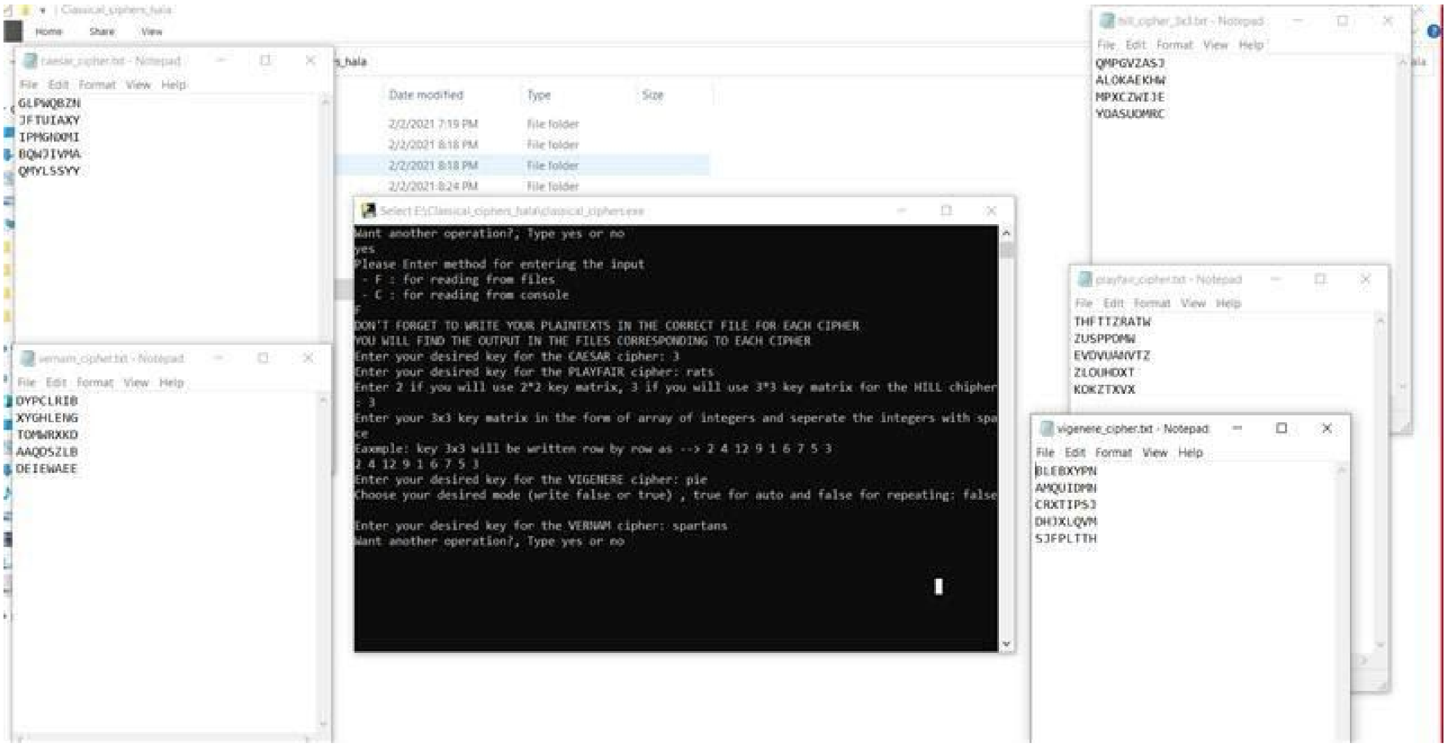
```
Please Enter method for entering the input
 - F : for reading from files
 - C : for reading from console
C
Enter the name of the cipher you want to use
[caesar - hill - playfair - vernam - vigenere]
playfair
Enter your plaintext for the PLAYFAIR cipher: ipmxxpzw
Enter your desired key for the PLAYFAIR cipher: rats
your ciphertext is:  KOKZTXVX
Want another operation?, Type yes or no
```

- Hill cipher With matrix (3 x 3)



```
Please Enter method for entering the input
 - F : for reading from files
 - C : for reading from console
C
Enter the name of the cipher you want to use
[caesar - hill - playfair - vernam - vigenere]
playfair
Enter your plaintext for the PLAYFAIR cipher: ipmxxpzw
Enter your desired key for the PLAYFAIR cipher: rats
your ciphertext is:  KOKZTXVX
Want another operation?, Type yes or no
yes
Please Enter method for entering the input
 - F : for reading from files
 - C : for reading from console
C
Enter the name of the cipher you want to use
[caesar - hill - playfair - vernam - vigenere]
hill
Enter your plaintext for the HILL cipher: FSSZULIH
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
your ciphertext is:  MPXCZWIJE
Want another operation?, Type yes or no
```

2. Reading from text files:


Classical_ciphers_hala
Home
Share
View
caesar_cipher.txt - Notepad
vernam_cipher.txt - Notepad
hill_cipher_3x3.txt - Notepad
playfair_cipher.txt - Notepad
vigenere_cipher.txt - Notepad
File Edit Format View Help
Date modified
Type
Size
2/2/2021 7:19 PM
2/2/2021 8:18 PM
2/2/2021 8:18 PM
2/2/2021 8:24 PM
File folder
Select E:\Classical_ciphers_hala\classical_ciphers.exe

```
GLPWQBZN
JFTUIAXY
IPMGHXMI
BQWJIVMA
QMYLSSYY
```

```
DYPCLRIB
XYGHLENG
TOMWRXKD
AAQDSZLB
DEIEWAEE
```

```
Want another operation?, Type yes or no
yes
Please Enter method for entering the input
 - F : for reading from files
 - C : for reading from console
F
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 spa
ce
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
```

```
QMPGVZASJ
ALOKAEKHW
MPXCZWIJE
YOASUOMRC
```

```
THFTTZRATW
ZUSPPOMW
EVDVUAHVTZ
ZLOUHDXT
KOKZTXVX
```

```
BLEBXYPN
AMQUIDMN
CRXTIPSJ
DHJXLQVM
SJFPLTTH
```