December 7, 2021

Mohammad Shahin

[Company name]

Lebanese American university

Encryption and Decryption

Csc243 project

Table of Contents

[Introduction: 2](#_Toc89770804)

[The meaning of encryption, decryption and its history: 2](#_Toc89770805)

[General History: 2](#_Toc89770806)

[Playfair cipher: 3](#_Toc89770807)

[Ceaser cipher: 3](#_Toc89770808)

[The code: 4](#_Toc89770809)

[Main: 4](#_Toc89770810)

[Ceaser function: 5](#_Toc89770811)

[Playfair function: 6](#_Toc89770812)

[Index finder: 6](#_Toc89770813)

[File reader with doubles and evens: 6](#_Toc89770814)

[Matrix: 6](#_Toc89770815)

[Letter replacer: 7](#_Toc89770816)

[When decrypting: 7](#_Toc89770817)

[Closing the files: 7](#_Toc89770818)

[Counting function: 8](#_Toc89770819)

[Flow chart: 8](#_Toc89770820)

[Bibliography: 9](#_Toc89770821)

[Appendix: 9](#_Toc89770822)

# Introduction:

## The meaning of encryption, decryption and its history:

When we encrypt a text, we turn it from an understandable text with meaning (plaintext/original) into a meaningless set of letters and signs (cipher text).

On the other hand, decrypting is turning a set of letters and signs back from being meaningless (ciphered) into a meaningful message that the user can understand (deciphered), which is the complete copy of the original text.

## General History:

First appearance

To start the first evidence of the use of cryptography was found in an inscription carved at ≈1900 BC, in the chamber of a tomb of a nobleman, in Egypt. The scribe used some unfamiliar hieroglyphic symbols in place of more ordinary ones. The purpose was not to hide the message, but to change its shape and meaning making the script not understandable unless the returned to its true form. Although the inscription was different, it incorporated some sort of transformation from the original text.

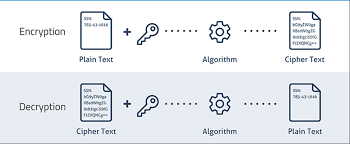
Evidence of some use of encryption and decryption (cryptography) appeared in most major ancient civilizations. For instance, the “Arthshashtra”, a classic work on statecraft written by Kautilya, describes the espionage service in India and mentions giving assignments to spies in “secret writing”.

In the world war

“During the first two years of [World War I](https://www.britannica.com/event/World-War-I), [code](https://www.britannica.com/topic/code-communications) systems were used for high-command and diplomatic communications, just as they had been for centuries, and [cipher](https://www.britannica.com/topic/cipher) systems were used almost exclusively for tactical communications. Field cipher systems such as the U.S. [Signal Corps’s](https://www.britannica.com/topic/Signal-Corps) cipher disk mentioned above, lacked sophistication (and security), however. Nevertheless, by the end of the war some complicated cipher systems were used for high-level communications, the most famous of which was the German ADFGVX fractionation cipher, described in the section [Cryptography: Product ciphers](https://www.britannica.com/topic/cryptology/Product-ciphers#ref25629)” (Simmons, 2016).

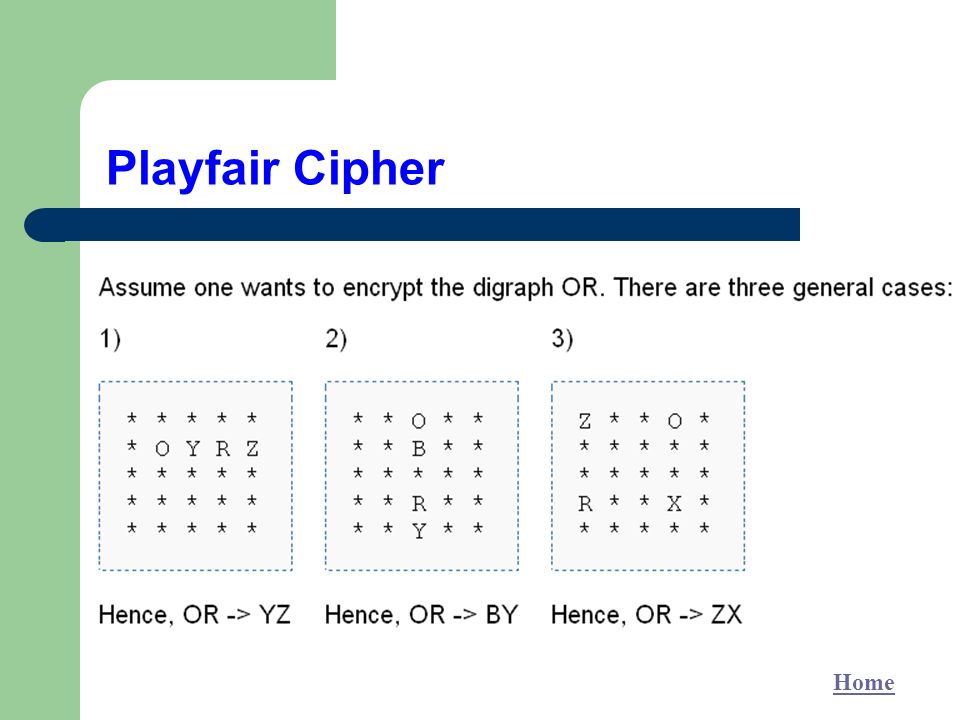
Modern use

In modern day, cryptography is widely used in banks, messaging apps such as (WhatsApp) were text and messages are all end to end encrypted.



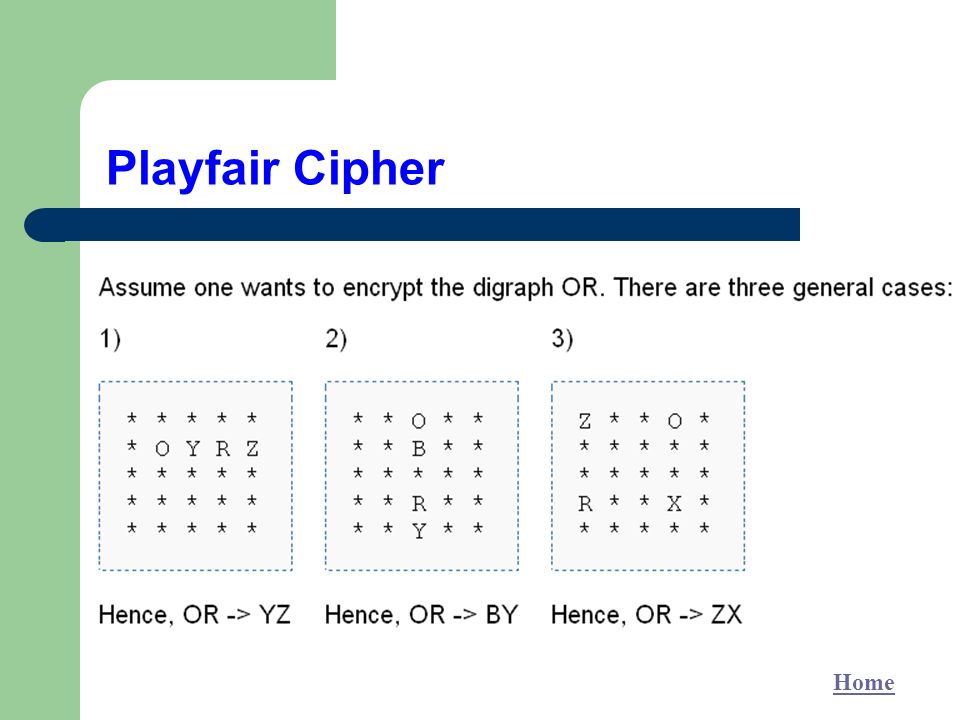
## Data Compression and Security - ppt video online downloadPlayfair cipher:

The playfair is based on three scenarios were each pair of letters meet in a 5\*5 Metrix/box were the letter are placed according to a keyword.



## Ceaser cipher:

The ceaser is a simple shift in the order of the letters were each a character jumps place according to the value placed by the user



# The code:

## Main:

The main code is used to call the other functions defined below according to the user input.

To further explain the main function start with a large while loop that will keep the code running until the user decides to turn it off either manually or by deciding to not continue in the last question. Furthermore, the main function is used to determine from the user if he wants:

1- Use an old file or create a new one

2- If he wants to decrypt, encrypt or count

3- In case the user choses to encrypt or decrypt. The user will be presented with the choice with following cipher languages: Ceaser, playfair, joined.

\* A while loop is created after each needed input to assure that the input is valid and ask the user to reenter their choice otherwise.

According to each choice the user will be presented with further question to input for instance if he chose to use an old file he will be asked to insert its name. While if he chose to create a new one the user will be asked to insert the new input “text” he wants to include in the file.

According to the cipher language he chooses the user will be

## Ceaser function:

Variables that must be inputted for the function:

1) A filename to read from, 2)a file to save the output, 3)an integer value to determine the shift 4) a statement of true or false to determine if the code used is a joined one.

The following code defines the first cipher language “Ceaser” the code start with opening the allocated “filename” file as r “read” in a new variable named “f”. Then a new variable is also introduced named “answer” in which the “wheresave” file is opened as w “write” to save the new output. Finally an empty string is introduced.

The major part of the function starts with a for loop where “I” moves across the lines in the file where the split function is used to cut the line into words under a variable named x and a new variable is introduce called “n” and it is used to count the number of words in each line to be able to jump a line in the right location. Then a nested loop is introduced to move across each word in a line under the variable “j”. Furthermore, the variable “n” is increased by a value of 1, and a new variable “m” with a value of zero, then a space is inserted into the string to separate each word from the other. Moreover, another nested for loop is used to move across each letter in a word where the current letter is called by variable “z” at this instance the letter is shifted based on an if statement regarding if it is an upper case or a lower case .

An if statement is now introduced which states: If the letter was an upper case then the num (the shift, which was inputted by the user) is either added or subtracted from the value “65” which stands for the ordinal “ord” of the first letter “A” then the shift is divide by 26 which is the amount of letters in the English alphabet. After all of that the shift is determined and is added to the ordinal of the letter allocated by the nested loop /variable “z” which is then added to the ordinal of the first letter “A”. Finally the resulting number is transformed into a letter through using the “chr” function to be introduced as the new letter in the variable “Q”.

\*In the case of lower case letters the process is repeated. However, instead of using the value 65 it is replaced by 97 which is the ordinal of “a”.

After this the letter is added/inserted into the string (string+=Q) and the value of variable “m” is increased by 1 to count the number of letters in a word. Afterwards another if statement is used which states that if the value of variable “n” which stands for the number of word in a line equales the “len” function of variable “x” and if the value of variable “m” which stands for the number of letters in a word equal the function “len” of variable “j” then the code will insert a line skip/space (\n) into the string.

At this point the changes in the function output have ended. However, what is left is how function will present the output and that depends on the user input on what process was used is it (encryption or decryption) and if it is a single or joined use of cipher language.

Finally the files are closed and the function returns the new file associated with the “answer” variable.

## Playfair function:

### Index finder:

The index finder is used to move around the matrix with ease by determine the column and row of each letter

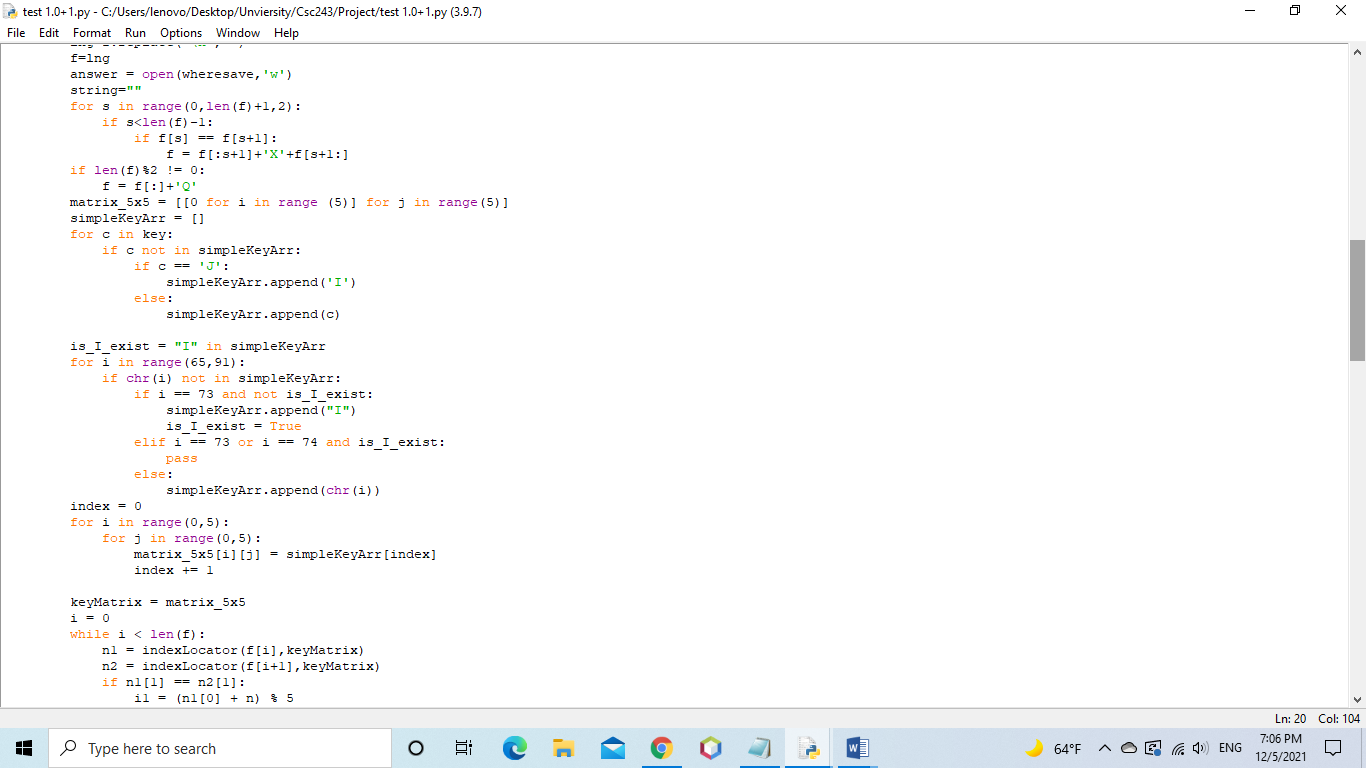
### File reader with doubles and evens:

The letter j is removed from the alphabet and replaced by the letter I,

And “X” is placed between all double letters for example “hello” would become “helxlo”

A “Q” is added at the end of any odd numbered sentence to turn it into an even one

### Matrix:

This part is used to create the alphabet matrix which is based on 25 letters as we will remove the letter “J” to create an equal square.

The matrix will move in alphabetical order after starting with the keyword inputted by the user as long as the letter is not found in the keyword itself

### Letter replacer:

The following is used to replace the letters according to the three situation of playfair (vertically associated, horizontally associated, and box like transfer).

Every 2 letters are taken togather

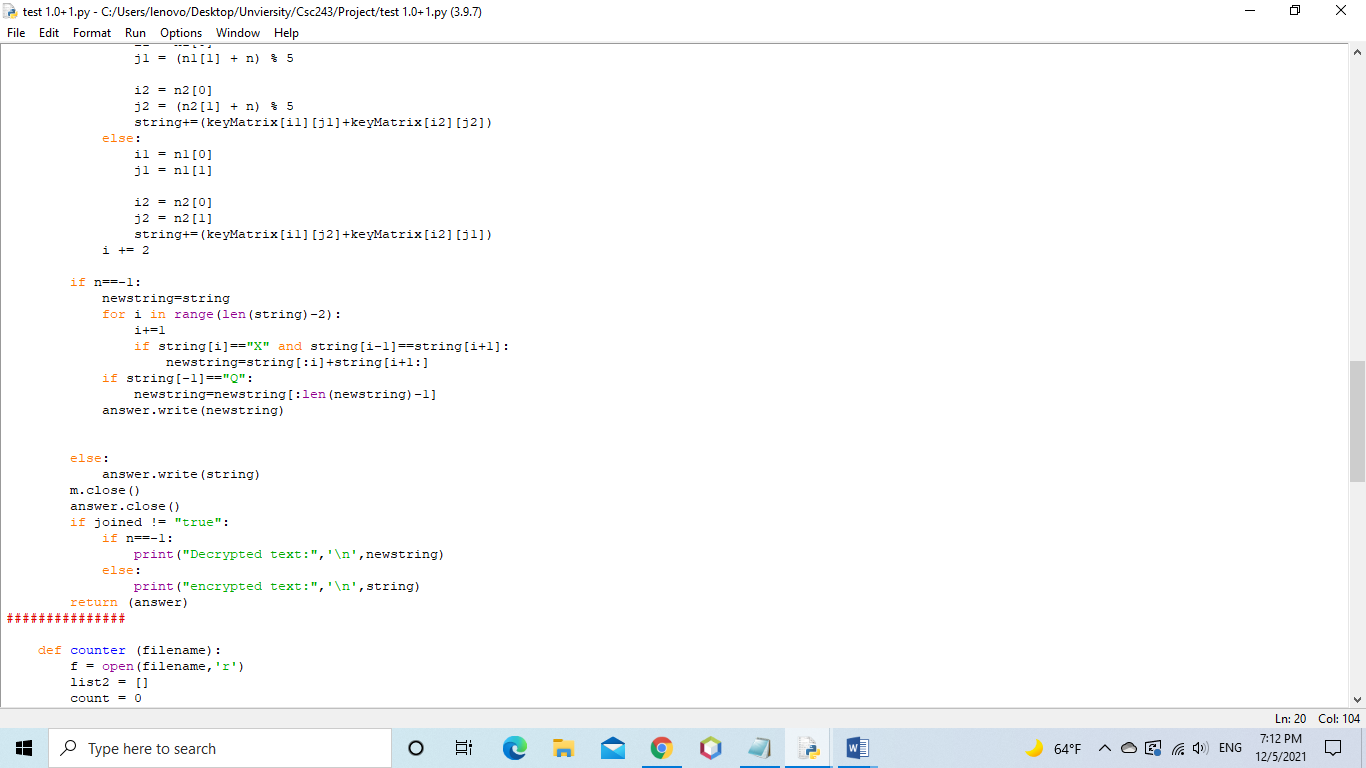
n1 stands for the first letter while n2 stands for the second letter

the value is divided by 5 as the matrix is created by 25 letters to create a 5\*5 square which makes it possible for the code to move across the matrix with ease .

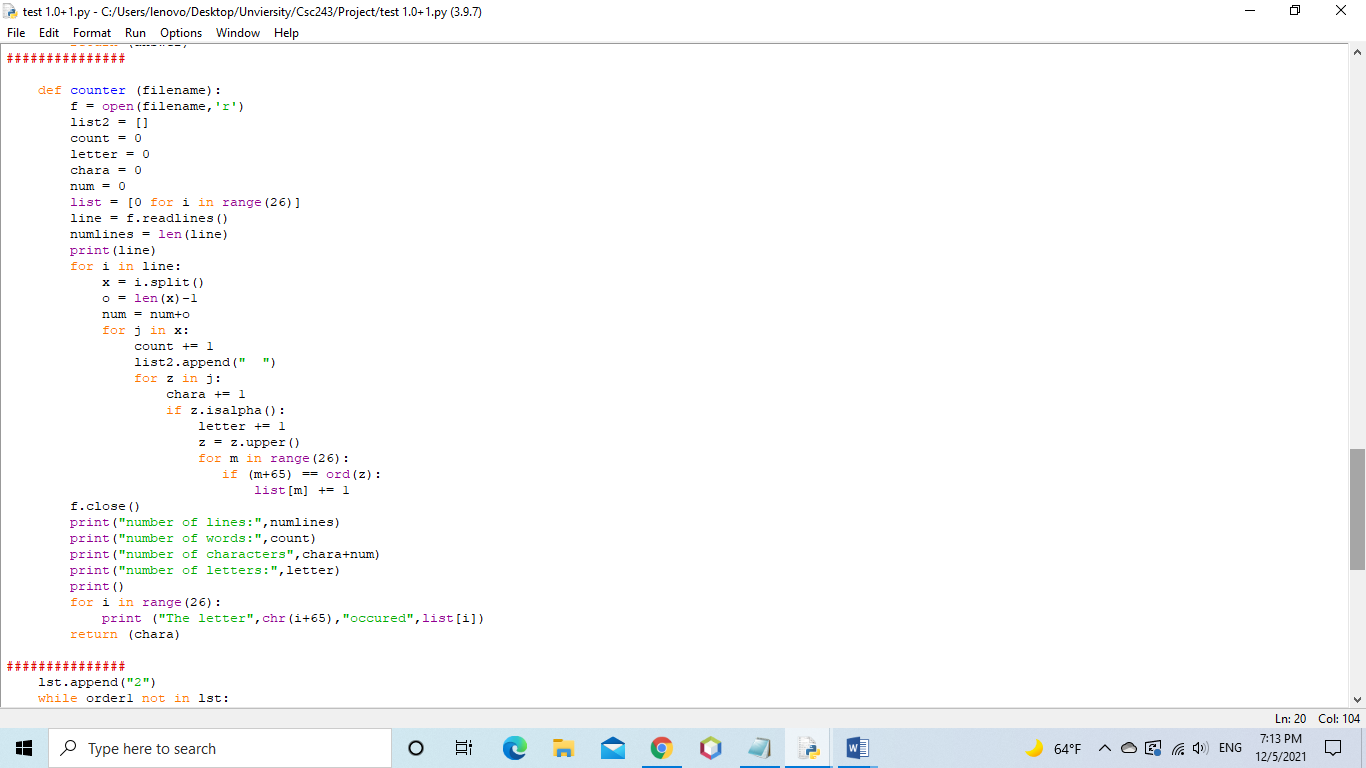
### When decrypting:

Removing the added X and Q ,

### Closing the files:

This part is used in the Playfair function to save the output in the file associated with the variable “answer”. Then the files are closed and the output is printed according to the user previous input regarding (the encryption, and decryption) and if the language

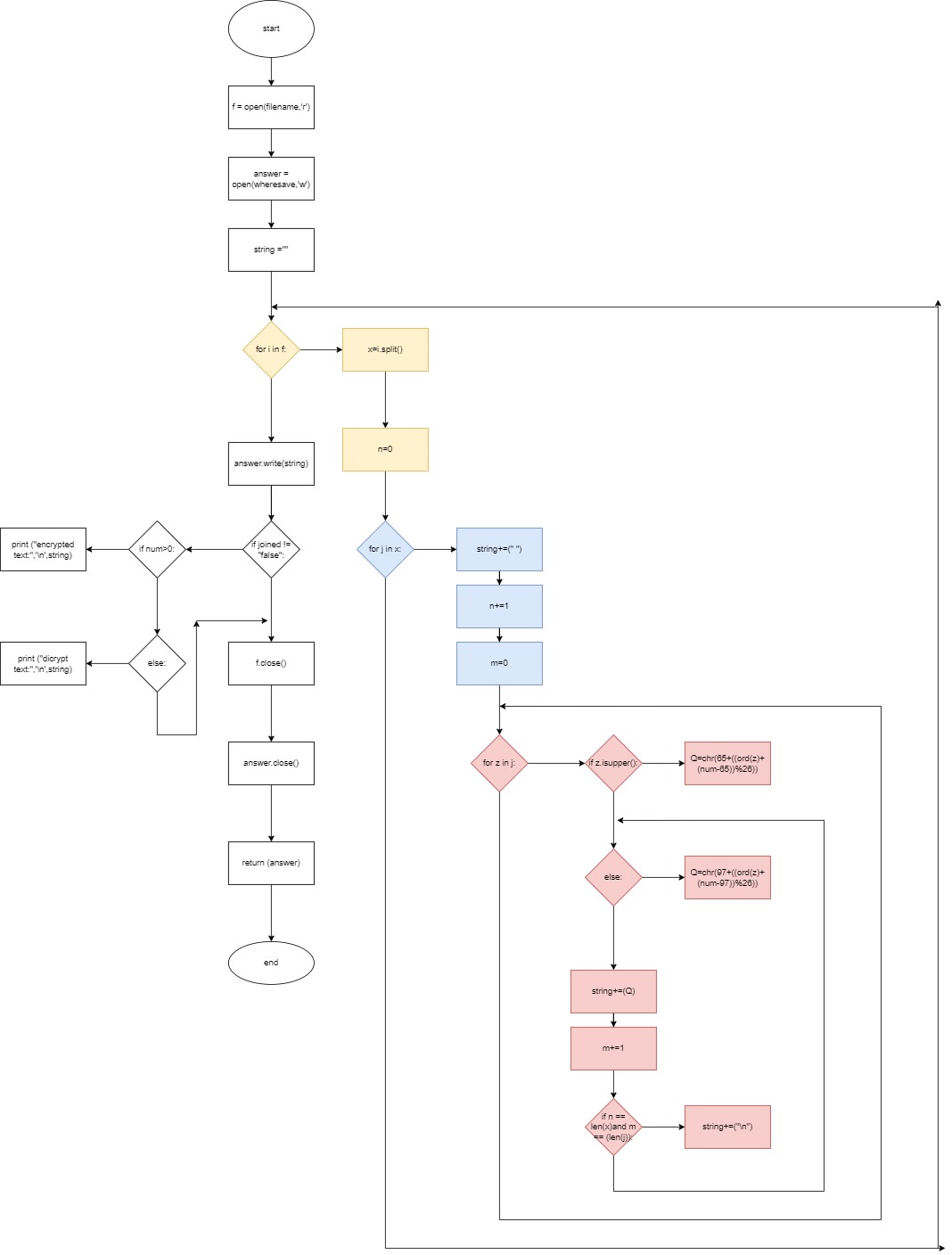
# Counting function:

This function is used to test for the accuracy of the code and the cipher language used. The counter function checks the number of words, characters, lines, and repetitions of each letter found in the file before its encryption and after its decryption. Then the user can manually compare both results to notice any problems. 

# Flow chart:

The following flowchart is only for the main function. However, a flowchart for all the other “def functions” must be draw to make the chart complete.

## Ceaser cipher:



# Bibliography:

Sidhpurwala, H. (2013, August 14). *A Brief History of Cryptography*. Red Hat Customer Portal. Retrieved December 5, 2021, from <https://access.redhat.com/blogs/766093/posts/1976023>

Simmons, G. J. (2016, August 17). cryptology. Encyclopedia Britannica. https://www.britannica.com/topic/cryptology

# Appendix:

