Dominic Beletti-Naccarato 17/20 Arias

CMPT 220-201

4/6/18

Abstract:

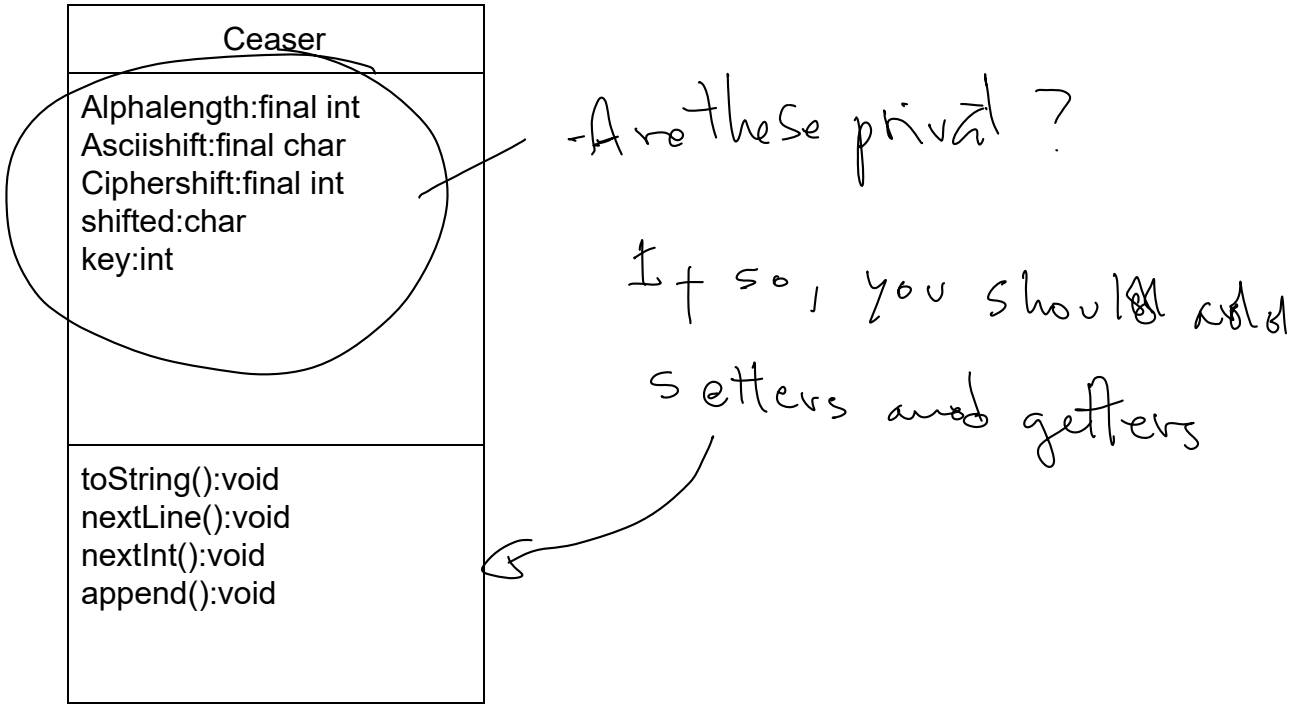
I am writing a code that will give the user the option to encode a message in multiple different ways depending on how they want it encoded. The program will also offer the ability to decode the message as well provided the user knows what key was used to encode it. I plan on having 3+ different ways to encode the message. If time allows I would also like to look into modifying the code more so that It will be able to open read and produce a new text document with the decoded or encoded message.

Intro:

Sometimes whether it be for professional or private reasons I have to send a message across a public system such as facebook messenger. Although it is secure due to the recent events that have taken place I feel like this is ever more prevalent. When sending sensitive info across these channels it can be a good idea to encrypt the info so that it is not read by people you don't want reading it.

Detailed system description:

The system runs as follows. The user inputs what message they would like to have encoded or decoded. The system then asks them what type of encoding they would like to use (right now the only one working with no bugs is the caesar cipher). Then they are prompted to enter a number between 0 and 25 to encode the message. The code then find the letter of the message that is stored in a array and replaces it with the number that comes however many places after it working in round robin style. The encoded message is then printed out to the user.



Requirements:

Many people across the world value privacy. This has become very hard to come across in this digital era and the only way to have true secrecy is to encode messages so that only you know how to decode it as well as the person receiving the message. The program I am writing allows for the users to safely encrypt and decrypt messages easily without having to spend time decoding by hand the old fashioned way.

should find some references

Literature survey:

Many other systems like this exist but many of them are either single encoding systems that can only process one type of cipher or they can only encode or decode but not both. The system is far from complete and will need much more work as making encoders and decoders from scratch is difficult and prone to messing up. All the code will be accessed via a centralized class that will use the other codes.

User manual:

To use the encoder first run the class. You will be asked to enter a message. Once the message has been entered click over to the area asking for a number between 0 and 25. After entering that number hit enter and your message will be

Is there a GUI for the application?

encoded based upon what number you selected. That number is important because it will also be used to decode the message when it needs to be.

Conclusion:

In its current state the system can encode and decode a caesar cipher with 100% accuracy. The substitution cipher I am working on still has some bugs that need to be worked out but is coming along nicely. I am currently talking to different people about what other types of ciphers would work well in a program like this. I am considering one that translates the message to Ascii code as well as a binary translator for numbers.

References/Bibliography:

Lyons, james. “Crypto.” *Practical Cryptography*, Practical Cryptography, 2012, practicalcryptography.com/ciphers/.