Joe Marinich CMPT 220 Milestone

Abstract: This program takes text files as input and either encrypts them or decrypts them (depending on the user's choice) using a Caesar Cipher. The code that is written so far uses the console to prompt the user to enter three things. First is the name of a file that currently exists. Once this is passed, the program prompts for the user to decide whether the file should be encrypted or decrypted.. Once the input is validated, the program prompts the user to enter an offset value. All of these values are stored. What is left to do is implement the Caesar Cipher and return a new file to the user, printing it to the console as well.

Introduction: With cyber security becoming an increasingly significant issue in modern society, it is important to know that files are protected. This will help to make text files more secure so that unwanted personal cannot access it. Not only will files be encrypted, but also able to be decrypted so that people can send text message without worry of other people reading them. The cipher will make it difficult to crack.

Description: The system first prompts the user for a valid text file. It then asks for the file to be encrypted or decrypted. Finally, it will ask for an offset value to shift the characters. By the time this program is completed, it will cipher the text file and create a new one.

Logic		
	+createFile(fileName : String)	
	+validateOffsetValue(offsetVal:String) : boolean	
	+validateEnOrDec(enOrDec:String) : boolean	

Display		
	+promptForFile() : File	
	+promptForOffset() : int	
	+encryptOrDecrypt() : String	

The Display class calls the Logic classes in order to validate the user input. If they return true, then the input is passed and the program continues.

Joe Marinich CMPT 220 Milestone

Requirements:
This program addresses the problem of file security. By ciphering the text file, it will encrypt it and make it difficult to read by unwanted persons. The program and also decipher so that wanted persons can read the text file.

Literature:
Citation: Wong W., Lee L., Wong K. (2001) A Modified Chaotic Cryptographic Method. In: Steinmetz R., Dittman J., Steinebach M. (eds) Communications and Multimedia Security Issues of the New Century. IFIP — The International Federation for Information Processing, vol 64. Springer, Boston, MA

This work used a modified version of the chaotic cryptographic method to encrypt a text file. This method also did it with a shorter encryption time than originally. This makes it both safer and more efficient.

User manual:

1. Enter the name/location of a file. The prompter will keep asking until a valid and existing file is inputted.
2. Enter “e” or “d” to decide whether to encrypt or decrypt the file. This is not case-sensitive. The prompter will keep asking until a valid input is entered.
3. Enter the offset value to shift the contents of the text file. The file will keep asking until a valid integer is entered.
4. (Not completed yet) The program will create a new file that either encrypted or decrypted the old one. It will be stored in the same directory as the original file and also printed to the console.

References:

Wong W., Lee L., Wong K. (2001) A Modified Chaotic Cryptographic Method. In: Steinmetz R., Dittman J., Steinebach M. (eds) Communications and Multimedia Security Issues of the New Century. IFIP — The International Federation for Information Processing, vol 64. Springer, Boston, MA

Conclusion:

This program will be console-based. It will solve the problem of file security by using encryption and decryption of text files via a Caesar Cipher. This will help to improve security with text files, making it harder for unwanted personal to access and read them.