Joe Marinich

Final Writeup

Abstract: This program takes a text file as input and either encrypts it or decrypts it (depending on the user's choice). The code uses the console to prompt the user to enter three values. First is the name of a file that currently exists. Once this is passed, the program prompts 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. The program creates a new file that contains the ciphered version of the original file via shifting the keys by the offset value.

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 personnel cannot access them. Not only will files be encrypted, but also able to be decrypted so that people can send text files without concern of other people reading them. The cipher will make it more 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. The program will then shift the characters by the offset value. This will be stores in a new text file, as well as printed through the console.

Joe Marinich

Final Writeup

Logic Class		
	- fullFile : String	
	- fileNoTXT : String	
	- encrypt : boolean	
	- offset : int	
	+Logic (fileWithTXT : String, encypt : boolean, offset : int)	
	+openOrigFile() : File	
	+createNewFile() : File	
	+cipherFile() : File	
	+cipherLine(line : String, offset : int) : String	

Display Class		
	+promptForOffset() : int	
	+promptForEncrypt() : boolean	
	+validateOffset(offset : String) : boolean	
	+validateEnOrDec(String enOrDec) : boolean	
	+validateFileName(fileName : String) : boolean	
	+promptForFileName() : String	
	+printCiphFile(file : File) : void	

Joe Marinich

Final Writeup

Class Interaction:

The Display class collects the values from the user via console input. A Logic object is then created with said values as arguments. The Logic object then uses it's methods to cipher and create a new file with the values obtained from the Display class. The Display class then takes the newly ciphered file created from the Logic object and uses its own method to print the file to the console.

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 will also decipher the file so that wanted personnel 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 the file encryption security both safer and more efficient than before.

Joe Marinich

Final Writeup

User manual:

1. Enter the name/location of a file. The prompter will keep asking until a valid and existing text 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. Choosing to encrypt will offset the characters by a positive value while choosing to decrypt will offset the values by a negative value.
3. Enter the offset value to shift the contents of the text file. The file will keep asking until a valid positive integer (or zero) is entered.
4. 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. The name of the file will be the same as the original except with either “_e” or “_d” tagged at the end to indicate if it was encrypted or decrypted, with the offset value following it.

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 cipher that shifts each character of the text a set amount. This will help to improve security with text files, making it harder for unwanted personnel to access and read them. It will also make it easier for wanted personnel to decrypt text files. Together, this will make text files more secure.

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