Diego Bez Zambiazzi

July 31, 2021

Encryption Summary

CS-405

This assignment consisted of three TODOs; one for implementing the XOR encryption logic, another for loading file data into a string, and the last one to save data into a file. First, to implement the XOR encryption logic, I only needed to add the XOR bitwise operator between the source character and the key character. Since the key’s length is smaller than the source length, I used the modulo operator to loop through the indices of the key:

Text

Description automatically generated

Then, to read the data from files into a string, I used the std::fstream class. I created a file stream object, opened it in reading mode (std::ios::in), and looped through each line of the file appending it to the string. I also modified the initial value for the file\_text string variable to my full name:

Text

Description automatically generated

Lastly, to save the data to a file, I also used std::fstream but in writing mode (std::ios::out). To me, the most challenging part of this function was creating the timestamp. I first tried using the function localtime(), but Visual Studio generated a warning about the safety of the function. Upon research, I learned that localtime(), along with other ctime functions, is not thread-safe because it returns a pointer that could be overwritten by other threads. To resolve this issue, I used localtime\_s(), which uses pre-allocated buffers:

Text

Description automatically generated

The application’s console output only names the files that were generated:

A screenshot of a computer

Description automatically generated with medium confidence

The files are attached to this submission, but an example of their content can be seen below:

Graphical user interface, text, application

Description automatically generated

The application first uses XOR encryption to encrypt the data and save it as encrypteddatafile.txt, and then uses the same function to decrypt it and save it as decrypteddatafile.txt. It is also important to note that the key “password” was only used as a simple example, and a more secure key should be used for real implementations.