CMSC-5523
Project 1 – Secure Notepad
Due: February 15th, 2016, 11:59 PM
(1500 pt)

This is an individual only project.

Create a windowed notepad application or a web-based application which allows you to edit and store text files, and load these text files from storage. However, you should also provide the option, when saving a file, to save it as an encrypted file. When doing this, you'll need to ask the user for a password, which they will use to decrypt the file as well. Using this password, you should generate an encryption key by hashing the password using SHA-256. You should use AES encryption (with 256-bit key) in CBC mode to encrypt the file. The program should then store the file on the hard drive in the location specified by the user. If the user chooses not to encrypt, the program should simply save the file. On loading a file, the program should detect whether the file is encrypted or not (this will require that you insert some sort of known tag into the encrypted file telling you that the file is encrypted), and if it is encrypted, it should ask the user for the password.
It should then decrypt the file, and display the contents within the program. The program should *not* remember the password used, and the user should be prompted for a password each time the user wants to save an encrypted file. Keys should not be stored in memory if they are no longer in use. You should, however, implement a scheme to verify the correctness of the password, so that if the password used is incorrect, it does not display a gibberish file: [Hint, this might involve a cryptographic hash function].

Notes:

1. Do *not* try to implement SHA-256 or AES on your own. Find a library and use it.
2. You may use any programming language you wish. Java is freely available for download from Oracle. OC provides access to Microsoft Visual Studio for Visual C++ and C# development. If you would like access to that, let me know.

Execution Notes:

Please document your code well. I will want the source code for your program. In addition, I will post a sign up sheet outside my door to for demonstration times. (These will take place from February 16th, but your code is still due before then. You will need to sign up for one of those times and bring your computer to show your program working.)