EECS 3540 – Project 1 – One Way Hashing
Due: Tuesday February 12, 2019

Description:

In this project you will receive a filename on the command line for your program. You are to read in the file and compute a one way hash using the SHA 512 algorithm and output it.

Details:

A one-way hash takes a file and generates a digest or hash value from it. The purpose of a one way hash is to provide a check on the integrity of the file. If you have two files producing the same one way hash you have a collision. Collisions must occur but it is the intent of the one way hash that it should be difficult to generate files with the same hash value and any simple alteration of the original file should not produce a collision.

To do this in this project I would advise breaking into sections. The first section would include reading the input file and breaking it into blocks. The SHA-512 algorithm works with a block size of 1024 bits (128 bytes). The bytes are grouped into 8 byte (64 bit) groups for this operation and the individual pieces are referred to as M_0, M_1, …, M_{15}. Read the file and build the M's for each block. This is an easy point to check your output and code for validity.

The last block may need to be padded. There are rules for padding the final block (or 2) of a SHA 512 message. That should be done next (once you do the initial steps).

Third, you should start to compute the one way hash. We will talk about this process in class. There are test sets available that you can compare to your code to check if it is working.

Finally, you should output the 512 bit hash value at the end of the program.

Submission:

You should submit your source code on the class BlackBoard web site. I need all your .c, .cpp, .h, and .hpp files.