**CS4732/5732 Cryptography Summer 2022**

**Project #3 [75 points]**

---------------------------------------------------------------------------------------------------------

Due date is Friday, August 5th

**Overview:**

In this project you will be working with hashing functions, getting more familiar with using them in code.

**Task 1:**

For this task, I want you to work with SHA-256, a common cryptographic hash function. I want you to generate several files of different lengths (one of them very short, shorter than the output of 256 bits), another at least 1Kbyte. Document how many hashes you can do per second on your machine for each of the files. Calculate how long it would take to find a collision through brute-force to a particular value for SHA-256. This time might be large. Document these results, including the hardware specs of your system at least to a limited degree. If your library does not have SHA-256, use another hashing algorithm for this an the following question

**Task 2:**

The task here is something akin to trying to generate a vanity bitcoin address. For this task, again working with SHA-256, you are going to try and generate a specific hash. Your task is to start with 256-bits all set to 0. Your goal is to try and get as much of your birthdate as you can as the most significant hex digits of the hash. So for example, if my birthdate was 02231947, then I would want to find a hash starting with 02231947. I could do this by hashing my initial all-zeros, then seeing if the most significant digits (in hex) started with 02231947. Then increment 1 to it, hash it, and see if its what I want. Then add 1 again and hash. Note, to get a hash equal to the entire birthdate would take a silly amount of time depending on your machine. So start looking for one that just has the first hex digit correct. Then try for a second digit. Now extrapolate how long it took to get the third one. Document your results and logic.

**Submission:**

For turnin I want a text document or pdf explaining in detail all information you learned and the steps you completed, as well as documenting your results. Make sure to specify initial environment chosen, any source code, results obtained in the various tasks, etc.