ECE: Information and Network Security
Computer Project, Due Date: April 19, 2018

Project Description

In this project, your team (consisting of at most four students) will implement code that examines the complexity of crypto-based puzzles, which are used as the foundation of cryptocurrency. You are allowed to use whatever language you desire, and whatever library you desire. Of course, some languages will have advantages over other languages.

Your task is to implement a hash-based crypto puzzle using SHA-256. The way the crypto puzzle works is as follows. Alice issues a challenge to Bob: Alice creates a puzzle P that is B-bytes long, where $B < 32$. She challenges Bob to find a message M that, when fed into the SHA-256 function $h()$ yields the last B bytes equal to P. That is, $h(M) = [* * * \cdots * **, P]$. Bob attempts to find such an M by generating random guesses and hashing them. When he finds one, he reports it to Alice and has solved the crypto puzzle.

You and your team are to estimate the amount of time it takes to solve the hash-based crypto puzzle for different values of B. This will necessitate that you perform timing measurements. Please note that part of the challenge will be coping with the granularity of the clock, as well as capturing the randomness in the result (i.e. you could be lucky and guess M on your first try). Therefore, you will need to average over an amount of trials in order to get an accurate time estimate. It is up to you and your team to ensure that your timing estimates are accurate.

Your team will turn in a short report (roughly 8 pages) that describes the approach you used and the explains your observations. Make certain to describe which language and libraries you used (if they are public), and submit a copy of your code. Your grade will be based upon the clarity and thoroughness of your report. Be sure to include the name of all team members on the report.