CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 11

Question 1

Alice tries to create a zero knowledge proof protocol as follows. First, she flips a coin, giving the word "Heads" or the word "Tails". She then computes the SHA3 hash of the coin's output and sends it to Bob. Alice wants to be able to prove to Bob that she knows what side of the coin came up without revealing which one.

1. Which properties (completeness, soundness, and zero-knowledgeness) does this protocol satisfy?
2. Suppose Alice decides to add 40 random digits to the end of "Heads" or "Tails" before hashing it (this is too large to brute force). Now which properties does the protocol satisfy?

Question 2

Suppose we change the three-coloring ZKP protocol from lecture to use 2-coloring instead (a problem which is solvable in polynomial time). Would this still be a valid ZKP protocol? Why or why not?

Contributors:

- Ryan Cottone, Will Giorza