Assignment 1
INSE 6110: Foundations of Cryptography
Due: In class on October 9 (or via email before class ends)

Assignments/Projects are to be completed individually. Any reference to external material should be cited. Each student has available one slip day for use on one, and only one, assignment/project of his/her choosing. Using the slip day allows the assignment to be submitted at noon on the Monday that follows the due date without penalty (in this case, assignments must be submitted digitally or slipped under my office door). Late assignments will not otherwise be accepted (exceptions made for medical certificates).

1 Hash Functions (2.5 marks)

Bitcoin is a decentralized digital currency. In order to make sure that new money is not created too quickly (which would cause inflation), new money cannot be created until someone solves a crypto puzzle that is meant to take around 10 minutes on a modern cluster of computers. A simplified version of the puzzle is as follows:

Find any value \( t \) such that for a hash function \( \mathcal{H} \), the 256 bit binary output \( y = \mathcal{H}(t) \) begins with 50 zeros.

Answer the following questions and justify your answers. If the answer is ‘it depends,’ state what the answer depends on. You may assume the hash produces uniformly random output.

(a) (1 mark) Assuming a secure hash function is used, how many calls to the hash function must be made to solve the puzzle on average (i.e., approximately how many hashes must be computed so that you expect to find a \( t \) value that satisfies the condition)?

(b) (0.5 mark) Assume the hash function is found to not be pre-image resistant. Is the puzzle easier to solve?

(c) (0.5 mark) Assume the hash function is found to not be collision-resistant. Is the puzzle easier to solve?

(d) (0.5 mark) Generally, it should be quicker to verify that a solution to a puzzle is correct than to solve it. How many calls to the hash function are required to verify if a given solution \( t \) is correct?

2 Entropy and More Hashing (5 marks)

Alice, Bob, Carol and David play the game ‘spin the bottle,’ where they sit in a circle around a bottle, the bottle is spun, and whoever the bottle points at (or is closest to where the rested bottle points) must do something embarrassing. However, the four players do not spread themselves out equally and so the bottle is more likely to point to certain people. Specifically, it points to Alice, Bob, Carol and David with, respectively, probability: \{0.28,0.22,0.25,0.25\}.

(a) (0.5 marks) What is the Shannon/average entropy of one spin of the bottle?

(b) (0.5 marks) What is the min-entropy of one spin?
(c) (0.5 marks) Alice suggests they instead chose someone using flips of a fair coin. How many coin flips are required to fairly chose one of the four participants?

After everyone goes home, Alice and Bob decide to keep playing over the phone. Unfortunately, they can no longer both see the same coin. Alice suggests the following protocol: Alice thinks of random number and gives Bob its hash (luckily her smartphone has access to a hash function). Bob does the same. They then both reveal their numbers (and check that what the other reveals matches the hash they were given). They then use the parity of the number to decide the coin flip: if they both picked even or odd numbers, it is treated as flipping the coin as heads; if one picked an even and the other an odd, it is treated as tails.

(d) (0.5 mark) Alice makes sure to choose a large number to hash, even though only its parity is used in determining the coin flip. Why?

(e) (3 marks) Say Alice prefers the coin flip be heads, and Bob prefers tails. Would breaking the pre-image resistance of the hash function help Alice cheat and get heads? Would it help Bob cheat and get tails? Would breaking the collision resistance of the hash function help Alice cheat and get heads? Would this help Bob cheat and get tails? (For each case, briefly justify your answer).