

## CSci 4554 Assignment 1

Due Friday, February 1st in class

**Problem 1 (15 points).** Exercise 1.3 pp. 20-21. Please explain all of your answers. If the function cannot be used in the protocol, please give a concrete example of how one of the participants can exploit it to their advantage.

**Problem 2 (10 points).** Alice and Bob are high school friends. They decide to use the coin-flipping protocol (Prot. 1.1).

Alice decides to use the Java `Random` class as a random number generator. Alice was born on May 5th so 5 is her favorite number. She uses it as the seed for the random number generator: `new Random(5)` and then calls `nextLong()` to get a random long integer. She applies the agreed-upon one-way function  $f$  to the generated long integer and the protocol proceeds as specified.

Please explain why Alice may be giving Bob an unfair advantage. Refer to the description of the Java `Random` class. What should she change to fix the problem? Please explain (briefly) why the fix works.

**Problem 3 (10 points).** Exercise 2.10 p. 52. Give the exact sequence of messages.

**Problem 4 (10 points).** Exercise 2.13 p. 53.