

CSci 4554 Assignment 1

Due Friday, September 6 in class

Problem 1 (8 points). In the Coin Flipping example, suppose the following function is used as a hash function: it maps from a space of 200-bit integers to that of 100-bit integers as follows: $f(x)$ computes a bi-by-bit XOR ("exclusive or") of the most significant 100 bits of x with the least significant 100 bits of x , i.e. the first bit with the bit number 101, etc.

- Is it the case that $f(x)$ is easy to compute, given x ?
- Is it true that the knowledge of $f(x)$ does not provide any information about x ?
- is it true that it is very difficult or impossible to find $x \neq y$ such that $f(x) = f(y)$?
- If this function is used in the protocol, can Alice use it to manipulate the outcome in her favor? If yes, please explain how (be very specific). If not, please explain why.

Problem 2 (12 points). Problems 1.1 and 1.2 on p. 24.

Problem 3 (5 points). Problem 1.4 on p. 25.