CSE 484 In-class Worksheet #8 – Lecture 10– Fall 2017

Name: ________________ UW Student #: _____________ Date: __________________

Email address: ____

Partner names for this activity: ____________________________________

Q1: For hash functions, one-wayness does not imply collision resistance. We can prove this by constructing a hash function that is one-way but *not* collision resistant.

Suppose g is one-way.
Define h(x) as g(x') where x' is x except the last bit.

Then h is one-way (to invert h, must invert g).

But collisions for h are easy to find. **How?**

Q2: For hash functions, collision resistance does not imply one-wayness. We can prove this by constructing a hash function that is collision resistant but *not* one-way.

Suppose g is collision-resistant.
Define y=h(x) to be 0x if x is n-bit long, 1g(x) otherwise.

Then h is collision resistant: if y starts with 0, then there are no collisions. If y starts with 1, then must find collisions in g (which is hard by definition).

But h is not one-way. Some y's are easy to invert! **Which ones, and how?**

Q3: What problem do you see with the "Encrypt-and-MAC" approach for authenticated encryption?