CSE 484 In-Class Worksheet #9 – Spring 2019
Name: ____________________________ UWNetID: _____________ Date: ____________
Email address: ____
Partner names for this activity: ____________________________________
Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: Which property or properties of cryptographic hash functions (one-wayness, collision resistance, weak collision resistance) are needed for the following applications, and why?

(a) Storing password hashes?

(b) Integrity of software distribution?

(c) Private auction bidding?

Q2: What problem do you see with the “Encrypt-and-MAC” approach for authenticated encryption?