

**CSE 484 In-Class Worksheet #9 – Autumn 2018**

Name: \_\_\_\_\_ UWNetID: \_\_\_\_\_ Date: \_\_\_\_\_

Email address: \_\_\_\_\_

Partner names for this activity: \_\_\_\_\_

Will you want to pick up your worksheet later? Circle one: Yes / No

**Q1:** The one-time pad theoretically provides perfect secrecy, but only under certain conditions.

For example:

(a) What problem arises if I reuse the same key -- what can an attacker learn?

(b) Can a one-time pad protect the integrity of messages?

**Q2:** How many different keys are there, for a block cipher with 128-bit blocks and 256-bit keys?

**Q3:** How many different permutations are there over 128-bits (for a 128-bit block cipher)?

**Q4:** What security concerns do you see with the ECB block cipher mode?

**Q5:** Why might you want to use CTR mode instead of CBC mode?

**Q6:** Do CTR mode or CBC mode protect the integrity of messages? If so, why? If not, can you give a counter example?

