CSE 484 In-class Worksheet #7 – Lecture 8– Fall 2017

Name: ________________ UW Student #: _____________ Date: __________________

Email address: ____

Partner names for this activity: ____________________________________

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 permutations are there over 128-bits (for a 128-bit block cipher)?

Q3: How many different keys are there, for a block cipher with 128-bit blocks and 256-bit keys?

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?