CSE 484 In-Class Worksheet #8 – 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: Can you think of some potential tradeoffs between symmetric and asymmetric cryptography?

Q2: 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?