CSE 484 In-Class Worksheet #7 – 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: Why is C's rand() function not a great choice for security-critical applications that rely on randomness?

Q2:

(a) What is the key space for the Caesar (or shift) cipher? (That is, how many possible keys, or shifts, are there?)

(b) How could you attack a Caesar/shift cipher?

Q3:

(a) What is the keyspace for a substitution cipher?

(b) How could you attack a substitution cipher?