CSE 484 In-class Worksheet #6 – Lecture 7– Fall 2017

Name: _____ UW Student #: _____ Date: _____

Email address: _____

Partner names for this activity: _____

Q1:

(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?

Q2:

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

(b) How could you attack a substitution cipher?

Q3: 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?