**CSE 484 In-class Worksheet #6 – Lecture 7**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UW Student #: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

**Q1:** What is the key space for the Caesar (or shift) cipher? (That is, how many possible keys, or shifts, are there?)

**Q2:** How could you attack a Caesar/shift cipher?

**Q3:** What is the keyspace for a substitution cipher?

**Q4:** How could you attack a substitution cipher?

**Q5:** What is the key space for an Enigma machine with n rotors?

**Q6:** The one-time pad theoretically provides perfect secrecy, but only under certain conditions. For example:

1. What problem arises if I reuse the same key -- what can an attacker learn?
2. Can a one-time pad protect the integrity of messages?