**CSE 484 In-class Worksheet #6 (Fall 2016)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_\_\_\_

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

**Q1:** Due to the Debian key generation bug, there were thousands and thousands of computers using weak keys drawn from a very small set of keys. Given the number of Debian installations in the world, I have to assume that many computers were actually using THE SAME KEYS. My intuition says that should be obvious to someone, but it went unnoticed for 2 years. How would you design a company, operating system, Internet, or computer such that those kinds of errors couldn’t go unnoticed for 2 years?

**Q2**: Why Kerchhoff’s Principle? What are some advantages of using crypto where the only secret part is the key? Any disadvantages?

**Q3:** (briefly) What are some disadvantages of symmetric cryptography?