**CSE 484 In-class Worksheet – Lecture 21 – Spring 2017**

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

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

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

**Q1:** What are some of the root causes of usability issues in computer security?What are some approaches for addressing usability challenges in computer security?

**Q2:** What is anonymity? Why might people want anonymity, or NOT want anonymity, on the internet?

**Q3:** Consider the message that A sends to B via the mix: {r1,{r0,M}pk(B),B}pk(mix)

Why do we need the random numbers?