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

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

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

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

**Q1:** It’s easy to see why criminals and dissidents might want anonymity. What are some other groups that might find anonymity really useful?

**Q2:** Alice and Bob are talking using OTR. Bob receives a message MACed with their shared secret, so he’s sure that Alice sent it. Can he prove to Eve that Alice sent the message? Why or why not?

**Q3:** Chaum’s mix required a trusted re-mailer whose job was to provide obscurity to the question of which messages went to which people. What if the mix is malicious? What might you do differently in order to defend against malicious mixers? Consider solutions with more than one mix.