CSE 484 In-Class Worksheet #12 – Autumn 2018
Name: _____ UWNetID: _____ Date: _____
Email address: _____
Partner names for this activity: _____
Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: Suppose you are creating a new website, and you expect millions of users. How will you store those user's usernames and passwords, so that users can authenticate later but an adversary who breaks into your computers and steals all your data can't easily figure out everyone's password?

Q2: What problem, if any, do you see with the "Encrypt-and-MAC" approach for authenticated encryption?

Q3: Alice and Bob are both cryptographers, and they are talking on the phone. They want to randomly flip a coin. If they were together, in person, they would flip a real coin and see if it was Heads or Tails. But they are not together, in person, and they don't trust each other enough to have one of them flip a coin and tell the other person the answer.

Using the techniques we've discussed so far in class, how can Alice and Bob effectively flip a random coin together, over the phone, such that they both trust the answer even though they don't trust each other?