**CSE 484 In-class Worksheet #-32,768 (Fall 2016)**

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

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

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

**Q1:** (Review): What security concerns are there with the ECB block cipher mode? Describe ECB mode in one sentence, then explain the biggest problem with it in one sentence.

**Q2:** (Review): Draw the CBC mode decryption process.

**Q3:** How will you break the phonebook hash function’s one-wayness?

**Q4:** Why is hashing better than encryption for passwords?

**Q4:** Write definitions (mathematical or English) for each of these properties we want in a cryptographic hash function.

One-wayness:

Collision resistance:

Weak collision resistance: