**CSE 484 In-class Worksheet – Lecture 8 – Spring 2017**

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

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

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

**Q1:** How many different permutations are there over 128-bits (for a 128-bit block cipher)?

**Q2:** How many different keys are there, for a block cipher with 128-bit blocks and 256-bit keys?

**Q3:** What security concerns do you see with the ECB block cipher mode?

**Q4:** Draw the CBC mode decryption process.

**Q5:** Why might you want to use CTR mode instead of CBC mode?

**Q6:** What do you think it means for an encryption scheme to be secure? Said another way, what properties must an encryption scheme have in order to be secure?

**Q3:** Block ciphers are an encryption primitive which take a fixed-length block of message and encrypt it. For example, AES is a modern block cipher with 128-bit block size. Let’s say you have a message that’s more than 128 bits long. How would you go about encrypting it with a block cipher? What you’ve invented is called a “block cipher mode of encryption”. Can you think of any dangers or flaws in your approach?

**Q3:** Researchers found the following code in use on a Diebold voting machine to perform a CBC mode encryption:

DesCBCEncrypt((des\_c\_block\*)tmp, (des\_c\_block\*)record.m\_Data,

 totalSize, DESKEY, **NULL**, DES\_ENCRYPT)

The NULL parameter sets the IV to all 0s.

1. What’s bad about constant IV used across multiple CBC encryptions with the same key?
2. What’s bad about using all 0s for your IV?