**CSE 484 In-class Worksheet #1337 (Fall 2016)**

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

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

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

**Q1:** In a hypothetical course, you are told you will take an exam tomorrow in which you are expected to write the first 100 digits of pi on a sheet of paper. The goal is to cheat on the exam in a way that will not be caught by typical exam proctoring procedures. You may cheat alone or collaboratively. What are some of the ways you would consider cheating on this intentionally unfair exam?

**Q2**: Look at the picture of Electronic Codebook Mode (EBC Mode) on the slide. In this example, AES is used to encrypt a plaintext of length 128 \* 5 = 640 bits by breaking it into five chunks of length 128 and separately encrypting each one with the key K. What’s wrong with this approach? What kind of information can leak from EBC Mode?

**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?