**CSE 484 In-class Worksheet #7 (Fall 2016)**

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

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

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

**Q1:** What can we say about the security of a one time pad? Say I encrypt some plaintext message M with a ***random*** key K to create ciphertext C. Let’s say that C = 01101111. What statistical properties are true about the relationship of this particular C to the domain of messages that I might have encrypted? What does knowing C tell you about my message M?

**Q2**: One-time pads are cumbersome because your key needs to be the same length as your message. But they have other problems too. What are some other problems with one time pads? What security properties don’t they provide? How can they be misused?

**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?