CSE 484 In-class Worksheet #4

Name: ________________ UWNetID: _____________ 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?