# Homework 4 – Due Tuesday, February 20

1. The AES handout mentions that there is an attack on a block cipher that requires building a table whose size is a function of the block size (see the "Block Size" discussion in the "Background" section). How much memory/storage would this require for a block cipher with 80-bit blocks?

2. You are developing an application in which you have to regularly send packets that are 36 bytes (288 bits) long using AES. If you use CBC mode, how much data do you need to transmit? Explain the reasoning behind your answer (show your work).

3. Joe Crypto always loved playing the "guess which hand is holding a prize" game, so proposes the following guessing game: You can give him two files, containing whatever data you want them to contain, but with the restriction that they are the same length. He will then encrypt both of them, shuffle up the order randomly, and let you choose one of the two — he gives that to you, and you have to guess which file was encrypted to produce that ciphertext! Joe's crypto knowledge isn't so great, however, and he uses AES in ECB mode. How can you play this game so that you can always win? Be very specific, including a clear explanation of why your strategy allows you to win. (*Hint: What is the main weakness of ECB mode, and how can you create a file that displays this weakness?*)