Homework 7 – Due Tuesday, March 7

1. Prove that using CBC mode with a fixed IV (e.g., always using all zeros as the IV) and any basic block cipher (like DES or AES) cannot be IND-CPA secure. Your answer should be a full and well-written proof.

2. Next consider CBC mode with a randomly chosen IV, but with only a small amount of entropy in the IV. Say that only 32 bits of the IV are random. Prove that this is not IND-CPA secure (the probability analysis and advantage calculation are very important in this problem, so make sure you do that analysis clearly!).

3. Consider a cipher that has the following property: When you view the plaintext bits and ciphertext bits as binary numbers, the cipher preserves the evenness of the number. In other words, if the plaintext is an even number then the ciphertext will also be an even number, and if the plaintext is odd then the ciphertext will also be odd.

   (a) Prove that such a cipher cannot be IND-CPA secure.

   (b) Joe decides to "fix" the cipher by doing the following: he adds one additional bit to the key, and then adds this (as a number) to the ciphertext after encryption. If this key bit is chosen randomly, then half the time even numbers map to even numbers, and the other half of the time even numbers map to odd numbers. Since this is random and unpredictable if the bit isn't known, he thinks this fixes the problem. However, it is still not IND-CPA secure — prove this.