Assignment 4 – Due Friday, October 14

The first two problems are from the book, and deal with error propagation in two block cipher modes.

1. Page 216, Problem 6.4
2. Page 216, Problem 6.8

The remaining problems explore the security models that we discussed in class, in particular the notion of indistinguishability under chosen plaintext attack. First, let's review the ideas and define some notation.

We define security in terms of a "game" that an adversary plays against "oracles" — if you can define an adversary that wins the game with probability significantly better than making a random guess, then the scheme is insecure. Conversely, if no adversary can win the game with probability non-negligibly higher than guessing then the scheme is secure. Note that it's much easier to prove a scheme is insecure than to prove that one is secure!

The "IND-CPA game" is as follows. At the beginning of the game the oracle(s) randomly choose a key for the encryption scheme that is being attacked. During the game, there are two oracles that the adversary can interact with, called Encrypt and Challenge. If the adversary calls Encrypt(M) for some message M, the oracle encrypts M using the key that it selected at the beginning of the game and returns the ciphertext. The other oracle takes two plaintext inputs, chosen however the adversary wants, and is called by Challenge(M_0, M_1). The Challenge oracle picks a random bit $b \in \{0, 1\}$ and returns Encrypt(M_b) without letting the adversary know what b was chosen. Note that Challenge can only be called once for the duration of the game. At the end of the game, the adversary must guess the value of b (in other words, which plaintext did the Challenge oracle encrypt?) — if the adversary is correct, than it wins the game. Clearly it's easy to make an adversary that wins with probability $\frac{1}{2}$ just by guessing randomly, so the challenge is to win with probability significantly greater than $\frac{1}{2}$. In all of the problems below, the adversary can win every time (i.e., it wins with probability 1).

1. A *deterministic* encryption scheme is one that produces the same ciphertext every time the same plaintext is encrypted. Prove that a deterministic encryption scheme cannot be IND-CPA secure. More specifically, carefully and precisely define an adversary algorithm that wins the IND-CPA game against any deterministic encryption scheme. Define the adversary using pseudo code, and make sure you give your reasoning describing why this wins the IND-CPA game.

2. It turns out that ECB mode is horribly insecure with respect to the IND-CPA game. Devise an adversary that can win the IND-CPA game against an ECB mode scheme by only using a single call to the Challenge oracle, and never calling the Encrypt oracle.

3. When we talked about CBC mode, we stressed that the IV should be unpredictable. What if this is not the case? Consider an encryption scheme that uses CBC mode with a standard deterministic block cipher so that encryption of a message M produces a ciphertext of the form $\langle IV, C\rangle$, where IV is the initialization vector for CBC mode encryption of M. Now assume that we have some function Predict(IV) that computes IV' with the following property: if a call to Encrypt produces $\langle IV, C\rangle$ then the next call to Encrypt will produce a ciphertext of the form $\langle IV', C'\rangle$ (for example, if we used a counter for the IVs, then we could predict the next IV). Show that if this is the case then the scheme is not IND-CPA secure — again define the adversary carefully, but in this case you can call Encrypt in addition to the oracles.