CS 380/525: Intro to Cryptography
Fall 2022
Assignment 2, due 9/27, before class
Total points: 100

September 12, 2022

Please write your name on your assignment that you turn in.

1. (10 points) What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operation?

2. (30 points) In class, we'd seen the stateful variant of CBC mode is IND-CPA insecure. However, the stateful variants of OFB and CTR modes are IND-CPA secure. Write the IND-CPA attack games for the stateful OFB and CTR modes, akin to the one for stateful CBC mode, assuming adversary knows the first IV/nonce. Briefly point out and explain why the attack games fail.

3. (20 points) Consider a stateful variant of CBC mode, where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing a random IV every time). In this case, the IVs are *distinct*, but not random. Write the IND-CPA game, and informally argue why the resulting scheme is IND-CPA insecure. Assume adversary knows first IV.

4. (20 points) What is the output of an n-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

   (a) Each round function outputs all 0s, regardless of the input.

   (b) Each round function is the identity function (if f is an identity function, then $f(x) = x$).

5. (20 points) Let $\mathsf{Feistel}_{f_1,f_2}(\cdot)$ denote a 2-round Feistel network using functions f_1 and f_2 (in that order). Show that if $\mathsf{Feistel}_{f_1,f_2}(L_0, R_0) = (L_2, R_2)$, then $\mathsf{Feistel}_{f_2,f_1}(R_2, L_2) = (R_0, L_0)$. (Hint: no formal proof is required, just focus on the Feistel network formulas for computing $\mathsf{Feistel}_{f_1,f_2}(L_0, R_0)$, and $\mathsf{Feistel}_{f_2,f_1}(R_2, L_2)$. You can mathematically derive this).

How to submit: Please upload your **pdf** file on Canvas. You can use my posted template for typesetting your assignment, but aren't required to do so.