Name:

Purdue E-mail:

I collaborated with (...). I affirm that I wrote the solutions in my own words and that I understand the solutions I am submitting.

Homework 2

Due date: Tuesday, October 2$^{\text{nd}}$ 3:00 PM

Question 1 (15 points)

1. What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operations?

2. Show that the CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption schemes (regardless of F). Briefly describe how an attacker could win the CCA-Security game with non-negligible advantage.

3. Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $\mathsf{ctr} \in \{0,1\}^n$ is chosen, and the i^{th} ciphertext block c_i is computed as $c_i := F_k(\mathsf{ctr} + i + m_i)$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

Question 2 (20 points)

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a length-preserving pseudorandom function. For the following construction of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-2} \to \{0,1\}^{4n}$, state whether F' is a pseudorandom function: if yes prove it, if not show an attack.

- $F'_k(x) \stackrel{\text{def}}{=} F_k(00||x)||F_k(x||01)||F_k(10||x)||F_k(x||11)$

- $F'_k(x) \stackrel{\text{def}}{=} F_k(0||x||0)||F_k(0||x||1)||F_k(1||x||0)||F_k(1||x||1)$

Question 3 (20 points)

Before HMAC, it was common to define a MAC of arbitrary-length message as $\mathsf{Mac}_{\mathsf{s,k}}(m) = H^s(k||m)$ where H is a collision-resistant hash function. We assume s is known to the attacker, and k is kept secret.

- (5 points) Show that this is not a secure MAC when H is constructed using Merkle-Damgård transform. Explain how an attacker can win the MAC security game.

- (15 points) Prove that this is a secure MAC if H is modeled as a random oracle.

Question 4 (20 points)

Let (Gen_1, H_1) and (Gen_2, H_2) be two hash functions. We define (Gen, H) as follow:

- Gen : runs $\mathsf{Gen_1}$ and $\mathsf{Gen_2}$ to obtain s_1, s_2
- $H^{s_1,s_2}(x) = H_1^{s_1}(x)||H_2^{s_2}(x)$

Prove that if at least one of (Gen_1, H_1) and (Gen_2, H_2) is collision resistant, then (Gen, H) is collision resistant

Question 5 (25 points)

One way to build a Pseudorandom Permutation from a pseudorandom function is to use a Feistel Network. In particular, if we select k PRF keys $K_1, K_2, ..., K_k$ we can define the Pseudorandom Permutation $PRP_{K_1,K_2,...,K_k}(L_0, R_0) = (L_k, R_k)$ where for each $0 \leq i < k$ we have $L_{i+1} = R_i$ and $R_{i+1} = L_i \oplus F_{K_{i+1}}(R_i)$.

It has been shown that if F_K is a secure PRF and we use a $k = 4$ round Feistel network that the permutation PRP_{K_1,K_2,K_3,K_4} is a strong pseudorandom permutation. When $k = 3$ it is known that PRP_{K_1,K_2,K_3} is a pseudorandom permutation, but not a *strong* pseudorandom permutation. **Recall:** A strong PRP means that no PPT attacker can distinguish PRP_{K_1,K_2,K_3} from a truly random permutation f when given oracle access to *both* the permutation (either PRP_{K_1,K_2,K_3} or $f()$) AND its inverse (either $PRP^{-1}_{K_1,K_2,K_3}$ or $f^{-1}()$). In the security game for a regular PRP the distinguisher is not given oracle access to the inverse permutation.

1. (2 points) Show that when $k = 1$ the function is not a regular PRP. You should explain what the distinguisher does and show that its advantage is non-negligible.

2. (5 points) Show that when k=2 the function is not a regular PRP. You should explain what the distinguisher does and show that its advantage is non-negligible.

3. (10 points) We will show that when $k = 3$ the function is not a strong PRP. Consider a distinguisher that makes two queries to the permutation g (either PRP_{K_1,K_2,K_3} or $f()$) and one query to g^{-1}. The first two queries to $g()$ are as follows $g(L_0, R_0)$ and $g(L'_0, R'_0)$ where $R_0 = R'_0$ but $L'_0 \neq L_0$. Let (L_3, R_3) and (L'_3, R'_3) denote the outputs of both queries. Finally, consider the query $g^{-1}(L'_3, R'_3 \oplus L_0 \oplus L'_0)$ and let (L''_0, R''_0) denote the output of this query. Supposing that $g = PRP_{K_1,K_2,K_3}$ is the Feistel Network defined above write down a formula for R''_0 in terms of variables known to the distinguisher. **Note:** Your formula should only use variables that are known to the distinguisher such as L_0, L'_0, R_0, R'_0 or L_3, L'_3, R_3, R'_3. By contrast, your formula should not involve the secret keys K_1, K_2, K_3 or internal values (e.g., R'_2) that would not be known to the distinguisher.

4. (5 points): Supposing that $g = f$ is a truly random permutation and letting (L''_0, R''_0) denote the output of the query $g^{-1}(L'_3, R'_3 \oplus L_0 \oplus L'_0)$ upper bound the probability that R''_0 satisfies the above formula.

5. (3 points): Using the last two observations explain why our $k = 3$ Feistel round construction PRP_{K_1,K_2,K_3} is not a strong PRP. What does the distinguisher do? (Note: it is possible to answer parts D and E without answering part C).