CS255: Cryptography and Computer Security **Winter 2014**

Final Exam

Instructions:
– **Answer all five questions.**
– The exam is open book and open notes. Wireless devices are not allowed.
– Students are bound by the Stanford honor code.
– You have two and a half hours.

Problem 1. Questions from all over.

a. PRPs vs. PRFs. Let $\Pi : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a secure PRP. Explain how an adversary can win the PRF security game against Π with advantage $1/2$ using $O(|\mathcal{X}|^{1/2})$ queries.

b. Is the following function collision resistant: $f(k, x_0, x_1) = \text{AES}\big(k,\ \text{AES}(k, x_0) \oplus x_1\big)$? If so explain why, if not explain how to find collisions.

c. For nonce-based encrypt-then-MAC mode to provide authenticated encryption the same nonce must never be reused with a single key. What can go wrong if a nonce is reused? Is encrypt-then-MAC no longer CPA secure or does it no longer provide ciphertext integrity (or both)? Explain briefly.

d. When using RSA-FDH to sign messages, how many valid signatures are there for a given message m for a fixed verification key? (the hash function used in RSA-FDH is fixed) Same question for Lamport one-time signatures built from a one-way permutation: how many valid signatures are there for a given message m?

e. Is it the case that for all many-time existentially unforgeable signature schemes there must only be one valid signature for every message? If so explain why. If not, give a counter-example.

f. Let $H : M \to \{0,1\}^{128}$ be a collision resistant hash function known to the adversary. Does the function $f(k, m) = H(m) \oplus k$ give a secure MAC? If so explain why. If not, describe an attack.

Problem 2. Recall that in the homework you constructed a secure PRF that becomes insecure if an attacker learns a *single* bit of the key. Here your goal is to build a PRF that remains secure even if the attacker learns any *single* bit of the key.

a. Let $F : K \times X \to Y$ be a secure PRF where $K = \{0,1\}^{128}$. Construct a new PRF $F_2 : K^2 \times X \to Y$ that remains secure if the attacker learns any *single* bit of the key. Your function F_2 may only call F once. Briefly explain why your PRF remains secure if any single bit of the key is leaked.

b. Is your PRF from part (a) secure if the attacker learns *two* bits of her choice from the key? If so explain why, if not give an example secure F for which F_2 becomes insecure when the attacker learns some two bits of the key.

Problem 3. One way functions.

a. Let p be a prime where 3 does not divide $p-1$. Is the following function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ defined by $f(x) = x^3$ in $\mathbb{Z}_p$ a one-way function? Justify your answer.

b. Recall that the RSA function is defined as $\text{RSA}(x) = x^e \bmod N$, where N is a product of two large primes. For each of the following explain if RSA is a secure trapdoor permutation on $\mathbb{Z}_N$. If so explain why, if not explain why not.

b1. $e = 2$ **b2.** $e = 1$ **b3.** $e = -1$

c. Suppose $f : X \to X$ is a one-way permutation. Prove that $g(x) = f(f(x))$ is also a one-way permutation. As usual, please prove the contra-positive statement. (this question comes up in the security analysis of the S/key authentication system)

d. Our goal next is to show that part (c) may not hold for one-way functions. Suppose $f : X \to X$ is a one-way function and define $h : X^2 \to X^2$ as

$$h(x,y) = \begin{cases} (0,0) & \text{if } y = 0 \\ (f(x),0) & \text{otherwise} \end{cases}$$

d1. Show that $h(x,y)$ is a one-way function.

d2. Show that $h(h(x,y))$ is not a one-way function.

This means that for some one-way functions S/key may be insecure.

Problem 4. Ciphertext expansion vs. security. Let (E, D) be a symmetric encryption scheme encrypting bit strings.

a. Suppose that for all keys and all messages m, the encryption of m is the exact same length as m. Show that (E, D) cannot be CPA-secure.

b. Suppose that for all keys and all messages m, the encryption of m is exactly ℓ bits longer than the length of m. Show an attacker that can win the CPA security game using $2^{\ell/2}$ queries and non-negligible advantage (in fact, advantage close to $1/2$). Consequently the cipher becomes insecure if a key is used to encrypt $2^{\ell/2}$ messages.
Hint: for simplicity you may assume that every message m can be mapped to exactly 2^ℓ ciphertexts. Note that a similar statement can be shown to hold without this assumption. You may also assume that the message space contains more than 2^ℓ messages.

Problem 5 Let $N = pq$ be an RSA modulus. Let $g \in [0, N^2]$ be an integer satisfying $g = 1 \bmod N$. Consider the following encryption scheme. The public key is (N, g). To encrypt a message $m \in \mathbb{Z}_N$ do: (1) choose a random h in $\mathbb{Z}_{N^2}$, and (2) compute $c := g^m \cdot h^N$ in $\mathbb{Z}_{N^2}$. Our goal is to develop a decryption algorithm.

a. Show that the discrete log problem base g is easy. That is, show that given g and g^x in $\mathbb{Z}_{N^2}$ there is an efficient algorithm to compute x. Recall that $g = aN + 1$ for some integer a and you may assume that a is in $\mathbb{Z}_N^*$.
Hint: use the binomial theorem.

b. Show that given g and the factorization of N, decrypting $c = g^m \cdot h^N$ in $\mathbb{Z}_{N^2}$ can be done efficiently.
Hint: consider $c^{\varphi(N)}$ in $\mathbb{Z}_{N^2}$. Use the fact that by Euler's theorem $x^{\varphi(N^2)} = 1 \bmod N^2$ for all $x \in \mathbb{Z}_{N^2}^*$. Recall that $\varphi(N^2) = N\varphi(N)$. You may assume that $\varphi(N)$ is relatively prime to N.

c. Show that this system is additively homomorphic. That is, show that given $E(\text{pk}, m_0)$ and $E(\text{pk}, m_1)$ it is easy to construct $E(\text{pk}, \ m_0 + m_1)$.