CS255: Cryptography and Computer Security **Winter 2012**

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 hours and thirty minutes.

Problem 1. Questions from all over.

a. Suppose $G : \{0,1\}^s \to \{0,1\}^n$ is a secure PRG. Is $G'(x) = G(x \oplus 1^s)$ a secure PRG? If so, explain why. If not, describe an attack.

b. Suppose $F : K \times \{0,1\}^n \to \{0,1\}^n$ is a secure PRF. Is $F'(k,x) = F(k,x) \oplus F(k,\ x \oplus 1^n)$ a secure PRF? If so, explain why. If not, describe an attack.

c. Let (S,V) be a secure MAC with message space $\{0,1\}^n$ for some large n. Define the MAC (S',V') as

$$S'(k,m) = \big(S(k,m)\ ,\ S(k,0^n)\big) \quad \text{and}$$

$$V'\big(k,\ m,\ (t_1,t_2)\ \big) = \begin{cases} 1 & \text{if } V(k,m,t_1) = V(k,0^n,t_2) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Is this (S',V') a secure MAC? If so, explain why. If not, describe an attack.

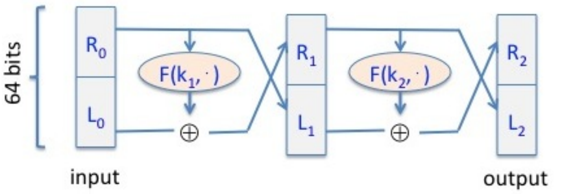
d. Suppose an attacker intercepts a ciphertext c which is the encryption of a messages $m \in \{0,1\}^n$ under nonce-based counter mode. Can the attacker create the encryption of $m \oplus 1^n$ just given c? If so, explain how. If not, explain why not.

e. Same question as part (d) except that now m is encrypted using Galois Counter Mode (GCM). Can the attacker create the encryption of $m \oplus 1^n$ just given c? If so, explain how. If not, explain why not.

f. Let $\mathbb{G}$ be a group in which the Computational Diffie-Hellman problem (CDH) is easy. That is, there is an efficient algorithm $\mathcal{A}$ that for all $x, y \in \mathbb{Z}$, given $(g, g^x, g^y) \in \mathbb{G}^3$ outputs g^{xy}. Can this algorithm be used to break the ElGamal encryption system in $\mathbb{G}$? If so, explain how. If not, explain why not.

Problem 2. Luby-Rackoff

Recall that the Luby-Rackoff theorem states that using a secure PRF in a *three* round Feistel network results in a secure block cipher. Let's see what goes wrong if we only use a *two* round Feistel. Let $F : K \times \{0,1\}^{32} \to \{0,1\}^{32}$ by a secure PRF. Recall that a 2-round Feistel defines the following block cipher $F_2 : K^2 \times \{0,1\}^{64} \to \{0,1\}^{64}$:



Here R is the right 32 bits of the 64-bit string and L is the left 32 bits.

a. Draw the circuit for $F_2^{-1}(k, \cdot)$.

b. Show that F_2 can be distinguished from a truly random one-to-one function with advantage close to 1.
Hint: Think about querying the PRF challenger at two points and xoring the results. Then see if you can find a relation among the returned values that will let you distinguish the PRF from random.

Problem 3. Recall that Lamport signatures are one-time signatures built from a one-way function f. Key generation outputs a public key containing $O(n)$ points in the image of f. A signature on an n-bit message is a set of $O(n)$ pre-images of certain points in the public key.

Show that the length of Lamport signatures can be reduced by a factor of t at the cost of expanding the public and secret keys by a factor of at most 2^t. Make sure to describe your key generation, signing, and verification algorithms.
Hint: Think of signing t bits of the message at a time as opposed to just one bit at a time.

(in fact, one can shrink the size of Lamport signatures by a factor of t without expanding the public key. This is a little harder and not discussed here.)

Problem 4. Private equality test. Suppose Alice has a secret number $a \in \mathbb{Z}_q$ and Bob has a secret number $b \in \mathbb{Z}_q$, for some prime q. They wish to design a private equality protocol, namely a protocol such that at the end, if $a = b$ Alice learns that fact, but if $a \neq b$ then Alice learns nothing else about b. Either way Bob learn nothing about a. Think of a and b as hashes of a file. The two want to test if they have the same file without leaking any other information about the contents of their files.

Let $\mathcal{E}$ be a public key encryption system with message space $\mathbb{Z}_q$. $\mathcal{E}$ satisfies the following property: given pk and $c_1 = E(\text{pk}, x)$ and $c_2 = E(\text{pk}, y)$ for x, y in $\mathbb{Z}_q$ it is possible to create a new ciphertext c that is a fresh random encryption of $x + y$, namely $c = E(\text{pk}, x + y)$ and c is independent of c_1 and c_2. An encryption scheme with this property is said to be *additively homomorphic.* Now, Alice proposes the following protocol:

- Alice generates a pk/sk pair for $\mathcal{E}$ and sends pk and $c_1 := E(\text{pk}, a)$ to Bob.
- Bob chooses random $s \xleftarrow{\text{R}} {\mathbb{Z}_q}^*$ and computes the encryption of $E(\text{pk},\ s(a - b))$. Call the resulting ciphertext c_2. Bob sends c_2 back to Alice.

a. Explain how Bob computes c_2 given pk, c_1 and s.
Hint: you will need to use a variant of the repeated squaring algorithm.

b. Explain how Alice uses c_2 and her secret key to test if $a = b$. If $a \neq b$, explain why Alice learns nothing about b other than the fact that $a \neq b$.

c. Let $\mathbb{G}$ be a group of order q where the Decision Diffie Hellman problem is hard. Let g be a generator of $\mathbb{G}$ and let $\mathcal{E}$ be the following variant of ElGamal encryption: the public key is $\text{pk} = (g, h = g^d)$ and the secret key is d. The "encryption" of a message $a \in \mathbb{Z}_q$ is defined as:

$$E(\text{pk}, a) = (g^r, h^{r+a}) \quad \text{where } r \xleftarrow{\text{R}} \mathbb{Z}_q$$

Show that given $E(\text{pk}, a)$ Alice can use her secret key d to compute h^a. Note that this system is not really an encryption system since Alice cannot fully recover the plaintext a from a given ciphertext.

d. Explain how to instantiate the protocol above using the system from part (c). Describe exactly what message Alice would send to Bob, how Bob would respond, and how Alice would learn the comparison result.

Problem 5. Challenge response from weak PRFs. Let $F : K \times X \to \{0,1\}^n$ be a PRF where the input space X is large (so that $1/|X|$ is negligible). We say that F is weakly secure if the adversary cannot distinguish F from a truly random function $f : X \to \{0,1\}^n$ when the adversary only sees the evaluation of $F(k,\cdot)$ at *random* points. That is, the adversary is given pairs $(x_i, f(x_i))$ for $i = 1,\ldots,q$ where all x_i are chosen at random in X, and is supposed to distinguish the case where f is a truly random function from the case where f is a random instance of the PRF.

a. Write the precise security game defining a weakly secure PRF and define the advantage function for this game. Say that F is weakly secure if no efficient adversary can win the game with non-negligible advantage.

b. Let $F : K \times X \to \{0,1\}^n$ be a secure PRF (in the standard sense) and define

$$F'(k,x) = \begin{cases} k & \text{if } x = 0 \\ F(k,x) & \text{otherwise} \end{cases}$$

b.1. Is F' a secure PRF in the standard sense? If so explain why, if not give an attack.

b.2. Is F' a weakly secure PRF? If so explain why, if not give an attack.

c. Suppose we use a weakly secure PRF in the standard MAC-based challenge-response protocol. That is, we directly use the weakly secure PRF as the MAC in this protocol. Is the resulting authentication protocol secure against active attacks?

Hint: Give an example weakly secure PRF for which there is an active attack on the resulting challenge-response protocol.

Note: it is possible to design an authentication protocol secure against active attacks from a weakly secure PRF, but we will leave that as a puzzle for another time.