Problem set 2

This assignment is due **at 10:00pm ET** on **Thursday, October 13, 2022**.

Please make note of the following instructions:

- Remember that your solutions must be submitted on Gradescope. Please sign-up for 6.1600 Fall 2022 on Gradescope, with the entry code `577GE7`, using your MIT email.
- We require that the solution to the problems is submitted as a PDF file, **typeset on LaTeX**, using the template available on the course website (`https://61600.csail.mit.edu/2022/`). Each submitted solution should start with your name, the course number, the problem number, the date, and the names of any students with whom you collaborated.

Problem 2-1. Message Signing [30 points]

Let $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme with message space $\{0,1\}^k$ (where k is the security parameter), and let H be a seeded hash function with domain $\{0,1\}^*$ and range $\{0,1\}^k$. Consider the new signature scheme $(\mathsf{Gen}', \mathsf{Sig}', \mathsf{Ver}')$, with message space $\{0,1\}^*$, defined via the following "hash-then-sign" paradigm:

- Gen' runs Gen to generate a pair (sk, vk) and samples a seed s for H. It outputs $sk' = (sk, s)$ and $vk' = (vk, s)$.
- Sig' takes as input a secret key $sk' = (sk, s)$ and a message M, and outputs a $\mathsf{Sig}(sk, H_s(M))$, i.e., it signs the hashed message $H_s(M)$.
- Ver', given the verification key $vk' = (vk, s)$, a message M, and a signature σ, outputs 1 if and only if $\mathsf{Ver}(vk, H_s(M), \sigma) = 1$.

(a) Suppose that $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ is secure (existentially against adaptive chosen message attack) then which of the following properties of H do we need to ensure that $(\mathsf{Gen}', \mathsf{Sig}', \mathsf{Ver}')$ is also secure?

1. One-wayness.
2. Target collision resistance
3. Collision resistance.

[15 points]

(b) Suppose that H is modeled as a random oracle. What is the minimal security notion we need of $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ to ensure that $(\mathsf{Gen}', \mathsf{Sig}', \mathsf{Ver}')$ is secure existentially against adaptive chosen message attacks:

1. Security for any message (existential security) against adaptive chosen message attacks.
2. Security for random messages against adaptive chosen message attacks.
3. Security for any message (existential security) against random message attacks.
4. Security for random messages against random message attacks.

We encourage the students to refer to the lecture notes for the definitions of these security notions. [15 points]

Problem 2-2. Pseudo-Random Functions [40 points]

Let F be a pseudorandom function (PRF) that takes messages in $\{0,1\}^n$ to messages in $\{0,1\}^n$.

(a) Propose a way to use F to construct a PRF that takes messages in $\{0,1\}^n$ to messages in $\{0,1\}^{2n}$. [10 points]

(b) We wish to use F to construct a PRF that takes messages in $\{0,1\}^{2n}$ to messages in $\{0,1\}^{2n}$. Suppose the key to F is also in $\{0,1\}^n$.

Below are four proposals of such a PRF, where $x_0, x_1, K, K_0, K_1 \in \{0,1\}^n$ and where we use $||$ to denote concatenation. Notice that the constructions 1, 3, and 4 use a key in $\{0,1\}^n$ whereas the second construction uses a key in $\{0,1\}^{2n}$.

1. $G_1(K, x_0||x_1) = F(K, x_0)||F(K, x_1)$.
2. $G_2(K_0||K_1, x_0||x_1) = F(K_0, x_0)||F(K_1, x_1)$.
3. $G_3(K, x_0||x_1) = F(K', 0^n)||F(K', 1^n)$, where $K' = F(F(K, x_0), x_1)$
4. $G_4(K, x_0||x_1) = F(F(K, x_0), x_1)||F(F(K, x_0), x_1 \oplus 1^n)$.

Only one of the above four proposals is a secure PRF. Which one is the secure one? For each of the three others, show an attack that distinguishes it from a truly random function (recall the definition of a PRF given in the lecture). [30 points]

Problem 2-3. Device Synchronization via an Untrustworthy Server [30 points]

This problem explores the security properties of the photo-sharing application that you will construct in Lab 2. In that application, a users' devices communicate via an untrustworthy server. For this question, assume that all devices are using an error-free implementation of the Lab-2 specification. **For all problem parts except part (d), assume that the server is malicious**.

For each true/false question, state whether the statement is true or false. Then give a construction or attack that proves your claim.

(a) **True or false:** Alice and Bob are friends. If Alice adds a photo p, Bob will *eventually* receive photo p when he calls `get_friend_photos(alice)`. [5 points]

(b) Say that Alice's devices correctly use a MAC to authenticate all the log entries that they exchange. That is, her devices correctly use a MAC to prevent the server from tampering with the log entries.

True or false: In this setting, the *server* can use the MAC tags to authenticate messages from Alice. [5 points]

(c) Alice has three devices: a laptop, a tablet, and a phone. She adds these three devices to her account with the photo-sharing service. Later, Alice (on her laptop) issues a `revoke_device` command to remove her tablet from her account.

True or false: After Alice's laptop issues the `revoke_device` command and the server acknowledges its receipt, Alice's phone will never accept a new photo from her tablet. [5 points]

(d) Assume for this part that the server is honest. Alice has d devices. Each device holds a set of n photos of b bits each. The devices want to determine whether they hold the same unordered set of photos. (If two devices hold the photos in different orders, they should conclude that they hold the same set.) Give a protocol for checking this while minimizing the amount of communication between the devices. Your protocol should use $\ll nb$ bits of communication. [15 points]