Introduction to Cryptography and Software Security
Problem Set 2: MACs and Hash Functions

Due date: 24/4/2017

Instructions.

- You are allowed to rely on any statement that we proved in class, unless you are explicitly asked to prove it, and as long as you state it clearly and accurately.
- Justify your answers with formal proofs.
- **On-line submissions only! Hard copies will not be accepted.** Please make sure that scanned submissions are readable (unreadable submissions will not be accepted).

Problem 1 (20%). Let F be a pseudorandom function such that for any $n \in \mathbb{N}$ and $k \in \{0,1\}^n$ it holds that $F_k : \{0,1\}^n \to \{0,1\}^n$. Show that each of the following MAC schemes is insecure. In each case, the scheme's key-generation algorithm, Gen, outputs a uniform key $k \in \{0,1\}^n$, and we let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.

1. To authenticate a message $m = m_1 || \cdots || m_d$, where $m_i \in \{0,1\}^n$ for every $i \in \{1, \ldots, d\}$, output $t = F_k(m_1) \oplus \cdots \oplus F_k(m_d)$.
2. To authenticate a message $m = m_1 || \cdots || m_d$, where $m_i \in \{0,1\}^{n/2}$ for every $i \in \{1, \ldots, d\}$, output $t = F_k(\langle 1 \rangle || m_1) || \cdots || F_k(\langle d \rangle || m_d)$.
3. To authenticate a message $m \in \{0,1\}^n$, sample a uniform $r \leftarrow \{0,1\}^n$, and output (r, t), where $t = F_k(r) \oplus F_k(m)$.

Problem 2 (0%). Let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a secure MAC scheme, where the algorithm Gen produces uniformly distributed keys, and the algorithm Mac is deterministic (as a function of the key and the message). Is Mac necessarily a pseudorandom function? Prove your answer.

[Note that in class we proved the opposite implication: Any pseudorandom function (whose output is "not too short") can be used to construct such a MAC scheme.]

Problem 3 (0%). Let $\mathcal{H} = (\mathsf{Gen}, H)$ be a collision-resistant hash family. Let Vrfy be the algorithm that on input (s, m, t) outputs 1 if $H_s(m) = t$ and outputs 0 otherwise. Is $\Pi = (\mathsf{Gen}, H, \mathsf{Vrfy})$ necessarily a secure MAC scheme? Prove your answer.

Problem 4 (20%). Let $G : \{0,1\}^* \to \{0,1\}^*$ be a length-doubling pseudorandom generator, and let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be the following MAC scheme:

- The algorithm Gen on input 1^n uniformly samples and outputs $k \leftarrow \{0,1\}^n$.
- The algorithm Mac on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$ outputs $t = G(k||m)$.
- The algorithm Vrfy on input a key $k \in \{0,1\}^n$, a message $m \in \{0,1\}^n$ and a tag $t \in \{0,1\}^{4n}$, outputs 1 if $t = G(k||m)$ and outputs 0 otherwise.

Is Π necessarily a secure MAC scheme? Prove your answer.

Problem 5 (20%). Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Mac}_1, \mathsf{Vrfy}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Mac}_2, \mathsf{Vrfy}_2)$ be two MAC schemes, for which it is known that at least one is secure (both schemes are guaranteed to be *correct*). The problem is that you do not know which one is secure, and which one may not be.
Show how to combine them into one MAC scheme that is guaranteed to be secure as long as at least one of them is secure. Prove the security of your proposal.

Problem 6 (20%). Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Mac}_1, \mathsf{Vrfy}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Mac}_2, \mathsf{Vrfy}_2)$ be two MAC schemes, for which it is known that at least one is secure (both schemes are guaranteed to be *correct*). The problem is that you do not know which one is secure, and which one may not be.

Assuming that the algorithms Mac_1 *and* Mac_2 *are both deterministic* (as functions of the key and the message), prove that the following MAC scheme $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is guaranteed to be secure:

- The algorithm Gen on input 1^n samples $k_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $k_2 \leftarrow \mathsf{Gen}_2(1^n)$ independently, and outputs the key $k = (k_1, k_2)$.
- The algorithm Mac on input a key $k = (k_1, k_2)$ and a message m outputs $t = \mathsf{Mac}_1(k_1, m) \oplus \mathsf{Mac}_2(k_2, m)$.
- The algorithm Vrfy on input a key $k = (k_1, k_2)$, a message m and a tag t, outputs 1 if $t = \mathsf{Mac}(k, m)$ and outputs 0 otherwise.

Problem 7 (20%). Let $\mathcal{H}^{(1)} = \left(\mathsf{Gen}^{(1)}, H^{(1)}\right)$ and $\mathcal{H}^{(1)} = \left(\mathsf{Gen}^{(2)}, H^{(2)}\right)$ be two hash families, for which it is known that at least one is collision resistant. The problem is that you do not know which one is collision resistant, and which one may not be.
Show how to combine them into one hash family that is guaranteed to be collision resistant as long as at least one of them is collision resistant. Prove the security of your proposal.

Problem 8 (0%). Recall the "hash-and-authenticate" approach that we have seen in class for constructing a MAC scheme Π for arbitrary-length messages given any MAC scheme $\widehat{\Pi}$ for fixed-length messages and any collision-resistant hash family (Gen_H, H). Prove the security of Π based on the security of $\widehat{\Pi}$ and (Gen_H, H).

[Instructions: Recall that for any adversary $\mathcal{A}$ it holds that $\Pr\left[\mathsf{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right] \leq \Pr[\mathsf{Collision}] + \Pr\left[\mathsf{MacForge}_{\Pi,\mathcal{A}}(n) = 1 \ \wedge \ \neg\mathsf{Collision}\right]$. Prove that each of these two terms must be negligible.]