Cryptography ENEE/CMSC/MATH 456: Homework 3

Due by beginning of class on 3/6/2024.

1. Say $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is a secure MAC, and for $k \in \{0,1\}^n$, the tag-generation algorithm Mac_k always outputs tags of length $t(n)$. Prove that t must be super-logarithmic or, equivalently, that if $t(n) = O(\log n)$ then Π cannot be a secure MAC.
   Hint: Consider the probability of randomly guessing a valid tag.

2. Consider the following MAC for messages of length $\ell(n) = 2n - 2$ using a pseudorandom function F: On input a message $m_0||m_1$ (with $|m_0| = |m_1| = n - 1$) and key $k \in \{0,1\}^n$, algorithm Mac outputs $t = F_k(0||m_0)||F_k(1||m_1)$. Algorithm Vrfy is defined in the natural way. Is $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ secure? Prove your answer.

3. Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticated fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)
   (a) To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$.
   (b) To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{n/2}$, compute $t := F_k(\langle 1 \rangle||m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle||m_\ell)$.

4. Show that appending the message length to the end of the message before applying basic CBC-MAC does not result in a secure MAC for arbitrary length messages.

5. Let F be a keyed function that is a secure (deterministic) MAC for messages of length n. (Note that F need not be a pseudorandom function.) Show that basic CBC-MAC is not necessarily a secure MAC (even for fixed-length messages) when instantiated with F.

6. Show a CPA-secure private-key encryption scheme that is unforgeable but is not CCA secure.

7. Generalize the Merkle-Damgard construction for any compression function that compresses by at least one bit. You should refer to a general input length ℓ' and general output length ℓ (with $\ell' > \ell$).

8. Consider defining a MAC by $\mathsf{Mac}_k(m) = H^s(k||m)$ where H is a collision-resistant hash function. Show that this is not a secure MAC when H is constructed via the Merkle-Damgard transform. As usual, assume that the hash key s is publicly known.

9. Assume collision-resistant hash functions exist. Show a construction of a fixed-length hash function (Gen, h) that is not collision resistant, but such that the hash function (Gen, H) obtained from the Merkle-Damgard transform to (Gen, h) is collision resistant.