Exercise 3 – Introduction to Cryptography 89-656

Due Date: November 25, 2018

November 19, 2018

Exercise 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.

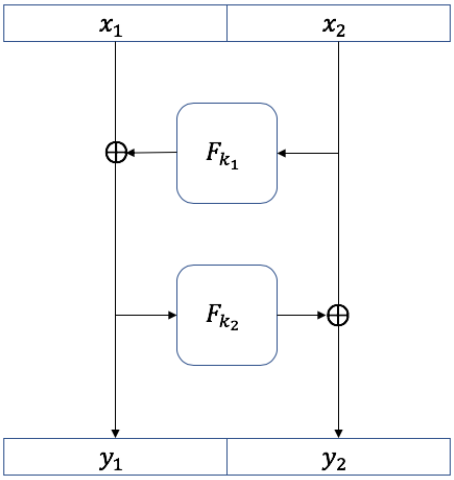
Exercise 2: Let F be a pseudorandom function. Is the following MAC for messages of length $2n$ secure? The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1 \| m_2$ with $|m_1| = |m_2| = n$, compute the tag $\langle F_k(m_1), F_k(F_k(m_2)) \rangle$. Prove your answer.

Exercise 3: Show that the basic CBC-MAC construction is *not* secure when used to authenticate messages of different lengths (but are of lengths that are a multiple of the block length).

Exercise 4:

1. Prove or refute: the following encryption scheme is CPA-secure: Let $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a secure MAC with tags of length n. Encrypt a message $m \in \{0,1\}^n$ by choosing a random $r \in \{0,1\}^n$ and outputting $(r, \mathsf{Mac}_k(r) \oplus m)$.

2. Let $F : \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Consider the function $F2 : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined by a 2-round Feistel network where in the first round the round function uses F_{k_1}, and in the second round it uses F_{k_2}, where k_1, k_2 are independent keys. Formally, we define $F2(x_1 \| x_2) = (F_{k_1}(x_2) \oplus x_1,\ F_{k_2}(F_{k_1}(x_2) \oplus x_1) \oplus x_2)$; see the figure below. Prove or refute: $F2$ is a pseudorandom function.



Exercise 5: Provide formal definitions for second (or target) pre-image resistance and pre-image resistance. Formally prove that any hash function that is collision resistant is second pre-image resistant. (For preimage resistance consider random inputs of length $2n$. For second (target) preimage resistance, consider a game where first a message x is output by the adversary, then s is chosen.)

Exercise 6: For each of the following modifications to the Merkle-Damgård transform, determine whether the result is collision resistant or not. If yes, explain where the proof differs from the proof we saw in class; if not, show an attack.

1. Modify the construction so that the input length is not included at all (i.e., output z_B and not $z_{B+1} = h^s(z_B \| L)$).
2. Modify the construction so that instead of outputting $z = h^s(z_B \| L)$, the algorithm outputs $z_B \| L$.
3. Instead of using an IV, just start the computation from x_1. That is, define $z_1 := x_1$ and then compute $z_i := h^s(z_{i-1} \| x_i)$ for $i = 2, \ldots, B+1$ and output z_{B+1} as before.
4. Instead of using a fixed IV, set $z_0 := L$ and then compute $z_i := h^s(z_{i-1} \| x_i)$ for $i = 1, \ldots, B$ and output z_B.

Exercise – for fun (not to be handed in): This is a true story. A reliable website explaining how to carry out CBC encryption discussed the problem that since the IV is needed for decryption, it is impossible to choose it randomly, since if it is random, then how will the decryptor know it (the author seems to not have thought of the idea of sending the IV as part of the ciphertext). As a result, the recommendation by the author was to use the key as the IV. In general, the recommendation for encryption was to use plain CBC mode AES-128 and PKCS5 padding, and with $IV = k$. Explain in words how a padding-oracle attack can be used in this case in order to retrieve the secret key k. Write pseudocode for the attack. Assume that you have an encryption oracle and a padding oracle (where the padding oracle returns YES or NO, depending if the provided ciphertext has correct padding or not).