

CSE 794 Homework 4

Due: Tuesday, February 17 by class time

1. Let $\{f_k : \{0,1\}^n \rightarrow \{0,1\}^n, k \in \{0,1\}^n\}$ be a family of n -bit pseudorandom functions.

Construct a MAC scheme for messages of length $2n$ as follows. The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1 \parallel m_2$ with $|m_1| = |m_2| = n$, let the tag be $\langle f_k(m_1), f_k(m_2) \rangle$. Show that this scheme is insecure (i.e., *not* existentially unforgeable) against chosen-message attacks?

2. The same as Question 1, but the tag is now $\langle f_k(m_1), f_k(f_k(m_2)) \rangle$.

3. Show that the following variant of CBC-MAC (without padding) is insecure.

- Divide the input message m into blocks:

$$m = m_1 \parallel m_2 \parallel \dots \parallel m_s, \text{ where } |m_i| = n.$$

- Apply the block cipher E to m in CBC mode using key k :

$$c_0 \leftarrow \text{IV (typically } 0^n)$$

$$\text{for } i \leftarrow 1 \text{ to } s \text{ do } c_i \leftarrow E_k(c_{i-1} \oplus m_i)$$

- Let c_s (the last cipher block) be the tag.

4. Let $\{h_s : \{0,1\}^* \rightarrow \{0,1\}^n, s \in \{0,1\}^n\}$ be a family of collision-resistant hash functions.

Define $\tilde{h}_s(x) = h_s(h_s(x))$. Is $\{\tilde{h}_s : s \in \{0,1\}^n\}$ necessarily a family of collision-resistant hash functions. Justify your answer.