Modern Cryptography
Bachelor Computer Science, University of Amsterdam, 2017/18
TEACHER: Christian Schaffner, TA: Jan Czajkowski, Christian Majenz

Problem Set 7

We will work on the following exercises together during the work sessions on Tuesday, 3 October 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

Problem 1: Short tags

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.

Problem 2: A simple MAC from a PRF

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.

Problem 3: Modified CBC-MAC

Prove that the following modifications of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages):

1. Mac outputs all blocks $t_1, \ldots, t_\ell$, rather than just t_ℓ. (Verification only checks whether t_ℓ is correct.)

2. A random initial value is used each time a message is authenticated. That is, $t_0 \in \{0,1\}^n$ is chosen uniformly at random rather than being fixed to 0^n, and the tag is $\langle t_0, t_\ell \rangle$. Verification is done in the natural way.

Problem 4: A randomized variable-length MAC from a PRF

Let F be a pseudorandom function. Show that the following MAC is insecure for variable-length messages. Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.

To authenticate a message $m = m_1 \| \ldots \| m_\ell$, where $m_i \in \{0,1\}^{n/2}$, choose a uniform $r \leftarrow \{0,1\}^n$, compute $t := F_k(r) \oplus F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle \| m_\ell)$ and let the tag be (r, t).

★ Problem 5: Appending the message length in CBC-MAC

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.