Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 7

Exercise 7-1 Suppose F is a pseudo-random function.

Define a fixed-length message-authentication code $(\mathsf{Gen}, \mathsf{MAC})$ as follows: The key generation function Gen takes as argument the security parameter n and returns a random key of length n. The function MAC takes as input the key of length n and a message m of length $2n-2$. It splits the message m into two halves m_0 and m_1 and outputs $F_k(0m_0) \parallel F_k(1m_1)$.

Is this scheme secure? Prove your answer.

Exercise 7-2 Recall from the lecture that CBC-MAC computes a message-authentication code from a message consisting of L equal-sized blocks $m = m_1m_2 \dots m_L$ using a pseudo-random function F as follows:

$$
\begin{aligned}
t_0 &= F_k(L) \\
t_{i+1} &= F_k(t_i \oplus m_i) \quad \text{for } i = 0, \dots, L-1.
\end{aligned}
$$

The message-authentication code for m is t_L.

Show that this scheme becomes insecure if the code is taken to be $t_0 \parallel t_1 \parallel \dots \parallel t_L$ instead.

Exercise 7-3 Consider the following changes to the Merkle-Damgård construction. In which of these cases does the construction still produce a collision-resistant hash function?

a) The message length L is not appended in the last step, i.e. the output is z_B instead of $h_s(z_B \parallel L)$.

b) Instead of letting z_0 be a word of all zeros, one chooses some random word IV and sets $z_0 := IV$. Then one computes z_B as before, i.e. $z_i = h_s(z_{i-1} \parallel x_i)$ for $i = 1 \dots, B$, and returns $IV \parallel h_s(z_B \parallel L)$ as the final output.

c) One completeley omits the inital value z_0 and starts computation with $z_1 := x_1$. This means that one computes $z_i = h_s(z_{i-1} \parallel x_i)$ for $i = 2 \dots, B$, and then returns $h_s(z_B \parallel L)$ as the output.