Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 4

Exercise 3-3 was not finished in Tutorial 3 and will be discussed in Tutorial 4.

Exercise 4-1 Let $F\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function (PRF).

a) Let y be a fixed word. Show that $F'_k(x) = F_k(x) \oplus y$ is then also a PRF.

b) Show that $F'_k(x) = F_k(0x) \,\|\, F_k(x1)$ is not a PRF, where $\|$ denotes concatenation. Construct a distinguisher and argue why it has a non-negligible advantage.

Exercise 4-2 Let $F\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Let $G\colon \{0,1\}^n \times \{0,1\}^{n+1}$ be a pseudorandom generator.

The following three definitions of $\mathsf{Enc}_k(m)$ define encryption schemes. Which of them has indistinguishable encryptions in the presence of an eavesdropper? Which is CPA-secure?

a) To encrypt $m \in \{0,1\}^{n+1}$, choose $r \in \{0,1\}^n$ uniformly at random and output $r \,\|\, (G(r) \oplus m)$.

b) A message $m \in \{0,1\}^n$ is encrypted to $m \oplus F_k(0^n)$.

Hint: Recall the construction of a semantically secure cryptosystems from a pseudorandom generator from the lecture.

c) A message $m \in \{0,1\}^{2n}$ is encrypted by splitting it into two parts m_1 and m_2 of equal length, choosing $r \in \{0,1\}^n$ uniformly at random and letting the ciphertext be $r \,\|\, (m_1 \otimes F_k(r)) \,\|\, (m_2 \otimes F_k(r+1))$.