Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2018/12/11

Solution

Cryptography – Questionnaire 1

Name: _____

Matr.: _____

"One-liners"

Exercise 1.1 **2P**

Let k be a positive integer and let $K_1 := \{0,1,2,3\}^k$ and $K_2 := \{A \mid A \subseteq \{1,\dots,k\}, |A| = 5\}$. Give closed-form expressions for $|K_1|$ and $|K_2|$.

Answer: $|K_1| = 4^k$. $|K_2| = \binom{k}{5}$.

Exercise 1.2 **2P**

Often, encryption schemes (ES) are based on block ciphers which can only process inputs of a fixed size l (called the block length). If we want to process messages $m \in \{0,1\}^*$ of arbitrary length, we need to pad the message to a multiple of l in a suitable way. Briefly describe one possible way to do so. (We want to be able to recover m in the end!)

Answer: use $m||10^r$ with r minimal s.t. we get a multiple of l

Exercise 1.3 **2P**

Briefly state the meaning of the *sufficient keyspace principle*:

Answer: The keyspace should be large enough such that exhaustive search becomes infeasible.

Exercise 1.4 **2P**

Name a major disadvantage of publice-key schemes compared to private-key schemes.

Answer: Public-key schemes are slower than private-key schmemes in general.

Exercise 1.5 **2P**

Name one ES from the lecture that satisfies $\mathsf{Enc}_k = \mathsf{Dec}_k$ for a given key k.

Answer: One-time pad.