Prof. Dr. Jasmin Blanchette
Dr. Martin Desharnais-Schäfer
Dr. Michael Kirsten
Elisabeth Lempa

Ludwig-Maximilians-Universität München
Institut für Informatik
Discussion on 22.10.2025
Homework due on 29.10.2025 at 16:00

Exercise Sheet 2 in

Scientific and Technical English for Computer Scientists

The exercise sheets consist of in-class exercises and homework. The in-class exercises take place in the second half of the lecture time slots. The homework, which is optional and ungraded, can be submitted via the "Homework" section in Moodle. The homework is subject to peer review.

Unless indicated otherwise, generative artificial intelligence assistants such as ChatGPT may be used, as long as you acknowledge how you use them as specified by the Institute's policy on plagiarism.[1] However, you may not use such tools to generate peer reviews for you. In addition, we strongly recommend that you do not use them to generate entire solutions, since this would defeat the purpose of the exercises.

In-class exercise 2-1 ***Curse of Knowledge*** Start by reading the following definition adapted from Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, Second Edition, CRC Press, 2014:

> A *message authentication code* (or *MAC*) consists of three probabilistic polynomial-time algorithms (Gen, Mac, Vrfy) such that:
>
> - The *key-generation algorithm* Gen takes as input the security parameter 1^n and outputs a key k with $|k| \geq n$.
> - The *tag-generation algorithm* Mac takes as input a key k and a message $m \in \{0,1\}^*$, and outputs a tag t. Since this algorithm may be randomized, we write this as $t \leftarrow \mathsf{Mac}_k(m)$.
> - The deterministic *verification algorithm* Vrfy takes as input a key k, a message m, and a tag t. It outputs a bit b, with $b = 1$ meaning *valid* and $b = 0$ meaning *invalid*. We write this as $b := \mathsf{Vrfy}_k(m, t)$.
>
> It is required that for every n, every key k output by $\mathsf{Gen}(1^n)$, and every $m \in \{0,1\}^*$, it holds that $\mathsf{Vrfy}_k(m, \mathsf{Mac}_k(m)) = 1$.
>
> If there is a function ℓ such that for every k output by $\mathsf{Gen}(1^n)$, algorithm Mac_k is only defined for messages $m \in \{0,1\}^{\ell(n)}$, then we call the scheme a *fixed-length MAC for messages of length* $\ell(n)$.

Identify the background knowledge required to understand this definition for a novice to the field of cryptography.

[1] `https://www.medien.ifi.lmu.de/lehre/Plagiate-IfI.pdf`

In-class exercise 2-2 ***From Title to Ideas*** Together with your colleagues, you invented, implemented, and evaluated a new sorting algorithm. You now want to write and submit a 15-page paper to a renowned international conference in the field of algorithms.

a) Choose a title for your paper. It may be catchy, informative, or double-barreled.

b) Write your paper's table of contents, and allocate a page budget to every section and subsection.

c) In each section and subsection, write down at least two bullet points standing in for the future content.

Homework 2-3 ***From Title to Ideas, then to Sketch*** Dijkstra's algorithm solves the single-source shortest-paths problem on a positive-weighted directed graph. Sketch a 15-page paper describing and evaluating the algorithm by following these steps:

a) Choose a title for your paper. It may be catchy, informative, or double-barreled.

b) Write your paper's table of contents, and allocate a page budget to every section and subsection.

c) In each section and subsection, write down at least two bullet points standing in for the future content.

d) Refine your bullet points by adding descriptions of the examples, definitions, code excerpts, tables, and figures that will appear in each section and subsection.