Reference group meeting 21/09-23

Attendees: Tjerand, Nimer, Espen, Diderik, Simen

Topics that we discussed at the meeting:

- Lectures
  - Good pace in the lectures and everything is understandable
  - Can maybe go a bit more in detail on certain topics
  - Add references to the course books in the slides, e.g., to relevant chapters in Serious Cryptography for more details
  - It is fun and interesting to discuss problems together in class

- Exercises class / lab
  - Most students get help in due course but sometimes it's busy
  - Next year, we might need two TAs to help a larger class
  - Probably needs extra capacity in the end of November

- Exercises
  - Maybe split the weekly problems into two parts next year?
    - Half of it done by October and the rest in December
    - Could make individual agreements for those who prefer more frequent deadlines and more structure
  - Quite a bit of work, especially on randomness. A bit less later on.
  - Evaluate the number of exercises that are mandatory vs bonus
  - Add hints to (some of) the problems to make them a bit easier
  - Emphasize that we give points for partial solutions and understanding even if the problems are not completely solved
  - Pen & paper problems. What is a "break"?
    - We will explain in more detail what an attack means in the given setting and what kind of leakage we expect.
  - Cryptohack problems. What is expected?
    - Write down a paragraph or two about how you understand the problem and what you need to do to solve it, even if you are not able to solve all of it and find the flag
  - ChipWhisperer Lab. What is expected?

        - Document the code you wrote to complete the lab exercises and share the graphs you plotted. Summarize what you did and what you learned
    - Time estimates of weekly problems: total time spent by showing up to the exercises class during the full semester (it will not always be enough time to solve the problems of the current topic in 1-2 weeks, but during all sessions during the semester)

- Final project
    - You can choose a topic on your own that is related to the course description, and we have suggested some examples for you.
    - The aim is to read academic papers and understand some problems or solutions we must deal with in practice. The project can involve programming or experiments if relevant.

- Recordings
    - We will not record any lectures in this course since the lectures are interactive and we want to have joint discussions.
    - We will anyway not record lectures this year since it is the first time we teach this course, and it will need some adjustments.
    - We have ambitions to create recordings of special topics that we record in an isolated setting outside of lectures in case students cannot attend a lecture or want to recap. But not this year.