

# TTM4135 reference group meeting on 18-03-2026

**Attendees:** Tjerand, Emil, Adelin, Mina, and Gianluca

## **Topics that we discussed:**

- Lectures:
  - Slides are useful when working on problems and preparing for the exam
- Exercises lectures / sheets:
  - The staff are creating a few more PQ problems since this topic is new
  - The exercises and solutions are useful for practising to the exam
- Quizzes:
  - Useful for practicing and get an overview of the weekly content
  - The reference group think we should continue with quizzes next year also
  - Could make deadlines on Fridays, independent of the lecture hours
- Ed Discussion
  - ED is kind of spammy, so it is possible to miss emails, e.g., if it goes to a different mailbox automatically, depending on the email client used
  - Mail is possible through Blackboard, but leads to duplicated work
  - Will use Canvas next year, which might be a better solution in general
  - Make it more explicit what tool we will use for announcements
- Lab:
  - First two parts are quite easy, and some more work on the third part
  - Okay to solve things when discussing with other groups and the TAs
  - Challenges with Certbot certificates using ECC instead of RSA in part 2, and then creating problems in part 3 when downgrading the connection
  - Should make a clearer remark in the assignment that part 3 requires some exploration outside of the instructions
  - Make a remark that there are different names for cipher suites across different browsers and tools, e.g. configuration on Apache servers
  - Possible to include PQC in part 1 and 2 of the assignment next year, would also make the discussion more interesting
  - Make the discussion part clearer about the expectations, and maybe tie it more closely to the content covered in the lectures
  - There might not be enough work for groups of 4 people. 2-3 instead?
  - Students are mostly stopping by the lab to ask for help or get milestones approved. It is okay this year, but not ideal that they do not have a dedicated place to work. Use Sahara next year when it is available.
  - It is likely not needed to offer TA help 9-17 every day, but at least a handful of slots throughout the week in a lab where students can work.

- Roughly 12 hours of work to complete the milestones over three weeks, including collecting some information for the report. Maybe 20 h total?
- Exam:
  - Reminder about the exam lecture; date, time, lecture hall, content
  - Exam structure will be similar to earlier years, and we will share information about this in advance of the exam