

Reference group meeting TTM4205 on 23-09-2024

Attendees: Tjerand, Caroline, Emil, Jiaqi, Daniel, Adrian

Topics we discussed:

- *Lectures*
 - We make slides available, and encourage you to check out the books and references for more details or to read up if you miss out on lectures
 - We will continue with interactive discussions during the lectures and never record them. We received a lot of positive feedback about the interactivity
 - The lectures are helpful for exercises and tied to the weekly exercise topics
 - (Long-term goal: publish videos and more detailed notes of the content)
- *Exercise class / lab*
 - CW tutorial was essential (it is still possible to get help during lab sessions)
 - Next year: CW intro and Linux/Mac + Windows installation over two sessions
 - More clear marking of equipment at the lab (extra boards led to confusion)
 - Lab-sessions: first half in B2 and second in the CRYPTO-LAB going forward
 - There is a dead link in the installation guide (it will be updated asap)
- *Assignments*
 - Weekly problems
 - Varying progress among the students so far, but it is going well
 - We will facilitate structured discussion about the most recent lectures during the exercise class whenever we change topics
 - The late deadline is both good and bad: it allows for extra freedom and flexibility but also often leads to being less prioritized than other more urgent deadlines during the semester; student responsibility
 - Recall: there is roughly one month between the submission deadline and the last portion of new content covered in the lectures
 - ChipWhisperer lab
 - Most people are up and running with the first experiments
 - You do not have to conduct the labs in the given order (but you should do the intermediate tasks in order in each of the lab exercises)
 - We encourage you to use the CRYPTO-LAB more going forward; you are currently the only group of students that have access to it
 - You are allowed to discuss the exercises and help each other, but everything you submit must be your own work

- We only have 17 boards for the RSA-lab, so you are allowed to conduct this in smaller groups (as specified in the lab assignment)
- Technical essay
 - We will send a reminder to form groups in October, but you should start thinking about it already, and you can find groups through Ed
- *Ed Forum*
 - We have prioritized detailed replies over quick replies so far
 - Please use it more actively and help each other out with answers