Reference group meeting 31/10-23

Attendees: Tjerand, Espen, Diderik, Simen, Jonathan

Topics that we discussed at the meeting:

- Lectures
    - Like questions, problems and discussions in pairs
    - Practical examples to showcase are appreciated

- Exercises class / lab
    - Good capacity and get enough help
    - Same people showing up each week

- Exercises
    - ChipWhisperer
        - Maybe skip the first lab because of setup issues
        - Problems with the RSA exercises (evaluate)
        - Add information in the exercise about runtimes
        - Add hints about parameters and adjustments
        - Solve the first exercise in the exercise class next year
    - The last CryptoHack problems are a bit easier than earlier
        - Tie the ECDSA lecture more closely to the CH problem
        - Evaluate the hardness of each problem after submission
    - Text problems
        - They usually have some kind of "trick" or "insight"
        - Add hints or clarify based on handed in solutions