Topics for the exam in DM854

The topics are:

1. Information-theoretic security
2. Block ciphers and AES, plus modes of operation
3. Hash functions
4. RSA
5. Primality testing and factoring
6. Discrete logarithm problem and systems assuming its hardness
7. Goldwasser-Micali encryption and bit commitment
8. Secret sharing schemes, especially Shamir's
9. Zero-knowledge proofs

The exam will take place on January 23 and 24.

In order to be allowed to take the exam, there is a requirement that you turn in a page with your name, along with your preferences for when you would like your exam during those two days. If you have a very good reason for your preference, please state it on this page you upload to Blackboard (another exam one of those days is a much better excuse that having trouble getting out of bed in the morning). The deadline for uploading this page is 23:59 on December 28. You will receive a list through Blackboard of the order students in DM854 will take the exam, along with a starting time for the first student to draw a question. These lists cannot be used to exactly calculate an exam time since some students may not show up. If a student is not there, the next student on the list who is present will be taken. When there are no more students ready to be taken, the external examiner may leave, so show up plenty early to make sure you are examined. Two hours before your expected exam time is probably safe enough. The first first few students should show up at the start time.

You will draw a topic from the list of topics listed above. You will have about 30 minutes to prepare your presentation. During this time you may use the book and your notes. You may also make short notes that will help you to organize your presentation, but that will have no other technical content. The exam will take about 30 minutes per person. Prepare your presentation so that it takes about 10 to 15 minutes. Make sure you cover the most important ideas from your topic, though this may mean that you need to skip some details. Your presentation may be interupted with questions or cut short to go on to other topics. Towards the end of the 30 minute period, you will typically also be asked short questions not related to the material you talked about. No slides are allowed.

You may do your presentation in either Danish or English (though Danish is recommended if you are Danish).

Come ask Joan if you have any questions.