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 31. The sign-up list cannot be used to exactly calculate an exam time since some students may not show up. Since, as for all classes, the external examiner is only paid for students who are examined, not for sitting and waiting, 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.

You will draw a topic from the list of topics listed above. You will have 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).