

Topics for the exam in DM830

The topics are:

1. Symmetric encryption and message confidentiality
2. Public-key cryptography and message authentication
3. Key distribution and user authentication
4. Transport-level security
5. Wireless network security
6. Electronic mail security
7. IP security
8. Intruders
9. Malicious software
10. Firewalls

The exam will take place on June 20 and June 21. The first will draw a question at 8:30 each day. The sign-up sheets for the order in which students will be examined will be sent around in class on May 30. If you do not put your name on then, Lone will put it on for you. 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 interrupted 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).