

Topics for the exam in DM71

The exam will take place on June 7 and June 8. The sign-up sheets for the order in which students will be examined are already in the secretaries' office. Sign up well before the exam. 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.

When it is your turn, you will draw one out of the following topics, which correspond to sections or parts of chapters in the textbook. You will have 30 minutes to prepare a 15-20 minutes presentation about that topic. It is likely that you will be interrupted with questions during your presentation. After your presentation, you will be asked additional questions from one or several of the other topics as well.

The topics are:

1. Encryption algorithms: symmetric and asymmetric
2. Uses of encryption: hash functions, digital signatures, and certificates
3. Malicious code
4. Controls against program threats
5. Access control in operating systems
6. User authentication
7. Security models
8. Threats in networks
9. Network security controls
10. Firewalls and intrusion detection systems
11. Administering security
12. Mathematics of cryptography
13. Database Security