Department of Mathematics
(incl. Math. Statistics)

Stockholm
University

Syllabus

for course at advanced level

Mathematics of cryptography
Krypteringsmatematik

7.5 Higher Education Credits
7.5 ECTS credits

Course code:	MM7018
Valid from:	Autumn 2010
Date of approval:	2010-05-17
Department	Department of Mathematics (incl. Math. Statistics)
Main field:	Mathematics/Applied Mathematics
Specialisation:	A1N - Second cycle, has only first-cycle course/s as entry requirements

Decision

This syllabus was approved by the Board of the Faculty of Science at Stockholm University on 17 May 2010.

Prerequisites and special admittance requirements

Admission to the course requires knowledge equivalent to 60 credits in mathematics, where Linear algebra II, 7.5 credits (MM5004) and Mathematical analysis III, 7.5 credits (MM5001) or equivalent, are included.

Course structure

Examination code	Name	Higher Education Credits
F718	Mathematics of cryptography	7.5

Course content

The course covers the modern methods of cryptography, which form the basis for secure electronic communication, and methods to decrypt them. The focus will be on mathematical foundations in number theory, algebraic geometry and statistics, and how these are used in cryptography. The course is of interest for those who work with security aspects in electronic communication, but also for those who want to see one of the more spectacular modern applications of mathematics.

Learning outcomes

After the course, students are expected to be able to:
• account for a number of cryptographic systems, such as RSA and ElGamal, cryptography with elliptic curves and the different methods to decrypt these
• account for essential techniques and results in elementary number theory, combinatorics, information theory, statistics and algebraic geometry and their relevance for applications in cryptography.

Education

Instruction consists mainly of lectures. There can be home assignments and group seminars. Participation in seminars, if there are any, is compulsory. In the event of special circumstances, the examiner may, after consultation with the teacher concerned, grant a student exemption from the obligation to participate in certain compulsory instruction.

Forms of examination

a. The course is examined as follows: Knowledge assessment takes the form of written and/or oral examination. Written and/or oral presentations of group assignments and exercises.

b. Grades are assigned according to a seven-point goal-related grading scale:

A = Excellent
B = Very good
C = Good
D = Satisfactory
E = Sufficient
Fx = Fail (more work required before credit can be awarded)
F = Total fail

c. The grading criteria will be distributed at the beginning of the course.

d. To be awarded a pass, the minimum grade E is required together with approved home assignments, seminars and computer labs (if these are used).

e. Students who fail an ordinary examination are entitled to sit additional examinations as long as the course is offered. There is no restriction on the number of examinations. Examinations also include other obligatory elements of the course. Students who have passed an examination may not resit it in order to achieve a higher grade. Students who have failed on two occasions are entitled to request the appointment of a different examiner for the next examination. Any such request must be made to the departmental board.

Interim

Students may request that the examination be conducted in accordance with this course plan even after it has ceased to be valid. However, this may not take place more than three times over a two year period after course instruction has ended. Requests must be made to the departmental board.

Misc

The course is given as an individual course.

Required reading

Course literature is decided by the departmental board and described thereafter in an appendix to the course plan.