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:	MM7029
Valid from:	Spring 2021
Date of approval:	2020-08-17
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 August 2020.

Prerequisites and special admittance requirements

Admission to the course requires knowledge equivalent to

1, Mathematics II - Algebra and combinatorics, 7,5 credits (MM5013) and Programming Techniques for Mathematicians, 7,5 credits (DA2004).

or

2. A Bachelor's degree including at least 60 credits in mathematics, mathematical statistics, or computer science.

Also required is knowledge equivalent to Swedish upper secondary course English B.

Course structure

Examination code	Name	Higher Education Credits
LABO	Computer exercises	2.5
TENT	Theory	5

Course content

The course treats basic notions in cryptography and the mathematical problems, with associated mathematical theory, that are the basis for asymmetric cryptographical applications such as RSA (both as cryptosystem and digital signature), DH, El Gamal, ECDH, ECDSA and Miller-Rabin. Different algorithms (to solve these mathematical problems) are studied with a focus on their complexity. Algorithms that are treated include fast powering, Shank's baby-step giant-step, Pohlig-Hellman, Pollard's p-1, QS, index calculus, Pollard's rho och Lenstra's ECM.

Learning outcomes

After the course the student should be able to

Part 1, Theory, 5 ECTS credits:

-explain basic notions in cryptography,
-explain the mathematical problems and the associated mathematical theory that underlies the asymmetric cryptographic applications treated in the course, and to solve problems using this theory,
-explain the algorithms that are treated in the course, and account for and prove their complexity,

Part 2, Computer exercises, 2.5 ECTS credits:
-implement the simpler of these algorithms using mathematical software, and to analyze their complexity in practice.

Education

Instruction consists of lectures, exercises and computer exercises.

The course is offered in English.

Forms of examination

a. The course is examined in the following manner:

Assessment of module 1, Theory, takes place through a written exam.
Assessment of module 2, Computer exercises, takes place through written reports.

A passing final grade requires passing grades on all included parts.

The examiner can decide on adapted or alternative examination formats for students with disabilities.

The examination will be conducted in English.

b. The course has no compulsory instruction.

c. Grading: The course's final grade is set according to a seven-point criterion-referenced scale:
A = Excellent
B = Very good
C = Good
D = Satisfactory
E = Adequate
Fx = Failed, some additional work is required
F = Failed, much additional work is required

Grades of module 1, Theory, will be set according to a seven-point criterion-referenced scale.

Grades of module 2, Computer exercises, will be set according to a two-point grading scale: fail (U) or pass (G).

d. The course's grading criteria are handed out at the start of the course.

e. Students who receive a failing grade on a regular examination are allowed to retake the examination as long as the course is still provided. The number of examination opportunities is not limited. Other mandatory course elements are equated with examinations. A student who has received a passing grade on an examination may not retake the examination to attain a higher grade. A student who has failed the same examination twice is entitled to have another examiner appointed, unless there are special reasons to the contrary. Such requests should be made to the department board. Under normal circumstances, the course includes at least three examination opportunities per academic year the course is offered. For the academic years that the course is not offered, at least one examination opportunity is offered.

f. There is no possibility to improve the grade Fx to a pass grade in this course.

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. The provision also applies in the case of revisions of the course syllabus and revisions of the required reading.

Limitations

The course may not be included in a degree together with the course Mathematics of cryptography (MM7018).

Required reading

The required reading is decided by the departmental board and published on the Department of Mathematics' website at least 2 months before the start of the course.