**DIT250 Cryptography, 7.5 credits**

Cryptography, 7,5 högskolepoäng  
*Second Cycle*

---

**Confirmation**

This course syllabus was confirmed by The IT Faculty Board on 2006-11-17 and was last revised on 2017-06-16 by Department of Computer Science and Engineering to be valid from 2017-08-20, autumn semester of 2017.

*Field of education:* Science 100%  
*Department:* Computer Science and Engineering

---

**Position in the educational system**

The course is offered within the framework of several degree programmes. The course is also a single subject course at University of Gothenburg.

The course can be part of the following programmes: 1) Computer Science, Master's Programme (N2COS), 2) Applied Data Science Master's Programme (N2ADS), 3) Bachelor's Programme in Mathematics (N1MAT) and 4) Computer Science, Bachelor's Programme (N1COS)

**Main field of studies**  
**Specialization**

- Computer Science-Secure and Depend Compr Systems  
  - A1N, Second cycle, has only first-cycle course/s as entry requirements
- Computer Science  
  - A1N, Second cycle, has only first-cycle course/s as entry requirements

---

**Entry requirements**

To be eligible for the course the student should have successfully completed courses corresponding to 60 hec in the subject of Computer Science or Mathematics, including:

- 7.5 hec in discrete mathematics (for example DIT980 Discrete Mathematics for Computer Scientists, the sub-course Introductory Algebra of MMG200
Mathematics 1, or equivalent);
• 7.5 hec in programming (for example DIT142 Functional Programming, DIT012 Imperative Programming with Basic Object-orientation, MVG300 Programming with MatLab or equivalent).

Applicants must prove knowledge of English: English 6/English B or the equivalent level of an internationally recognized test, for example TOEFL, IELTS.

Learning outcomes
After completing the course the student is expected to be able to:

Knowledge and understanding
• summarize the main goals of cryptography and illustrate this with several examples of how cryptographic services are integrated in current applications, both in software and hardware.

Competence and skills
• describe goals and design principles for, and common structures of, secret key primitives such as block and stream ciphers and message authentication codes
• identify, analyse and explain various forms of attacks based on improper usage of primitives, modes or protocols;
• explain how basic public key primitives can be defined based on the difficulty of mathematical problems such as the discrete logarithm problem or factoring, and analyse variants of these systems;
• explain the various roles of hash functions as parts of other cryptographic primitives and protocols, and the requirements this places on hash functions.

Judgement and approach
• exemplify when various notions of security, such as information-theoretic, computational, provable and practical security, are applicable and describe the security guarantees provided;
• explain basic key management techniques in both secret key and public key cryptography.

Course content
Basic goals of cryptography (confidentiality, authentication, non-repudiation).
management, authentication and other services.

Sub-courses
1. **Written exam** (*Tentamen*), 6 higher education credits
   Grading scale: Pass with Distinction (VG), Pass (G) and Fail (U)
2. **Assignments** (*Inlämningsuppgifter*), 1.5 higher education credits
   Grading scale: Pass (G) and Fail (U)

**Form of teaching**
The course is composed of lectures as well as exercise sessions, and assignments.

*Language of instruction*: English

**Assessment**
The course is examined by home assignments done individually and a written exam done individually in an examination hall.

If a student, who has failed the same examined component twice, wishes to change examiner before the next examination, a written application shall be sent to the department responsible for the course and shall be granted unless there are special reasons to the contrary (Chapter 6, Section 22 of Higher Education Ordinance)

In cases where a course has been discontinued or has undergone major changes, the student shall normally be guaranteed at least three examination occasions (including the ordinary examination) during a period of at least one year from the last time the course was given.

**Grades**
The grading scale comprises: Pass with Distinction (VG), Pass (G) and Fail (U).
To be awarded Pass for the whole course, the student must pass both the exam and the home assignments. For the grade Pass with Distinction the student must pass the home assignments and get the grade Pass with Distinction on the exam.

**Course evaluation**
The course is evaluated through meetings both during and after the course between teachers and student representatives. Further, an anonymous questionnaire is used to ensure written information. The outcome of the evaluations serves to improve the
course by indicating which parts could be added, improved, changed or removed.

**Additional information**
It is recommended to have followed a course in statistics and/or Probability theory beforehand.

The course is a joint course together with Chalmers.