UNIVERSITY OF GOTHENBURG

# DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

## DIT352 Cryptography, 7.5 credits

Kryptografi, 7,5 högskolepoäng

*Second Cycle*

---

### Confirmation

This course syllabus was confirmed by Department of Computer Science and Engineering on 2023-11-13 to be valid from 2024-09-02, autumn semester of 2024.

*Field of education:* Science 100%
*Department:* Department of 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) Computer Science, Bachelor's Programme (N1COS) and 4) Bachelor's Programme in Mathematics (N1MAT)

| *Main field of studies* | *Specialization* |
|---|---|
| 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 90 credits in the subject of Computer Science or Mathematics, including:

- 7.5 credits in algebra or discrete mathematics (covering topics: modular arithmetic, and elementary probability theory)
- 7.5 credits in programming

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*

- Recognize well-established cryptosystems and identify settings where they can be used to improve the security of a given system
- Demonstrate knowledge of principles behind provable security
- Understand the theoretic foundations of cryptography

*Competence and skills*

- Describe goals and design principles for, and common structures of, several cryptographic primitives and proof systems
- Identify, analyse and explain various forms of attacks based on improper usage of primitives, modes of operation, or protocols
- Reproduce rigorous proofs of security

*Judgement and approach*

- Exemplify when various notions of security are applicable and describe the security guarantees provided
- Apply the acquired knowledge in new situations.

## Course content

- Basic and advanced goals of cryptography (confidentiality, authentication, anonymity, zero-knowledge)
- Symmetric key cryptography: block ciphers, design principles and examples, modes of operation, message authentication codes.
- Public key cryptography: key exchange, asymmetric ciphers, signatures. Attack models and security notions.
- Cryptographic Protocols: secret sharing, zero-knowledge proofs.

*Sub-courses*

1. **Written hall exam** *(Skriftlig salstentamen),* 6 credits
   Grading scale: Pass with distinction (5), Pass with credit (4), Pass (3) and Fail (U)
2. **Assignments** *(Inlämningsuppgifter),* 1.5 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 or in groups, and a written exam done individually in an examination hall.

If a student, who has failed the same examined element on two occasions, wishes to change examiner before the next examination session, such a request is to be submitted to the department in writing and granted unless there are special reasons to the contrary (Chapter 6, Section 22 of Higher Education Ordinance).

In the event that a course has ceased or undergone major changes, students are to be guaranteed at least three examination sessions (including the ordinary examination session) over a period of at least one year, though at most two years after the course has ceased/been changed. The same applies to work experience and VFU, although this is restricted to just one additional examination session.

**Grades**
The grading scale comprises: Pass with distinction (5), Pass with credit (4), Pass (3) and Fail (U).
In order to pass the course both the assignments and the written hall examination have to be approved. The grade for the entire course will be determined by the written hall 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**
The course is a joint course together with Chalmers.

Course literature to be announced the latest 8 weeks prior to the start of the course.

The course replaces the course DIT250, 7.5 credits. The course cannot be included in a degree which contains DIT250. Neither can the course be included in a degree which is based on another degree in which the course DIT250 is included.