1 Name, Scope and Level of the Course
The course is provided by the University of Skövde and is named Practical Cryptology A1N. It comprises 7.5 credits and is on advanced level. The level of progression of the course is A1N.

2 Objectives
After completed course the student should be able to:

- describe and critically reflect upon cryptographic primitives and algorithms,
- describe and critically reflect upon formal models for security,
- apply cryptographic tools in practical scenarios, and
- implement and critically evaluate cryptographic systems.

3 Course Content
Security is a fundamental requirement in modern day computing and cryptography is a fundamental building block in ensuring confidentiality and integrity. This course presents cryptographic primitives and functions as well as formal models of security. An overview of common terms such as elliptic curves, blockchain, digital watermarking and steganography is also presented. Further, aspects related to the implementation and usage of crypto systems are discussed and the students will implement and review a cryptosystem chosen on their own based on their background.

4 Forms of Teaching
The teaching comprises lectures and laboratory sessions.

The teaching is conducted in English.

5 Examination
The course is graded A (Excellent), B (Very good), C (Good), D (Satisfactory), E (Sufficient) or F (Fail).

Registration of examination results:

<table>
<thead>
<tr>
<th>Name of examination</th>
<th>Credits</th>
<th>Grading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupervised examination</td>
<td>4.5</td>
<td>A/B/C/D/E/F</td>
</tr>
<tr>
<td>Written assignment</td>
<td>3</td>
<td>G/U</td>
</tr>
</tbody>
</table>

1 Determines the final grade of the course.

Students with a permanent disability who have been approved for special educational support may be offered adapted or alternative examinations.

6 Admission Requirements
A Bachelor’s degree (equivalent to a Swedish kandidatexamen) within the fields of informatics or computer science or the equivalent.

A further requirement is proof of skills in English equivalent of studies at upper secondary level in Sweden, known as English course 6 / English course B (or the equivalent). This is normally demonstrated by means of an internationally recognized test, e.g. IELTS, TOEFL.
7 Subject, Main Field of Study and Disciplinary Domain

The course forms a part of the academic subject area of Informatics. The course is a part of the main field of study in Informatics at the University of Skövde. The disciplinary domain of the course is Technology.

Every course at the University of Skövde belongs to a subject. The division of subjects is used for follow-up and quality assurance. A main field of study is an area in which a degree can be awarded. Disciplinary domain is a division which is used by the government for the allocation of resources for studies at basic level and advanced level.

8 Approval of Course and Course Syllabus

The course was approved by the Curriculum Committee for Informatics on 4 October 2018. This course syllabus was approved by the Curriculum Committee for Informatics on 4 October 2018. It is valid from 1 July 2019.

9 Overlapping with Another Course

This course cannot constitute a part of a degree also containing a course the content of which is totally or partly equivalent to the content of this course.

10 Additional Information

Further information will be available on the university’s website before a course is given.

National and local regulations for higher education are available on the university’s website.

Upon completion of the course there will be a follow-up. The main purpose of this follow-up is to contribute to improvements of the course. The students’ experiences and views constitute one of the criteria for the follow-up and are gathered by means of course evaluations. The students will be informed of the results of the follow-up and any decisions regarding actions that are to be taken.

11 Course Literature and Other Educational Materials


Scientific articles indicated on the course website.