Course and Examination Fact Sheet: Autumn Semester 2024

7,377: Introduction to Cryptography and Cybersecurity

ECTS credits: 4

Overview examination/s

(binding regulations see below)
decentral - Written work, Digital, Group work group grade (40%)
Examination time: Term time
decentral - Written work, Digital, Group work group grade (60%)
Examination time: Term time

Attached courses

Timetable -- Language -- Lecturer
7,377,1.00 Introduction to Cryptography and Cybersecurity -- English -- Newman Marc , Horlemann Anna-Lena

Course information

Course prerequisites

Basic mathematical knowledge from the assessment level.

It is advantageous to have preliminary knowledge in programming, e.g. with R or Python. However, we will have a quick introduction to programming with SAGE during the course, and with some motivation it is easily possible to acquire these skills in the first weeks of the semester, also without previous programming knowledge.

Learning objectives

At the end of the course the students will know how digital information is represented in binary or hexadecimal form, and how it can be encrypted and decrypted. The students know the difference between symmetric and asymmetric cryptosystems and where they can or should be applied. The strengths and weaknesses of these systems are known, and the students know some important security issues that should be considered when implementing the respective algorithms. With these cryptographic basics the technical functionality of blockchains can be understood and explained.

Course content

In the modern age of digitization, cyber security is a central and important topic for any organization. Cyber attacks happen on a daily base - both from private hackers or larger criminal organizations. The dangers can be manifold: leakage of sensitive data, loss of intellectual property, tampering of data, scandals and loss of reputation, and many more. Therefore, any management should understand the dangers of cyber attacks to their organization and come up with a suitable cyber security strategy. To be able to do so, a basic understanding of the underlying cryptographic algorithms and mathematical foundations is crucial. Acquiring this basic understanding is the focus of this class.

The main topics we will treat are:

- Historic ciphers (from Caesar cipher to the Enigma machine)
- Classical attacks (brute force, known plaintext attacks, chosen plaintext attacks)
- Symmetric encryption (DES/AES)
- Asymmetric encryption (Diffie-Hellman algorith, RSA)
- Hash functions (password storage)
- Digital signatures
- Blockchains (bitcoin)

To understand how these cryptographic instances work we will need some mathematical tools regarding prime numbers and polynomials. However, we will keep the abstract mathematics at a minimum and spend more time on implementing these algorithms with the help of the open-source software SAGE (www.sagemath.org). Moreover, we will discuss the possible mistakes and problems when using (or not using) the above algorithms, and talk about known public scandals in this regard.

Course structure and indications of the learning and teaching design

There will be one class of two hours each week. The lectures will deal with cryptographic algorithms, their mathematical foundations, as well as their applications. The lectures will be complemented by homework exercises.

Course literature

Lecture notes, online resources. Further literature recommendations will be announced on StudyNet.

Additional course information

--

Examination information

Examination sub part/s

1. Examination sub part (1/2)

Examination modalities

Examination type	Written work
Responsible for organisation	decentral
Examination form	Written work
Examination mode	Digital
Time of examination	Term time
Examination execution	Asynchronous
Examination location	Off Campus
Grading type	Group work group grade
Weighting	40%
Duration	--

Examination languages

Question language: English
Answer language: English

Remark

Regular homework exercises

Examination-aid rule

Free aids provision

Basically, students are free to choose aids. Any restrictions are defined by the faculty members in charge of the examination under supplementary aids.

Supplementary aids

--

2. Examination sub part (2/2)

Examination modalities

Examination type	Written work
Responsible for organisation	decentral
Examination form	Written work
Examination mode	Digital
Time of examination	Term time
Examination execution	Asynchronous
Examination location	Off Campus
Grading type	Group work group grade
Weighting	60%
Duration	--

Examination languages

Question language: English
Answer language: English

Remark

Final term paper

Examination-aid rule

Free aids provision

Basically, students are free to choose aids. Any restrictions are defined by the faculty members in charge of the examination under supplementary aids.

Supplementary aids

--

Examination content

- There will be weekly homework exercises that may be solved in groups of up to three participants. The exercises may involve programming in SAGE.
- For the final term paper, every group of three/four participants will work on an advanced topic in cybersecurity. The paper may focus on theory or applications of cybersecurity, as well as political or legal aspects of it.

Examination relevant literature

Lecture notes, made available via Canvas, or online resources chosen by the participants.

Please note

Please note that only this fact sheet and the examination schedule published at the time of bidding are binding and takes precedence over other information, such as information on StudyNet (Canvas), on lecturers' websites and information in lectures etc.
Any references and links to third-party content within the fact sheet are only of a supplementary, informative nature and lie outside the area of responsibility of the University of St.Gallen.

Documents and materials are only relevant for central examinations if they are available by the end of the lecture period (CW51) at the latest. In the case of centrally organised mid-term examinations, the documents and materials up to CW 42 are relevant for testing.

Binding nature of the fact sheets:

- Course information as well as examination date (organised centrally/decentrally) and form of examination: from bidding start in CW 34 (Thursday, 22nd August 2024);
- Examination information (supplementary aids, examination contents, examination literature) for decentralised examinations: in CW 12 (Monday, 18 March 2024);
- Examination information (supplementary aids, examination contents, examination literature) for centrally organised mid-term examinations: in CW 42 (Monday, 14 October 2024);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised examinations: Starting with de-registration period in CW 45 (Monday, 04 November 2024).