University of St.Gallen

Course and Examination Fact Sheet: Autumn Semester 2020

7,377: Introduction to Cryptography and Cybersecurity

ECTS credits: 4

Overview examination/s

(binding regulations see below)
Decentral - Group examination paper (all given the same grades) (60%)
Examination time: term time
Decentral - Group examination paper (all given the same grades) (40%)
Examination time: term time

Attached courses

Timetable -- Language -- Lecturer
7,377,1.00 Introduction to Cryptography and Cybersecurity -- Englisch -- 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 week 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

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. Moreover, there will be an introduction to programming in SAGE in the beginning of the semester.

Course literature

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

Additional course information

In the case of the President's Board having to implement new directives due to the SARS-CoV-2 pandemic in AS2020, the course information listed above will be changed as follows:

- The course is conducted online via the platform Zoom;
- The recordings of the course are available for 30 days;
- The lecturer informs via StudyNet on the changed implementation modalities of the course.

The examination information listed below would be changed as follows:

- There are no changes necessary to the examination information.

Examination information

Examination sub part/s

1. Examination sub part (1/2)

Examination time and form

Decentral - Group examination paper (all given the same grades) (60%)
Examination time: term time

Remark

Final term paper

Examination-aid rule

Term papers

Term papers must be written without anyone else's help and in accordance with the known quotation standards, and they must contain a declaration of authorship which is a published template in StudentWeb.

The documentation of sources (quotations, bibliography) has to be done throughout and consistently in accordance with the chosen citation standard such as APA or MLA.

For papers in law, the legal standard is recommended (by way of example, cf. FORSTMOSER, P., OGOREK R. et SCHINDLER B., Juristisches Arbeiten: Eine Anleitung für Studierende, newest edition respectively, or according to the recommendations of the Law School).

The indications of the sources of information taken over verbatim or in paraphrase (quotations) must be integrated into texts in accordance with the precepts of the applicable quotation standard, while informative and bibliographical notes must be added as footnotes (recommendations and standards can be found, for example, in METZGER, C., Lern- und Arbeitsstrategien, newest edition respectively.

For any work written at the HSG, the indication of the page numbers is mandatory independent of the chosen citation standard. Where there are no page numbers in sources, precise references must be provided in a different way: titles of chapters or sections, section numbers, acts, scenes, verses, etc.

Supplementary aids
--

Examination languages
Question language: English
Answer language: English

---

2. Examination sub part (2/2)

Examination time and form
Decentral - Group examination paper (all given the same grades) (40%)
Examination time: term time

Remark
Homework exercises

Examination-aid rule
Term papers

Term papers must be written without anyone else's help and in accordance with the known quotation standards, and they must contain a declaration of authorship which is a published template in StudentWeb.

The documentation of sources (quotations, bibliography) has to be done throughout and consistently in accordance with the chosen citation standard such as APA or MLA.

For papers in law, the legal standard is recommended (by way of example, cf. FORSTMOSER, P., OGOREK R. et SCHINDLER B., Juristisches Arbeiten: Eine Anleitung für Studierende, newest edition respectively, or according to the recommendations of the Law School).

The indications of the sources of information taken over verbatim or in paraphrase (quotations) must be integrated into texts in accordance with the precepts of the applicable quotation standard, while informative and bibliographical notes must be added as footnotes (recommendations and standards can be found, for example, in METZGER, C., Lern- und Arbeitsstrategien, newest edition respectively.

For any work written at the HSG, the indication of the page numbers is mandatory independent of the chosen citation standard. Where there are no page numbers in sources, precise references must be provided in a different way: titles of chapters or sections, section numbers, acts, scenes, verses, etc.

Supplementary aids
--

Examination languages
Question language: English
Answer language: English

Examination content

- There will be regular 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, online resources

University of St.Gallen

Please note

Please note that only this fact sheet and the examination schedule published at the time of bidding are is 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, 20 August 2020);
- Examination information (regulations on aids, examination contents, examination literature) for decentralised examinations: in CW 42 (Monday, 12 October 2020);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised mid-term examinations: in CW 42 (Monday, 12 October 2020);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised examinations: two weeks before the end of the registration period in CW 44 (Thursday, 29 October 2020).