Course and Examination Fact Sheet: Spring Semester 2019

4,584: Basics of Cyber Security - from Safe Passwords to Blockchains

ECTS credits: 3

Overview examination/s

(binding regulations see below)
Decentral - Group examination paper (all given the same grades) (50%)
Decentral - Group examination paper (all given the same grades) (50%)

Attached courses

Timetable -- Language -- Lecturer
4,584,1.00 Basics of Cyber Security - from Save Passwords to Blockchains -- 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. However, we will have a quick introduction to programming with SAGE during the course, and with some motivation it is possible to acquire these skills in the first week of the semester, also without previous programming knowledge.

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.

In the end we will discuss some legal issues regarding cyber security, and show which techniques are currently recommended as secure by governmental organizations.

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

--

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) (50%)

Remark

Homework

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.
- The documentation of sources (quotations, bibliography) has to be done throughout and consistently in accordance with the APA or MLA standards. The indications of the sources of information taken over verbatim or in paraphrase (quotations) must be integrated into the text 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. (2017), Lern- und Arbeitsstrategien (12th ed., Cornelsen Schweiz).
- For any work written at the HSG, the indication of the page numbers both according to the MLA and the APA standard is never optional.
- 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.
- For papers in law, the legal standard is recommended (by way of example, cf. FORSTMOSER, P., OGOREK R. et SCHINDLER B. (2018, Juristisches Arbeiten: Eine Anleitung für Studierende (6. Auflage), Zürich: Schulthess, or the recommendations of the Law School).

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) (50%)

Remark

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.
- The documentation of sources (quotations, bibliography) has to be done throughout and consistently in accordance with the APA or MLA standards. The indications of the sources of information taken over verbatim or in paraphrase (quotations) must be integrated into the text 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. (2017), Lern- und Arbeitsstrategien (12th ed., Cornelsen Schweiz).
- For any work written at the HSG, the indication of the page numbers both according to the MLA and the APA standard is never optional.
- 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.
- For papers in law, the legal standard is recommended (by way of example, cf. FORSTMOSER, P., OGOREK R. et SCHINDLER B. (2018, Juristisches Arbeiten: Eine Anleitung für Studierende (6. Auflage), Zürich: Schulthess, or the recommendations of the Law School).

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 cyber security. The paper may involve programming in SAGE, but can also focus on applications of cyber security, as well as political or legal aspects of it.

Examination relevant literature

Lecture notes, online resources

Please note

We would like to point out to you that this fact sheet has absolute priority over other information such as StudyNet, faculty members' personal databases, information provided in lectures, etc.When will the fact sheets become binding?

- Information about courses and examination time (central/decentral and grading form): from the start of the bidding process on 24 January 2019
- Information about decentral examinations (examination-aid rule, examination content, examination relevant literature): after the 4th semester week on 18 March 2019
- Information about central examinations (examination-aid rule, examination content, examination relevant literature): from the start of the enrolment period for the examinations on 08 April 2019

Please look at the fact sheet once more after these deadlines have expired.