University of St.Gallen

Course and Examination Fact Sheet: Autumn Semester 2023

7,850: Cyber Security

ECTS credits: 6

Overview examination/s

(binding regulations see below)
decentral - Written work, Digital, Individual work individual grade (20%)
Examination time: Term time
central - Analog written examination, Analog, Individual work individual grade (80%, 120 Min.)
Examination time: Lecture-free period

Attached courses

Timetable -- Language -- Lecturer
7,850,1.00 Cyber Security -- English -- Mitrokotsa Katerina
7,850,2.00 Cyber Security: Exercises -- English -- Kaluderovic Novak , Cheng Nan , Tomy Jenit

Course information

Course prerequisites

There are no required pre-requisites for students accepted in the master program. We assume that the students are familiar with basic notions of TCP/IP and basic notions programming for this course.

Learning objectives

- Knowledge of basic cryptographic primitives and protocols.
- Competence on arguing about the security of cryptographic primitivesand protocols.
- Knowledgeofvulnerabilities against existing schemes and how they can be avoided.
- Comprehension ofthe difficulties involved in employing security protocols and tools to build secure systems.
- Competencesin employing appropriate security mechanisms, primitives and protocols to safeguard systems andcommunications.

Course content

Security is becoming increasingly important to guarantee reliable data storage, communication and electronic transactions. This is an introductory course to cybersecurity. The main goal is to provide the students with means to reason about cybersecurity and get familiar with cryptographic primitives and protocols. More precisely, it aims to provide to the students: an overview of basic information and network security concepts and methods as well as a good knowledge of some commonly used network and cryptographic tools and protocols. The students will get a sound understanding of theory and implementation. We will describe attacks against existing schemes and how they can be avoided. The students will gain an appreciation of the difficulties involved in employing security protocols and tools to build secure systems.

Course structure and indications of the learning and teaching design

The course consists of weekly sessions (2-hourlecture and 2-hour exercise sessions). The content of the exercises will closely build upon the lecture content. Lecturenotesviatheprovidedslidesandexercises.

The lectures will cover following topics:

- Introduction to Security: Defining security goals and policies
- Introduction to Security: Historic ciphers, OTP
- Cryptographic primitives for confidentiality: Secret key and public key cryptography (i)

- Cryptographic primitives for confidentiality: Secret key and public key cryptography (ii)
- Key distribution and management
- Public key infrastructure
- Cryptographic primitives for data integrity:hash functions
- Message authentication codes and digital signatures.
- Security Protocols: key agreement protocols, SSL/TLS
- Security Protocols: Secure Multi Party Computation
- Security Protocols: identification protocols, intro to Zero Knowledge Proofs
- Computer/Network security: secure network architectures, Intrusion detection and prevention systems

Course literature

- Cryptography and Network Security, 7th Ed. Stallings
- lecture notes provided via slides
- additional material provided during the lectures and exercise sheets.

Additional course information

Prof. Dr. Katerina Mitrokotsa was appointed as full professor and chair of Cybersecurity at the School of Computer Science of the University of St. Gallen in August 2020. Before joining the University of St. Gallen, she was a professor at Chalmers University of Technology in Sweden. She has served as visiting professor at Tokyo Institute of Technology (Japan), ETHZ and Vrije Universiteit (Netherlands) as well as a visiting scholar at Harvard University (USA). The main aim of her research is to safeguard communication technologies and resolve security and privacy issues in current communications; with a special focus on provably secure and efficient cryptographic primitives and cryptographic protocols.

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	Individual work individual grade
Weighting	20%
Duration	--

Examination languages

Question language: English
Answer language: English

Remark

--

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

Literature and content covered during the course (lectures and exercise sessions).

---

2. Examination sub part (2/2)

Examination modalities

Examination type	Analog written examination
Responsible for organisation	central
Examination form	Written exam
Examination mode	Analog
Time of examination	Lecture-free period
Examination execution	Synchronous
Examination location	On Campus
Grading type	Individual work individual grade
Weighting	80%
Duration	120 Min.

Examination languages

Question language: English
Answer language: English

Remark

--

Examination-aid rule

Closed Book

The use of aids is prohibited as a matter of principle, with the exception of pocket calculator models of the Texas Instruments TI-30 series and, in case of non-language exams, bilingual dictionaries without any handwritten notes. Any other aids that are admissible must be explicitly listed by faculty members in the paragraph entitled “Supplementary aids” of the course and examination fact sheet; this list is exhaustive.

Procuring any aids, as well as ensuring their working order, is the exclusive responsibility of students.

Supplementary aids

No supplementary aid.

Examination content

The examination content includes the lecture material (slides), the indicated sections in the textbook as well as the material covered in the exercise sessions.

Examination relevant literature

Lecturenotesviatheprovidedslidesandexercises.CryptographyandNetworkSecurity,7thEd.Stallings.

University of St.Gallen

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, 24 August 2023);
- Examination information (supplementary aids, examination contents, examination literature) for decentralised examinations: in CW 42 (Monday, 16 October 2023);
- Examination information (supplementary aids, examination contents, examination literature) for centrally organised mid-term examinations: in CW 45 (Monday, 06 November 2023);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised examinations: two weeks before the end of the de-registration period in CW 45 (Monday, 06 November 2023).