Course and Examination Fact Sheet: Spring Semester 2021

9,015: Cryptography

ECTS credits: 6

Overview examination/s
(binding regulations see below)
Central ‑ Written examination (100%, 120 mins.)
Examination time: inter‑term break

Attached courses
Timetable ‑‑ Language ‑‑ Lecturer
9,015.1.00 Cryptography ‑‑ Englisch ‑‑ Mitrokotsa Aikaterini

Course information

Course prerequisites
Understanding of basic mathematical concepts (e.g. what is a probability).

Learning objectives

Cryptography is becoming increasingly important to enhance security in connection with data storage, communication and electronic transactions. This course aims to provide to the students:

- an overview of basic cryptographic concepts and methods
- a good knowledge of some commonly used cryptographic primitives and protocols
- a sound understanding of theory and implementation, as well as limitations and vulnerabilities of existing cryptographic primitives and protocols.
- an appreciation of the difficulties involved in employing cryptographic tools to build secure systems

Course content

The course is composed of four main parts and covers the following material:

- 1st Part ‑ Secret Key Cryptography: We will analyse how secret key cryptography is employed to achieve confidentiality. We will cover a small selection of classical cryptosystems, including substitution and transposition ciphers that were historical examples of secret key cryptography. We will describe how one time pad works, what are the stream ciphers and how block ciphers work. We will discuss components used in constructions of block ciphers (e.g. feistel networks) and describe concrete constructions e.g. AES, DES.
- 2nd Part ‑ Public Key Cryptography: We will discuss the notion of public key cryptography, see well known public key cryptosystems (textbook RSA, El Gamal). Describe attacks against existing schemes and how they can be avoided.
- 3rd Part ‑ Data Integrity: We will discuss how we can achieve data integrity using hash functions, message authentication codes and public key signatures. We will see vulnerabilities of existing schemes and how we can secure them.
- 4th Part ‑ Cryptographic protocols: We will describe how we employ cryptographic primitives in order to design cryptographic protocols between two or more parties to achieve identification, key agreement and secure multi‑party computation.

Course structure

The course is composed of lectures (2 hours per week) and some practical exercise sessions (2 hours per week). Some assignments will also be given to the students in order to test their comprehension on the concepts taught.
Course literature

Lecture notes via the provided slides.


Additional course information

In the case of the President’s Board having to implement new directives due to the SARS-CoV-2 pandemic in FS2021, the course information listed above will be changed as follows:

- The course is conducted online via the platform zoom.
- The recordings of the course will be saved. Extracts of the lectures will also be shared in short videos. Information will be provided later.

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 (1/1)

Examination time and form
Central - Written examination (100%, 120 mins.)
Examination time: inter-term break

Remark
--

Examination-aid rule
Extended Closed Book
The use of aids is limited; any additional aids permitted are exhaustively listed under "Supplementary aids". Basically, the following is applicable:

- At such examinations, all the pocket calculators of the Texas Instruments TI-30 series and mono- or bilingual dictionaries (no subject-specific dictionaries) without hand-written notes are admissible. Any other pocket calculator models and any electronic dictionaries are inadmissible.
- In addition, any type of communication, as well as any electronic devices that can be programmed and are capable of communication such as notebooks, tablets, mobile telephones and others, are inadmissible.
- Students are themselves responsible for the procurement of examination aids.

Supplementary aids
No supplementary material/documentation is required for the solution of the examination.

Examination languages
Question language: English
Answer language: English

Examination content

The examination will cover all material discussed during the lectures and focusing on the following parts:

- Secret key cryptography
- Public key cryptography
Data Integrity
Cryptographic protocols.

**Examination relevant literature**
All lectures slides and indicated sections in the textbook is part of the examination literature as well as the exercises covered in the course.

---

**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 (CW21) at the latest. In the case of centrally organised mid-term examinations, the documents and materials up to CW 12 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 04 (Thursday, 28 January 2021);
- Examination information (regulations on aids, examination contents, examination literature) for decentralised examinations: in CW 12 (Monday, 22 March 2021);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised mid-term examinations: in CW 12 (Monday, 22 March 2021);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised examinations: two weeks before the end of the registration period in CW 14 (Thursday, 8 April 2021).