h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Modulbeschreibung

Cryptography

Module numbers: 41.4936 [PVL 41.4937]

Language: english

Study programme:
Dualer Master 2021 - Katalog T: Theorieorientierte Module
Master 2021 - Katalog T: Theorieorientierte Module
Dualer Master 2013 - Katalog T: Theorieorientierte Module
JIM 2013 - Elective Catalogue T
Master 2013 - Katalog T: Theorieorientierte Module
JIM 2006 - Courses
Master 2006 - Katalog T: Theorieorientierte Module
Master 2006 - Vertiefung IS: IT-Sicherheit
MN Data Science 2022/2016 - Katalog M-I_I: Allgemeine Wahlpflicht Informatik

Type of course: V+Ü+P = Lecture+Exercise+Practical

Weekly hours: 2+1+1

Credit Points: 6

Exam: written exam

PVL (e.g. Practical): not graded (ungraded practical course and participation in the exercises)

Required knowledge: Desirable: Cryptology from the Bachelor's programme

Learning objectives:
After this course the students

- have an understanding of different security terms in cryptography.
- have knowledge of the significance of probabilities and entropy for the security of cryptographic schemes.
- understand the fundamental principles of quantum cryptography.
- know that alternative cryptographic schemes like elliptic curve based procedures exist and how to apply them in practice.
- are able to choose suitable parameters for cryptographic schemes.
- evaluate the security of pseudo random numbers and stream ciphers.
- have knowledge of implementation aspects of cryptography and are able to apply this knowledge in practice.
- are able to decide about the zero-knowledge property of a cryptographic protocol.

Content:

- Information theory (terms, probability, Shannon's theorem)
- Entropy
- Design principles of cryptographic hash functions
- Fundamentals of quantum cryptography
- A sketch of RSA and Elliptic curve cryptography
- Pseudo random number generators and stream ciphers
- Implementation issues (efficiency, obfuscation)
- Practical solutions to exercises

Additionally: Autonomous acquisition of zero knowledge protocols, which will be treated in the exam.

Literature:

- Nigel Smart: Cryptography. Mcgraw-Hill Professional, 2002
- Alfred Menezes, Paul van Oorschot, Scott Vanstone: Handbook of Applied Cryptography, CRC Press, 1996
- Bruce Schneier: Applied Cryptography, John Wiley & Sons, 1995
- Further current literature is mentioned in the lecture.

Lecture style / Teaching aids: Seminaristic lecture + practical course + exercise (half of the practical course consists of theoretical exercises)

Responsibility: Alex Wiesmaier

Professional competencies:

- formal, algorithmic, mathematical competencies: high
- analytical, design and implementation competencies: high
- technological competencies: medium (Dealing with cryptographic libraries (e.g. openssl), concealment methods for securing the private key, efficient implementations)
- capability for scientific work: medium

Interdisciplinary competencies:

- project related competencies: low
- interdisciplinary expertise: basic technical and natural scientific competence