

Wahlpflichtfach in den Bachelorstudiengängen (Bachelor of Arts)

Cryptography

Teaching load 4 hours per week

ECTS Credit points 5 = 150 hours

Lecture:
Self-study:

60 hours = 15 x 4 SWS
90 hours

- 30 h: Required Readings
- 20 h: Additional Readings
- 15 h: Preparation of presentations
- 25 h: Preparation for the examination

Lecturer Prof. Dr. Joachim Schreiber

Course objectives and Learning Outcomes

The students learn mathematical foundations and important applications of Cryptography. In addition to that they will learn to analyse security problems in computer networks and to find adequate solutions.

Particularly the students learn:

- basic facts of number theory and algebra, especially group theory
- history of cryptography and symmetric ciphers
- the importance of public-key encryption, e.g. the RSA-method
- the meaning of cryptography for network security

Topics

1. Mathematical Foundations

- 1.1 Number Theory
- 1.2 Algebraic Foundations

2. Applications

- 2.1 Symmetric Ciphers
- 2.2 Public-key Encryption
- 2.3 Network Security

Literature

Required readings/Additional readings

- Stallings W.: Cryptography and Network Security, Prentice Hall , 2006

	<ul style="list-style-type: none"> ➤ Koblitz N.: A Course in Number Theory and Cryptography, Springer, 1994
Teaching methods	<ul style="list-style-type: none"> • Lecture • Conversation in class • Exercises • Preparation of presentations by students
Grading	<ul style="list-style-type: none"> • Questions during the course • Solving of assignments • Preparation of presentation (20% of "Fachnote") • Examination "Business Information Systems Z" (80% of "Fachnote")
Teaching language	English