

COURSE DETAIL

CRYPTOGRAPHY

Country

Germany

Host Institution

Technical University Berlin

Program(s)

Technical University Berlin

UCEAP Course Level

Upper Division

UCEAP Subject Area(s)

Mathematics Computer Science

UCEAP Course Number

138

UCEAP Course Suffix**UCEAP Official Title**

CRYPTOGRAPHY

UCEAP Transcript Title

CRYPTOGRAPHY

UCEAP Quarter Units

8.50

UCEAP Semester Units

5.70

Course Description

This cryptography courses consists of the lectures "Public Key Cryptography" and "Cryptography for Security" as well as a practice session. Public Key Cryptography examines common methods in asymmetric encryption, as well as possible attacks in faulty implementation of these methods. Topics include RSA (including signatures), attacks on small public exponent, Wiener attack, primality tests and factorization, El-Gamal, Diffie-Hellman-Key-Exchange, elliptic curves, attacks on the discrete logarithm, and selected methods of Post-Quantum-Cryptography. Cryptography for Security discusses fundamental concepts of encryption as well as their construction and their connections, classical cryptographic problems and how to solve them, formal notions of security, One-Way-Functions, (Pseudo-)Random-Number-Generators, and Pseudo-Random-Functions. Practice sessions alternate between two formats that are both primarily focused on attacks learned in class. In the first, students read encryption code and write a corresponding decryption algorithm. In the second, students prove theorems/attacks' effectiveness and make calculations by hand, often involving topics in ring theory, field theory, and group theory.

Language(s) of Instruction

English

Host Institution Course Number

3435 L 10653,0434 L 964

Host Institution Course Title

CRYPTOGRAPHY

Host Institution Course Details

<https://moseskonto.tu-berlin.de/moses/modultransfersystem/bolognamodule/beschre...>

Host Institution Campus

Host Institution Faculty

FAKULTÄT IV ELEKTROTECHNIK UND INFORMATIK

Host Institution Degree

Host Institution Department

Institut für Softwaretechnik und Theoretische Informatik

Course Last Reviewed

2024-2025

[Print](#)