COURSE DETAIL

PUBLIC KEY 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
D

UCEAP Official Title
PUBLIC KEY CRYPTOGRAPHY

UCEAP Transcript Title
PUBLIC KEY CRYPTO

UCEAP Quarter Units
4.50

UCEAP Semester Units

3.00

Course Description

This course includes knowledge of common methods in asymmetric encryption, as well as possible attacks in faulty implementations of these methods: RSA, El-Gamal, Diffie-Hellman-Key-Exchange, elliptic curves, and selected methods of Post-Quantum-Cryptography. Students who completed this course possess profound knowledge of cryptographic methods. They are able to correctly and securely use cryptographic protocols. They are proficient in verifying the security of One-Way-Functions and (Pseudo-)Random-Number-Generators. Furthermore, they are able to recognize and avoid typical mistakes in asymmetric encryption.

Language(s) of Instruction
English

Host Institution Course Number
3435 L 10653

Host Institution Course Title
PUBLIC KEY CRYPTOGRAPHY

Host Institution Course Details
https://moseskonto.tu-berlin.de/moses/modultransfersystem/bolognamodule/beschre...

Host Institution Campus
Technische Universität Berlin

Host Institution Faculty

Host Institution Degree

Host Institution Department
Institut für Softwaretechnik und Theoretische Informatik

Course Last Reviewed

2022-2023

Print