Technology
Arts Sciences
TH Köln

Course Manual KRY

Cryptography

Version: 3 | Last Change: 05.04.2022 18:00 | Draft: 0 | Status: vom verantwortlichen Dozent freigegeben

General information

Long name	Cryptography
Approving CModule	KRY_MaCSN, KRY_MaTIN
Responsible	Prof. Dr. Heiko Knospe Professor Fakultät IME
Valid from	summer semester 2021
Level	Master
Semester in the year	summer semester
Duration	Semester
Hours in self-study	78
ECTS	5
Professors	Prof. Dr. Heiko Knospe Professor Fakultät IME
Requirements	Mathematics (Bachelor level) and programming skills.
Language	English
Separate final exam	Yes

Literature

M. Bellare, P. Rogaway, Introduction to Modern Cryptography, UCSD CSE

H. Delfs, H. Knebl, Introduction to Cryptography, Springer

S. Goldwasser, M. Bellare, Lecture Notes on Cryptography, MIT

J. Hoffstein, J. Pipher, J.H. Silverman, An Introduction to Mathematical Cryptography, Springer

J. Katz, Y. Lindell, Introduction to Modern Cryptography, CRC Press

H. Knospe, A Course in Cryptography, American Mathematical Society

C. Paar, J. Pelz, Understanding Cryptography. Springer

N.P. Smart, Cryptography Made Simple, Springer

K. H. Rosen, Discrete Mathematics and its Applications, McGraw-Hill

V. Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press

Final exam

Details	Written Exam

Minimum standard	Passing the exam
Exam Type	EN Klausur

− Lecture / Exercises

Learning goals

Goal type	Description
Knowledge	* Mathematical Fundamentals * Encryption Schemes and Definitions of Security * Elementary Number Theory * Algebraic Structures * Block Ciphers * Stream Ciphers * Hash Functions * Message Authentication Codes * Public-Key Encryption and the RSA Cryptosystem * Key Establishment * Digital Signatures * Elliptic Curve Cryptography * Outlook: Post-quantum cryptography

Special requirements

-

Accompanying material	undefined
Separate exam	No

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Lecture	2
Exercises (whole course)	1
Exercises (shared course)	0
Tutorial (voluntary)	0

− Practical training

Learning goals

Goal type	Description
Skills	- Solve mathematical and cryptographical problems in Python / SageMath: working with large integers and residue classes, factorization, primality and prime density, RSA key generation and encryption / decryption, Diffie-Hellman key exchange. - Write code to encrypt and decrypt files using the AES block cipher and different operation modes. Analyze the statistical properies of AES ciphertext. - Write code for RSA key generation, key encapsulation / decapsulation and hybrid encryption / decryption.

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Practical training	1
Tutorial (voluntary)	0

Special requirements

-

Accompanying material	undefined
Separate exam	Yes

Separate exam

Exam Type	EN praxisnahes Szenario bearbeiten (z.B. im Praktikum)
Details	Individual feedback and passing grade
Minimum standard	Successful completion of all lab tasks.