Technology
Arts Sciences
TH Köln

Lehrveranstaltungshandbuch KRY

Kryptographie

Version: 3 | Letzte Änderung: 05.04.2022 18:00 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

Allgemeine Informationen

Langname	Kryptographie
Anerkennende LModule	KRY_MaCSN, KRY_MaTIN
Verantwortlich	Prof. Dr. Heiko Knospe Professor Fakultät IME
Gültig ab	Sommersemester 2021
Niveau	Master
Semester im Jahr	Sommersemester
Dauer	Semester
Stunden im Selbststudium	78
ECTS	5
Dozenten	Prof. Dr. Heiko Knospe Professor Fakultät IME
Voraussetzungen	Mathematik (Bachelor Niveau) und Programmierkenntnisse.
Unterrichtssprache	englisch
separate Abschlussprüfung	Ja

Literatur

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

Abschlussprüfung

Details	Klausur

Mindeststandard	Bestehen der Klausur
Prüfungstyp	Klausur

− Vorlesung / Übungen

Lernziele

Zieltyp	Beschreibung
Kenntnisse	* 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

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Vorlesung	2
Übungen (ganzer Kurs)	1
Übungen (geteilter Kurs)	0
Tutorium (freiwillig)	0

Besondere Voraussetzungen

-

Begleitmaterial	undefined
Separate Prüfung	Nein

− Praktikum

Lernziele

Zieltyp	Beschreibung
Fertigkeiten	- 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.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Praktikum	1
Tutorium (freiwillig)	0

Besondere Voraussetzungen

-

Begleitmaterial	undefined
Separate Prüfung	Ja

Separate Prüfung

Prüfungstyp	praxisnahes Szenario bearbeiten (z.B. im Praktikum)
Details	Individuelle Lernstandsrückmeldung und Testat
Mindeststandard	Erfolgreiche Bearbeitung aller Praktikumsaufgaben