

Modul

KRY - Cryptography

Master Communication Systems and Networks 2020

Version: 4 | Letzte Änderung: 05.04.2022 17:46 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Knospe

^ Allgemeine Informationen

Anerkannte Lehrveranstaltungen	KRY Knospe
Modul ist Bestandteil der Studienschwerpunkte	CS - Communication Systems N S - Networks & Security
Dauer	1 Semester
ECTS	5
Zeugnistext (de)	Kryptographie
Zeugnistext (en)	Cryptography
Unterrichtssprache	englisch
abschließende Modulprüfung	Ja

Modulprüfung

Benotet	Ja
Frequenz	Jedes Semester

Prüfungskonzept

Schriftliche Prüfung (Klausur)

^ Allgemeine Informationen

Inhaltliche Voraussetzungen

Kompetenzen

Kompetenz	Ausprägung
kommunikationstechnische Systeme und Prozesse realisieren	Vermittelte Kompetenzen
kommunikationstechnische Systeme und Prozesse prüfen	Vermittelte Kompetenzen
Komplexe Fragestellungen sinnvoll auftrennen	Vermittelte Kompetenzen

^ Vorlesung / Übungen

Exemplarische inhaltliche Operationalisierung

- 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

Separate Prüfung

keine

^ Praktikum

Exemplarische inhaltliche Operationalisierung

- 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 properties of AES ciphertext.
- Write code for RSA key generation, key encapsulation / decapsulation and hybrid encryption / decryption.

Separate Prüfung

Benotet	Nein
Frequenz	Einmal im Jahr
Voraussetzung für Teilnahme an Modulprüfung	Ja

Prüfungskonzept

Testat und individuelle Lernstandsrückmeldung