Technology
Arts Sciences
TH Köln

Modulhandbuch KRY

Cryptography

Master Technische Informatik 2020

Version: 5 | Letzte Änderung: 05.04.2022 17:44 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Knospe

− Allgemeine Informationen

Anerkannte Lehrveranstaltungen	KRY_Knospe
Gültig ab	Sommersemester 2021
Dauer	1 Semester
ECTS	5
Zeugnistext (de)	Kryptographie
Zeugnistext (en)	Cryptography
Unterrichtssprache	englisch
abschließende Modulprüfung	Ja

Modulprüfung

Benotet	Ja
Konzept	Schriftliche Prüfung (Klausur)
Frequenz	Jedes Semester

− Allgemeine Informationen

Inhaltliche Voraussetzungen

Handlungsfelder

Komplexe Rechner-, Kommunikations- und Eingebettete Systeme sowie komplexe Software-Systeme unter interdisziplinären Bedingungen entwerfen, realisieren und bewerten

Wissenschaftlich arbeiten und wissenschaftliche Erkenntnisse anwenden und erweitern

Learning Outcomes

ID	Learning Outcome
LO1	Was: Die Studierenden lernen die mathematischen Grundlagen der Kryptographie kennen. Es werden Kenntnisse der wichtigsten kryptographischen Methoden und Algorithmen vermittelt (HF 1). Die Studierenden verstehen verschiedene Arten von SIcherheitsanforderungen und analysieren die Sicherheit von kryptographischen Verfahren. Womit: Der Dozent/die Dozentin vermittelt Wissen und Basisfertigkeiten in der Vorlesung. In der Übung bearbeiten die Studierenden unter Anleitung Aufgaben. Im Praktikum werden konkrete Probleme und Fragestellungen der Kryptographie bearbeitet. Wozu: Kryptographie wird eingesetzt um die grundlegenden Ziele der Informationssicherheit zu erreichen. Die Studierenden lernen die Implemenierung und Anwendung von kryptographischen Algorithmen und entwickeln Konzepte um Systeme, Netzwerke und Anwendungen gegen Angriffe zu sichern (HF 2).

Kompetenzen

Kompetenz	Ausprägung
Komplexe Systeme und Prozesse analysieren, modellieren, realisieren, testen und bewerten	diese Kompetenz wird vermittelt
Komplexe Aufgaben selbständig bearbeiten	diese Kompetenz wird vermittelt

Vorlesung / Übungen

Typ	Vorlesung / Übungen
Separate Prüfung	Nein
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

Praktikum

Typ	Praktikum
Separate Prüfung	Ja
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 properies 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
Konzept	Testat und individuelle Lernstandsrückmeldung