

# Modulhandbuch 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

<b>Anerkannte Lehrveranstaltungen</b>	<u>KRY_Knospe</u>
---	-------------------

---

<b>Gültig ab</b>	Sommersemester 2021
------------------	---------------------

---

<b>Modul ist Bestandteil der Studienschwerpunkte</b>	<u>CS - Communication Systems</u> <u>N S - Networks &amp; Security</u>
--	---

---

<b>Dauer</b>	1 Semester
--------------	------------

---

<b>ECTS</b>	5
-------------	---

---

<b>Zeugnistext (de)</b>	Kryptographie
-------------------------	---------------

---

<b>Zeugnistext (en)</b>	Cryptography
-------------------------	--------------

---

<b>Unterrichtssprache</b>	englisch
---------------------------	----------

---

<b>abschließende Modulprüfung</b>	Ja
---------------------------------------	----

### Modulprüfung

<b>Benotet</b>	Ja
----------------	----

---

<b>Konzept</b>	Schriftliche Prüfung (Klausur)
----------------	--------------------------------

---

<b>Frequenz</b>	Jedes Semester
-----------------	----------------

## – Allgemeine Informationen

### Inhaltliche Voraussetzungen

### Handlungsfelder

Algorithmen, Protokolle, Schaltungen und kommunikationstechnische Systeme unter interdisziplinären Bedingungen entwickeln und testen

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 Implementierung und Anwendung von kryptographischen Algorithmen und entwickeln Konzepte um Systeme, Netzwerke und Anwendungen gegen Angriffe zu sichern (HF 2).

### Kompetenzen

Kompetenz	Ausprägung
kommunikationstechnische Systeme und Prozesse realisieren	diese Kompetenz wird vermittelt
kommunikationstechnische Systeme und Prozesse prüfen	diese Kompetenz wird vermittelt
Komplexe Fragestellungen sinnvoll auftrennen	diese Kompetenz wird vermittelt



## – Vorlesung / Übungen

<b>Typ</b>	Vorlesung / Übungen
------------	---------------------

<b>Separate Prüfung</b>	Nein
-------------------------	------

<b>Exemplarische inhaltliche Operationalisierung</b>	<ul style="list-style-type: none"><li>- Fundamentals</li><li>- Encryption Schemes and Definitions of Security</li><li>- Elementary Number Theory</li><li>- Algebraic Structures</li><li>- Block Ciphers</li><li>- Stream Ciphers</li><li>- Hash Functions</li><li>- Message Authentication Codes</li><li>- Public-Key Encryption and the RSA Cryptosystem</li><li>- Key Establishment</li><li>- Digital Signatures</li><li>- Elliptic Curve Cryptography</li></ul>
--	--

## – Praktikum

<b>Typ</b>	Praktikum
------------	-----------

<b>Separate Prüfung</b>	Ja
-------------------------	----

<b>Exemplarische inhaltliche Operationalisierung</b>	<ul style="list-style-type: none"><li>- 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.</li><li>- Write code to encrypt and decrypt files using the AES block cipher and different operation modes. Analyze the statistical properties of AES ciphertext.</li><li>- Write code for RSA key generation, key encapsulation / decapsulation and hybrid encryption / decryption.</li></ul>
--	--

### Separate Prüfung

<b>Benotet</b>	Nein
----------------	------

<b>Frequenz</b>	Einmal im Jahr
-----------------	----------------

<b>Voraussetzung für Teilnahme an Modulprüfung</b>	Ja
--	----

<b>Konzept</b>	Testat und individuelle Lernstandsrückmeldung
----------------	---