03-IMAT-KRYPT	Einführung in die Kryptographie
	Introduction to Cryptography

Lehrform *(teaching format)* / **SWS** *(hours per week)*: 4K

Kreditpunkte *(credit points)*: 6

Turnus *(frequency)*: i.d.R. jedes WiSe

Inhaltliche Voraussetzungen *(content-related prior knowledge/skills)*: Programmierkenntnisse, Mathematische Grundlagen

Sprache *(language)*: Deutsch / English

Lehrende *(teaching staff)*: Prof. Dr. Dieter Hutter, PD Dr. Karsten Sohr

Studiengang *(degree program)*	Module	Semester
Infornatik (Master)	IMAT, IMA-SQ	ab 1.Sem.
Infornatik (Bachelor)	nur *Freie Wahl*	
Mathematik (Bachelor)	WP	

Lernergebnisse:

- Grundlagen der Kryptographie und Kryptanalyse verstehen
- Definitionen von kryptographischen Sicherheitskonzepten und Angreifer verstehen
- Einsatz der Sicherheitsmechanismen und der elementaren Zahlentheorie in kryptographischen Systemen verstehen
- Funktionsweisen und Einsatzgebiete der symmetrischen und asymmetrischen Kryptographie unterscheiden
- Grundlegende und erweiterte Sicherheitsdienste der Kryptographie erlernen

Learning Outcome:

- To understand the foundations of cryptography and cryptanalysis
- To understand the definitions of cryptographic concepts of security and attackers
- To understand the application of security mechanisms and elementary number theory in cryptographic systems
- To be able to distinguish between the functions and applications of symmetric and of asymmetric cryptography
- To know basic and extented security services based on cryptography

---

Inhalte:

- Grundbegriffe der Kryptographie und Kryptanalyse
- Mathematische Grundlagen: modulare Arithmetik, endliche Körper und elementare Zahlentheorie
- Sicherheitsdefinitionen und Angreifermodelle
- Historische Chiffren (Schiebe-, Substitution-, Vigenère-, etc.)
- Blockchiffren (DES, AES) und Betriebsmodi
- Message Authentication Codes
- Kryptographische Hashfunktionen (SHA–1, SHA–3)
- Trapdoor-Einwegfunktionen

- Diffie-Hellman Schlüsselaustausch, ElGamal Verschlüsselung
- RSA-Verfahren
- Grundlagen Digitaler Signaturen
- Elliptische Kurven Kryptographie
- Post-quantum Kryptographie und Quantenkryptographie

Contents:

- Basic definitions in cryptography and cryptanalysis
- Mathematical foundations: modular arithmetic, finite fields, and elementary number theory
- Definitions of security and models of the attacker
- Historic ciphers
- Block ciphers (DES, AES) and block modes
- Message Authentication Codes
- Cryptographic hash functions (SHA–1, SHA–3)
- Trapdoor one-way functions
- Diffie-Hellman key exchange, ElGamal
- RSA approach
- Basics on digital signatures
- Elliptic curves cryptography
- Post-quantum cryptography and quantum cryptography

Hinweise *(remarks)*: In der Tabelle sind nur die primären/spezifischsten Module aufgelistet, denen diese Veranstaltung zugeordnet ist.