

<b>Einführung in die Kryptographie</b> <i>Introduction to Cryptography</i>								Modulnummer: MB-699.09			
Master Pflicht/Wahl <input type="checkbox"/> Wahl <input checked="" type="checkbox"/> Basis <input checked="" type="checkbox"/> Ergänzung <input type="checkbox"/> Sonderfall <input type="checkbox"/>				Zugeordnet zu Masterprofil Sicherheit und Qualität (SQ) <input checked="" type="checkbox"/> KI, Kognition, Robotik (KIKR) <input type="checkbox"/> Digitale Medien und Interaktion (DMI) <input type="checkbox"/>						Basis <input checked="" type="checkbox"/> Ergänzung <input type="checkbox"/>	
Modulbereich: Mathematik und Theoretische Informatik Modulteilbereich: 699 Spezielle Gebiete der Theoretischen Informatik											
Anzahl der SWS		V	UE	K	S	Prak.	Proj.	$\Sigma$	Kreditpunkte: 6	Turnus unregelmäßig	
		2	2	0	0	0	0	4			
Formale Voraussetzungen: -											
Inhaltliche Voraussetzungen: Programmierkenntnisse, Netzwerktechnik, Mathematische Grundlagen											
Vorgesehenes Semester: ab 1. Semester											
Sprache: Deutsch/Englisch											
Ziele: <ul style="list-style-type: none"> <li>• Grundlagen der Kryptographie und Kryptanalyse verstehen</li> <li>• Definitionen von kryptographischen Sicherheitskonzepten und Angreifer verstehen</li> <li>• Einsatz der Sicherheitsmechanismen und der elementaren Zahlentheorie in kryptographischen Systemen verstehen</li> <li>• Funktionsweisen und Einsatzgebiete der symmetrischen und asymmetrischen Kryptographie unterscheiden</li> <li>• Grundlegende und erweiterte Sicherheitsdienste der Kryptographie erlernen</li> </ul>											
Inhalte: <ul style="list-style-type: none"> <li>• Grundbegriffe der Kryptographie und Kryptanalyse</li> <li>• Mathematische Grundlagen (modulare Arithmetik, endliche Körper) und elementare Zahlentheorie</li> <li>• Sicherheitsdefinitionen und Angreifermodelle</li> <li>• Historische Chiffren (Schiebe-, Substitution-, Vigenère-, etc.)</li> <li>• Blockchiffren (DES, AES) und Betriebsmodi</li> <li>• Message Authentication Codes</li> <li>• Kryptographische Hashfunktionen (SHA-1, SHA-3)</li> <li>• Trapdoor-Einwegfunktionen</li> <li>• Diffie-Hellman Schlüsselaustausch, ElGamal Verschlüsselung</li> <li>• RSA-Verfahren</li> <li>• Grundlagen Digitaler Signaturen</li> <li>• Elliptische Kurven Kryptographie (ECDH, ECIES, ECDSA)</li> <li>• Erweiterte Sicherheitsdienste (Commitment Schemes, Oblivious Transfer, Zero-Knowledge Proofs)</li> </ul>											
Unterlagen (Skripte, Literatur, Programme usw.): <ul style="list-style-type: none"> <li>• Christof Paar, Jan Pelzl: Understanding Cryptography, Springer-Verlag, 2010. Videomitschnitte unter <a href="http://www.crypto-textbook.com">www.crypto-textbook.com</a></li> <li>• Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, CRC PRESS, Boca Raton.</li> <li>• Nigel Smart, Cryptography Made Simple, Springer-Verlag</li> </ul>											
Form der Prüfung: Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung											

Arbeitsaufwand	Präsenz	56 h
	Übungsbetrieb/Prüfungsvorbereitung	124 h
	Summe	180 h
Lehrende: Prof. Dr. D. Hutter, N.N.		Verantwortlich: Prof. Dr. D. Hutter