Lehrveranstaltungsnummer		**57533**		
Bezeichnung		**Analyse kryptografischer Systeme**		
Kreditpunkte		**3**	**SWS**	**2**
Dozent(in)		Prof. Dr. Christoph Karg		
Lehrform/Medieneinsatz		Vorlesung mit Praktikum		
Voraussetzungen		Fundierte Kenntnisse in: • Programmierung in C/C++ • Arbeit mit UNIX/Linux Werkzeugen (GCC, Make, CMake) • Mathematik insbesondere Zahlentheorie und Wahrscheinlichkeitsrechnung		
Lernziele/Kompetenzen		Inhalt dieser Veranstaltung ist die Analyse ausgewählter kryptografischer Verfahren. Ziel ist es, Kryptosyteme hinsichtlich ihrer Sicherheit zu analysieren und bekannte Techniken zur Kryptoanalyse anzuwenden Die Veranstaltung orientiert sich am Ansatz des projektorientierten Lernens und findet als Blockveranstaltung in der vorlesungsfreien Zeit statt.		
Inhalt		Ausgewählte Themen aus folgenden Bereichen: • Verschlüsselungsverfahren • Techniken zur Kryptoanalyse • Systemnahe Implementierung auf Basis von Linux		
Bemerkungen/Sonstiges				
Sprache		Deutsch		
Literatur		• Stinson: Cryptography Theory and Practice, Dritte Auflage, CRC Press, 2006. • Joux: Algorithmic Cryptoanalysis, CRC Press, 2009. • Stroustrup:: The C++ Programing Language, Vierte Auflage, 2013. • Shotts: The Linux Command Line: A Guide to the Shell-Shocked, No Starch Press, 2012.		
Prüfung	Art	Durchführung von Projekten inklusive Erstellung eines Abschlussberichts	Dauer: —	
	Zulassungsvoraussetzung	• Abgeschlossenes Grundstudium • Praktischer Test im Vorfeld der Veranstaltung • Durcharbeiten der vorab bereitgestellten Dokumente • Anwesenheitspflicht bei der Veranstaltung		
	Zugelassene Hilfsmittel			
Workload	Kontaktstunden	2 SWS × 15 Wochen		30 Stunden
	Selbststudium			60 Stunden
	Durchschnittlicher Arbeitsaufwand pro Semester			90 Stunden

Stand: 3.5.2014