How-To

Seminar Symmetrische Kryptographie

Wintersemester 2013/14

Das Seminar dient zwei verschiedenen Zielen: Zum einen sollen Sie lernen, sich selbstständig in (wissenschaftliche) Themen einzuarbeiten und diese gut nachvollziehbar und ansprechend vorzutragen. Sprache ist wahlweise deutsch oder englisch. Beim Vortrag sollen Beamer und/oder Tafel benutzt werden.
Zum anderen benötigen Sie den zugehörigen Schein für Ihr Studium. Scheinkriterien sind:

1. Teilnahme an allen Terminen (inkl. Vorbereitungsterminen)
2. Aktive Teilnahme im Seminar
3. Erstellung eines Handouts (1-2 Seiten A4)
4. Halten eines Vortrags (40-50 Minuten, plus Fragen)

Einteilung

Gruppe 1 ***15.01.14***	Ekrem Aydin	Wahrscheinlich gut: Lineare Kryptanalyse (Teil lineare Kryptanalyse)
	Matthias Kraß	Die Guten ins Töpfchen: Differentielle Kryptanalyse (Teil differentielle Kryptanalyse)
	Frederic Schulz	Mithören beim Telefonieren - Angriff auf DECT
Gruppe 2 ***31.01.14***	Thorben Moos	Bit für Bit verdächtig: Differentielle Kryptanalyse gegen Stromchiffren / Beispiele (Beispiele)
	Sebastian Lauer	Ja was sehen wir denn da? - Differentielle Kryptanalyse gegen Stromchiffren / Modelle (Modelle)
	Marc Fyrbiak	Der große Hammer: Multiple Differentiale im Überblick
	Lena Meier	Und sagst Du's nicht, dann piecks ich Dich! - SAT-Solver und Fault-Injection
Gruppe 3 ***04.02.14***	Christian Koßmann	Hash-Funktion auf der Streckbank: Differentielle Kryptanalyse von MD5
	Fabian Jeschak	Was lief damals schief? - Kollisionsangriff auf SHA-1 im Überblick
	Robin Ulrich	Wir statuieren ein Exempel: Beispielhafte Krypanalyse einer Hash-Funktion

Zeitplan

	Erste Vorbesprechung	**Zweite Vorbesprechung**	**Vortrag**
Gruppe 1	*spätestens* 20.12.13	*spätestens* 8.1.	Mi, 15.1.2014
Gruppe 2	*spätestens* 17.1.	*spätestens* 24.1.	Fr, 31.1.2014
Gruppe 3	*spätestens* 21.1.	*spätestens* 28.1.	Di, 4.2.2014

Werden die angegebenen Termine nicht eingehalten, wird der betroffene Vortrag abgesagt.

Handout

Das Handout soll alle zentralen Sätze und Definitionen enthalten. Es muss mindestens 1 Seite A4 und höchstens 2 Seiten A4 umfassen. Eine erste Version wird bei der ersten Vorbesprechung mitgebracht werden. Die finale Version muss spätestens 2 ***Arbeits***tage vor Ihrem Vortrag Ihrem Betreuer als PDF vorliegen.