Das Modul entfällt ab dem Wintersemester 2012/13.

BOSS-NR. 63700

~~Modul INF-MSc-309: Sicherheit durch Kryptographie~~					
Englischer Modultitel: Security through Cryptography					
Studiengänge: Masterstudiengang Informatik, Masterstudiengang Angewandte Informatik					
Turnus nach Bedarf		Dauer 1 Semester	Studienabschnitt 2.–3. Semester	Credits 6	Aufwand 180 (60/120)

1 Modulstruktur

Nr.	Element / Lehrveranstaltung	Typ	Credits	SWS
1	Sicherheit durch Kryptographie	V	4	3
2	Übung zu Sicherheit durch Kryptographie	Ü	2	1

2 Lehrveranstaltungssprache: deutscher Vortrag / englische Unterlagen

3 Lehrinhalte

Um Sicherheitsanforderungen durchzusetzen, kann man die Sicherheitsmaßnahmen der Kryptographie einsetzen. Insbesondere sollen folgende Einzelthemen behandelt werden:

- kryptographische Isolation, Zusammenarbeit unter Bedrohungen, grundlegende kryptographische Bausteine, informationstheoretische Sicherheit, komplexitätstheoretische Sicherheit, kryptographische Sicherheit.
- Verschlüsselung: Einmal - Schlüssel und perfekte Verschlüsselungen, Strom-Verschlüsselungen mit Pseudozufallsfolgen, asymmetrische Verschlüsselungen, z.B. RSA, ElGamal, Elliptic Curves, symmetrische Verschlüsselungen, z.B. DES, IDEA, AES, Strom-Verschlüsselungen durch Betriebsarten.
- Authentifikation und Beweissicherung: Einmal-Schlüssel und perfekte Authentifikation, asymmetrische digitale Unterschriften, z.B. RSA, ElGamal, undeniable signatures, symmetrische Authentifikation.
- Anonymisierung: blinde digitale Unterschriften, anonymes Senden, MIX Server.
- fortgeschrittene Protokolle: verdeckte Verpflichtungen, Geheimnisteilung, Zero-Knowledge-Beweissysteme, Mehrparteien-Berechnungen, Schlüsselverwaltung.

4 Kompetenzen

Die Studierenden sollen aufbauend auf ein allgemeines Verständnis der Fragen zur Sicherheit die Theorie und die grundlegende Praxis der Kryptographie kennen und für größere Anwendungen selbständig einsetzen können. Darüber hinaus sollen sie auch fortgeschrittene kryptographische Sicherheitsmaßnahmen eigenständig bewerten, anwenden, weiterentwickeln und im Hinblick auf ihre informationstheoretischen und komplexitätstheoretischen Eigenschaften umfassend informatorisch-mathematisch untersuchen können.

5 Prüfungen

Modulprüfung: mündliche Prüfung (20 Minuten) BOSS-NR. 63791

Studienleistung: –keine–

6 Prüfungsformen und -leistungen

☒ Modulprüfung ☐ Teilleistungen

7 Teilnahmevoraussetzungen

Erfolgreich abgeschlossen: –keine–

Vorausgesetzte Kenntnisse: Es wird die Bereitschaft zur aktiven Teilnahme an den Übungen (inkl. Präsentation eigener Lösungen) erwartet.

Wünschenswerte Kenntnisse: Grundkenntnisse über Sicherheit aus dem Bachelor-Studium

8 Modultyp und Verwendbarkeit des Moduls

Vertiefungsmodul in den Masterstudiengängen Informatik und Angewandte Informatik
Forschungsbereich: Software, Sicherheit und Verifikation

9 Modulbeauftragte/r	Zuständige Fakultät	
Prof. Dr. J. Biskup	Informatik	Beschluss Fakultätsrat 13.01.2010 Außerkraftsetzung Fakultätsrat 12.12.2012