Modul: Formale Aspekte der Software-Sicherheit und Kryptographie (6 Credits)

Name im Diploma Supplement	Formal Aspects of Software Security and Cryptography
Verantwortlich	Prof. Dr. Barbara König
Voraussetzungen	Siehe Prüfungsordnung.
Workload	180 Stunden studentischer Workload gesamt, davon: • Präsenzzeit: 60 Stunden
Dauer	Das Modul erstreckt sich über 1 Semester.
Qualifikationsziele	Die Studierenden • erwerben fortgeschrittene Kenntnisse auf dem Gebiet der Software-Sicherheit und Kryptographie • sind mit den theoretischen und formalen Grundlagen dieses Gebiets vertraut • sind in der Lage komplexe Verschlüsselungsverfahren zu verstehen und ansatzweise zu bewerten • kennen die komplexitätstheoretischen Grundlagen der Kryptographie • besitzen Kenntnisse über Verfahren bei denen Nachrichten sicher ausgetauscht werden • können die Sicherheit dieser Verfahren in Teilen abschätzen • sind vertraut mit Techniken zur Verifikation kryptographischer Protokolle
Prüfungsmodalitäten	Zum Modul erfolgt eine modulbezogene Prüfung in Form einer Klausur oder mündlichen Prüfung.
Verwendung in Studiengängen	• SNE Master 2016 > Wahlpflichtbereich > 1.-3. FS, Wahlpflicht
Bestandteile	• Vorlesung mit integrierter Übung: Formale Aspekte der Software-Sicherheit und Kryptographie (6 Credits)

Vorlesung mit integrierter Übung: Formale Aspekte der Software-Sicherheit und Kryptographie (6 Credits)

Name im Diploma Supplement	Formal Aspects of Software Security and Cryptography		
Anbieter	Fachgebiet Theoretische Informatik http://www.ti.inf.uni-due.de/		
Lehrperson	Prof. Dr. Barbara König		
SWS	4	Sprache	deutsch
Turnus	unregelmäßig	maximale Hörerschaft	unbeschränkt

empfohlenes Vorwissen
keines

Abstract
Im Bereich der Software-Sicherheit und Kryptographie ist es wichtig, theoretische Grundlagen zu besitzen, aufgrund derer die Sicherheit von Verfahren und Protokollen bewertet werden kann. Im Rahmen dieser Vorlesung werden sowohl komplexitätstheoretische als auch semantische Grundlagen zu diesem Gebiet vermittelt.

Lehrinhalte
- Kryptographie (Grundlagen der Kryptographie, One-Time-Pad, Advanced Encryption Standard, RSA und Primzahltests, Einweg- und Falltür-Funktionen)
- Kryptographische Protokolle (Authentifizierung, Bit Commitment, Interactive Proof Systems, Zero-Knowledge Protokolle, Secure Multi-Party Computations)
- Verifikation kryptographischer Protokolle (Eindringlingsmodell nach Dolev-Yao, Sicherheitslücken in kryptographischen Protokollen, Angewandter pi-Kalkül, Model-Checking kryptographischer Protokolle)

Literaturangaben

- John Talbot, Dominic Welsh: Complexity and Cryptography - An Introduction. Cambridge, 2006.
- Christo H. Papadimitriou: Computational Complexity. Addison-Wesley, 1994
- Arto Salomaa: Public Key Cryptography. Springer, 1990
- William Stallings: Cryptography and Network Security: Principles and Practice. Prentice-Hall, 2003
- Oded Goldreich: Foundations of Cryptography (Basic Applications). Cambridge University Press, 2004

didaktisches Konzept
Die Veranstaltung entspricht einem Vorlesungsanteil von 3 SWS und einem Übungsanteil von 1 SWS.