Vorlesungsbeschreibung: Mathematisch-technische Grundlagen der IT-Sicherheit

Lernergebnisse

Nach erfolgreichem Abschluss dieses Moduls besitzen die Studierenden - im Bereich von Forensik und Auditing" - Kenntnisse und Fertigkeiten zur Anwendung der mathematischen und technischen Grundlagen der Sicherheit, insbesondere der Organisation von IT-forensischen Analysen und IT-Audits und dem Betreiben von IT-Systemen unter Berücksichtigung der Anforderungen an IT-Forensik und IT- Audit. Die Studierenden erhalten die Fähigkeit, IT-Forensik- bezogene Sicherheitsrichtlinien zu entwickeln und durchzusetzen sowie die Kenntnisse zur Bewertung der Verwendbarkeit von IT- Audit-Ergebnissen für Forensik.

Im Kontext der technischen Sicherheit" erhalten die Lernenden Kenntnisse über die symmetrische Verschlüsselung, insbesondere informationstheoretisch sichere Verschlüsselungen, klassische Verschlüsselungsverfahren, Blockchiffren (DES, AES), Stromchiffren, Verschlüsselungsmodi (z. B. CBC), Angriffe. Bei der asymmetrischen Verschlüsselung erhalten sie Kenntnisse zu RSA, Diffie-Hellman-Schlüsselaustausch, zahlentheoretischen Grundlagen (Euklidischer Algorithmus, modulare Arithmetik, etc.), Angriffen. Weiterhin erhalten die Studierenden Kenntnisse zur Nachrichtenauthentifizierung, digitalen Signaturen, Public-Key-Infrastruktur (PKI), Angriffen, aktuellen Trends in der Kryptographie (Quantenkryptographie, etc.).
Die erworbenen fachlichen und methodischen Kompetenzen zielen auf die Vorbereitung für das Berufsleben ab.

Inhalte

- Gesetzliche Voraussetzungen für IT-Forensik
- Prinzipien von IT-Audit
- Organisation von IT-forensischen Analysen
- Grundlagen und Anwendungen kryptografischer Verfahren

Lehrmethoden

Vorlesung, Übungen in Kleingruppen.

Lehrsprache

Deutsch

Studien-/Prüfungsleistung

Hausarbeit/Klausur/mündliche Prüfung pro Lehrveranstaltung

Credits

6

Workload: 180 h = 60 h Präsenz-, 120 h Eigenstudium (inkl. Prüfungsvorbereitung und Prüfungen)

Literatur

Geschonnek, Alexander: IT-Forensik, 2011.
The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, 2012.
Ertel, Wolfgang: Angewandte Kryptographie; Carl Hanser Verlag, 4. Auflage, 2012.
Paar, Christof, Pelzl, Jan: Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender; Springer Vieweg, 2016.
Schmeh, Klaus: Kryptografie: Verfahren, Protokolle, Infrastrukturen; dpunkt Verlag, 6. Auflage, 2016.

Besonderes

Im Bereich der Kryptographie: Verwendung des Werkzeugs „CrypTool“ zum Experimentieren mit kryptographischen Verfahren.

Alle öffnen Alle schließen