

Modul für den Studiengang Informatik / Softwaretechnik

Modulbezeichnung	Kryptologie
Kürzel für Stundenplan	Kry
Semester	4/5/6
Modulverantwortliche/r	Prof. Dr. Schiffer
Dozent/in	Prof. Dr. Schiffer
Sprache	Deutsch
Zuordnung zum Curriculum	INF, Wahlpflicht
Lehrform / SWS	<p>3V + 1P, Vorlesung mit Skript; begleitendes Praktikum. Das Praktikum besteht aus zwei Teilen.</p> <p>Im ersten Teil sollen zum einen einfache symmetrische Chiffrieralgorithmen zum Ver- und Entschlüsseln implementiert werden, und zum anderen sollen die Studierenden in die Rolle eines Lauschers schlüpfen, der versucht, abgefangene Geheimtexte zu entschlüsseln.</p> <p>Im zweiten Teil des Praktikums stehen asymmetrische Chiffrierverfahren im Mittelpunkt. Es wird eine Einführung in das Computeralgebra-System Maple gegeben, mit Hilfe dessen sich Ganzzahlen praktisch beliebig großer Länge, wie sie bei Public-Key-Verfahren eingesetzt werden, verarbeiten lassen. Auch in diesem zweiten Teil sollen sowohl kryptographische Algorithmen implementiert als auch Geheimtexte geknackt werden.</p>
Arbeitsaufwand	150 h
Leistungspunkte	5
Voraussetzungen	Beherrschen der Inhalte der Module Informatik I+II und Programmieren I+II
Lernziele / Kompetenzen	<p>Jeder Informatiker und jede Informatikerin kommt mit Sicherheit mit den Begriffen „verschlüsselte Kommunikation“, digitale Unterschriften“ und „Zertifikate“ in Berührung.</p> <p>Dieses Modul soll den Studierenden vermitteln, was hinter diesen Begriffen steckt, also wie kryptographische Verfahren auf der algorithmisch-mathematischen Ebene funktionieren, wobei sowohl die klassischen symmetrischen als auch die asymmetrischen, also Public-Key-Verfahren ausführlich behandelt werden.</p> <p>Erforderlich für das Verständnis der letzteren ist ein etwas tieferer Blick in das Gebiet der Zahlentheorie und hier besonders der Modulo-Arithmetik, die auch in anderen Feldern der Informatik eine wichtige Rolle spielt. Auch der Begriff der Einweg(hash)funktion ist hier von zentraler Bedeutung.</p> <p>Die Studierenden lernen die Zusammenarbeit zwischen</p>

	<p>symmetrischen und Public-Key-Verfahren kennen und erfahren, in welchen Anwendungsbereichen welche kryptographischen Techniken typischerweise eingesetzt werden. Auch kryptoanalytische Verfahren, also Methoden zum „Knacken“ von Geheimbotschaften, werden besprochen.</p> <p>Die Studierenden sollen aber auch erkennen, in welchem (auch historischen und gesellschaftlichen) Rahmen sich die kryptologischen Verfahren im Laufe der Zeit entwickelt haben, damit sie die bis heute erreichten Fortschritte einordnen können.</p> <p>Nach erfolgreichem Besuch dieser Lehrveranstaltung kennen die Lernenden alle wichtigen kryptographischen Verfahren mit ihren jeweiligen Vor- und Nachteilen und sind sich insbesondere über ihre Risiken im Klaren. Sie wissen über die Funktionsweise der zugrunde liegenden Algorithmen so gut Bescheid, dass sie kleinere darauf basierende Anwendungen selbst implementieren können.</p>
Inhalt	Siehe unten
Studien-/ Prüfungsleistungen	Projektarbeit, Klausur (90 min)
Medienformen	Skript, Beamer
Literatur	<ul style="list-style-type: none"> • Albrecht Beutelspacher et al.: „Moderne Verfahren der Kryptographie“, Vieweg • Gilbert Brands: "Verschlüsselungsalgorithmen", Vieweg • Bruce Schneier: „Applied Cryptography“, Wiley • Reinhard Wobst: „Abenteuer Kryptologie“, Addison-Wesley

Studieninhalte des Moduls **Kryptologie**

Überblick

- Kryptographie, Kryptoanalyse
- Steganographie
- Symmetrische und Public-Key-Chiffrierverfahren
- Digitale Unterschriften

Grundlegende Begriffe

- Chiffrierung, Algorithmus, Schlüssel
- Monoalphabetische/polyalphabetische Chiffrierungen
- Monographische/polygraphische Chiffrierungen
- Polyphonie
- Blockchiffrierung und Stromchiffrierung

Symmetrische Chiffrierverfahren

- Substitution und Transposition
- Caesar-Chiffrierung
- Redundanz der Sprache

- Häufigkeitsanalyse, Inzidenzindex
- Stromchiffrierungen: Chiffriermaschinen, One-Time-Pad, Zufallszahlengeneratoren
- Blockchiffrierungen: DES, IDEA, AES
- Einfluss der Schlüssellänge

Primzahlen und Modulo-Arithmetik

- Euklidischer Algorithmus
- Eulersche Phi-Funktion
- Modulo-Arithmetik, Galois-Felder
- Theoreme von Fermat und Euler
- Primzahlentests

Public-Key-Chiffrierverfahren

- Einwegfunktionen mit/ohne Falltür
- Diffie-Hellman-Verfahren
- ElGamal-Verfahren
- RSA-Verfahren (Rivest/Shamir/Adleman)
- Hybridverfahren
- PGP, SSL, Secure Shell
- Digitale Unterschriften
- Zertifikate, Schlüsselmanagement

Weiterführende Themen

- Chipkarten
- Zero-Knowledge-Protokolle
- Quantenkryptographie

Summe Workload für die Vorlesung ca. 50 h

Summe Workload für das Nacharbeiten der Vorlesung ca. 50 h

Summe Workload für das Praktikum ca. 50 h

Gesamt-Workload für das Modul "Kryptologie" ca. 150 h