Hochschule München
Fakültät für Elektro- und Informationstechnik
Prof. Dr. H. Kahl

Wintersemester 2024/25

Wahlmodul: Einführung in die Kryptologie

Zielgruppe:

Master-Studenten der Elektro- und Informationstechnik, die z.B. daran interessiert sind wie man

übers Telefon knobelt ohne mogeln zu können

oder

sichere digitale Unterschriften erstellt

oder

geheime Nachrichten übermittelt.

Voraussetzungen:

formal **keine**; Hilfreich sind Kenntnisse der Mathematik-1 Lehrveranstaltung.

Themen:

Grundbegriffe
Grundlegende Protokolle
Spezielle mathematische Grundlagen
Bekannteste symmetrische und asymmetrische Verfahren

Literatur:

Vorlesungsskript auf 'moodle'
A. Beutelspacher et al.: Moderne Verfahren der Kryptographie (1999) Vieweg-Verlag
A. Beutelspacher et al.: Kryptografie in Theorie und Praxis (2005) Vieweg-Verlag
J. Buchmann: Einführung in die Kryptographie (2004) Springer Verlag
R. Matthes: Algebra, Kryptologie und Kodierungstheorie (2003) Fachbuchverlag Leipzig
B. Schneier: Angewandte Kryptographie (2006) Pearson Studium

Beginn:

am zweiten Montag der Vorlesungszeit
(zwei Stunden seminaristischer Unterricht + eine Stunde Übung)

Prüfung:

Am Ende des Semesters wird eine benotete Prüfung angeboten.