SoSe 2026 WP Kryptographie (Dr. Moritz Minzlaff)

Inhaltsangabe

Wir folgen im Wesentlichen dem “Course Curriculum 2” aus dem Buch “Understanding Cryptography” (siehe Literatur). Begleitend werden wir mit Computeralgebrasystemen wie Sage Beispiele rechnen. Das Modul umfasst drei Teile:

Teil 1: Grundlagen und symmetrische Kryptographie
- Grundbegriffe der Kryptographie, Schlüsselängen
- Zufallszahlen und Stromchiffren
- Advanced Encryption Standard (AES)

Teil 2: Asymmetrische Kryptographie
- Mathematische Grundlagen der Public-Key-Kryptographie
- RSA-Verfahren
- Diffie-Hellman-Schlüsselaustausch und diskretes Logarithmusproblem
- Elliptische Kurven

Teil 3: Ausgewählte weiterführende Themen
- Digitale Signaturen
- Hashfunktionen
- Post-Quanten-Kryptographie

Anforderungen
- Lineare Algebra
- Programmierung in Python
- Neugier auf angewandte Zahlentheorie und Algebra
- Motivation kontinuierlich mitzuarbeiten

Vorwissen in den folgenden Themen ist hilfreich, aber keine Voraussetzung:
- Algebraischen Strukturen wie Gruppen, Ringe, Körper und Restklassen
- Jupyter und Computeralgebrasysteme

Literatur

Christof Paar, Jan Pelzl, Tim Güneysu: Understanding Cryptography (2nd edition). https://doi.org/10.1007/978-3-662-69007-9
Signal Technology Foundation: Technical information. https://signal.org/docs