PROSEMINAR KRYPTOGRAPHIE

AMIN COJA-OGHLAN
amin.coja-oghlan@tu-dortmund.de
Raum 3007, OH12

TERMIN

steht noch nicht fest

ORGANISATION

- Die Vortragsthemen werden in der ersten Semesterwoche vergeben.
- Es gibt keinen separaten Präsentationskurs. Sie nehmen am Präsentationskurs der Fakultät teil.
- Zu Ihrem Vortrag erstellen Sie ein 2-seitiges Exposé, das im Proseminar als Handout an alle verteilt wird.

VORKENNTNISSE

- Sie sollten die Mathematikveranstaltungen 1 und 2 absolviert haben.
- Grundkenntnisse im Bereich Algorithmen und Komplexitätstheorie sind von Vorteil.

THEMA

In diesem Proseminar geht es um praktisch anwendbare Verschlüsselungsverfahren wie beispielsweise das RSA-Verfahren und um die Frage, wie "sicher" diese Verfahren sind. Beginnend mit den mathematischen Grundlagen aus der Algebra und Zahlentheorie werden wir effiziente Algorithmen für die Ver- und Entschlüsselung kennenlernen. Darüber hinaus befassen wir uns mit Faktorisierungsalgorithmen, die verwendet werden können, um Verschlüsselungen zu brechen. Neben klassischen Algorithmen wird auch die Faktorisierung mit Quantencomputern thematisiert.

LITERATUR

Jonathan Katz, Yehuda Lindell: Introduction to modern cryptography. 3rd edition. CRC Press 2021.
Für die meisten Vorträge reicht auch die zweite Auflage, die in der Uni-Bibliothek elektronisch verfügbar ist.

VORTRAGSTHEMEN

Folgendes sind *Vorschläge* für Vortragsthemen auf Grundlage der o.g. Referenz. Sie können abweichende Vorschläge machen. Die Themenvergabe erfolgt am ersten Seminartermin.

- Perfekte kryptographische Sicherheit
- Private-Key-Kryptographie (2 Vorträge)
- Message authentication codes
- CCA-Security and authenticated encryption
- Hash functions
- Practical constructions (2 Vorträge)
- Theoretical constructions
- Number theory and cryptographic hardness (2 Vorträge)
- Factoring algorithms (2 Vorträge; nicht aus dem Buch)
- Key management
- Public key encryption (2 Vorträge)
- Digital signature schemes (2 Vorträge)
- Post-quantum cryptography
- Advanced topics (2 Vorträge)
- Attacks on hash functions (nicht aus dem Buch)