Leibniz Universität Hannover

CODIERUNGSTHEORIE UND KRYPTOGRAPHIE
BLOCK SEMINAR
SOSE 2023

DR. VICTORIA CANTORAL

Weitere Details entnehmen Sie bitte der Beschreibung in Stud.IP und kontaktieren Sie mich (cantoral@math.uni-hannover.de), wenn Sie einen Vortrag halten möchten und tragen sich für das Proseminar an.

1. Informationen über das Proseminar

Zielgruppen: FüBa studenten
Termin: Eine Woche im September 2023, wird in Zukunft bekannt gegeben.
Voraussetzungen: Linear Algebra I, Analysis I.

2. Vortragsthemen

2.1. **Codierungstheorie.**

Sep.: - Lineare, LDPC und Duale Codes

Sep.: - Gewichtspolynome und Decodierfehler

Sep.: - Zyklische Codes

Sep.: - Decodierung von BCH-Codes

2.2. **Kryptographie.**

Sep.: - Symmetrische Verfahren - die AES-Chiffrierung

Sep.: - Public-Key-Kryptographie

Sep.: - Signaturen und Hash-Funktionen

Sep.: - Der Diskrete Logarithmus

Sep.: - Wahrscheinlichkeitstheoretische Primzahltests

3. Literatur

- W. Willems, *Codierungstheorie und Kryptographie*, Birkhäuser 2008.
- J. Katz, Y. Lindell, *Introduction to modern cryptography*, 3rd edition, CRC Press 2021.

Date: July 5, 2023.