# Informationstheorie
# und
# Kryptologie

VO 2 + PS 1:

- Vorbesprechung: Di 5.3.2024 um 8:30 im HS C
- Vorlesung: Di 8.30-10.00 im HS C
- Proseminar: Do 12.00-12.45 in HS 11 oder 15:30-16:15 in HS F

In dieser Lehrveranstaltung werden folgende Themen diskutiert:

- Wahrscheinlichkeitsrechnung
  - Wahrscheinlichkeitsräume und Zufallsvariablen
  - Erzeugung von Zufallszahlen
  - Der Geburtstagsangriff
  - Randomisierte Algorithmen
- Informationstheorie
  - Die Entropie als Maß für Information
  - Die Redundanz natürlicher Sprachen
  - Verlustfreie Datenkompression
- Kryptographie
  - Symmetrische Kryptosysteme
  - Endliche Körper für effizientes Rechnen
  - Sicheres Teilen von Geheimnissen
  - Kryptosysteme mit öffentlichen Schlüsseln
  - Digitale Unterschriften und kryptographische Hashfunktionen
  - Pseudo-Zufallsgeneratoren

Unterlagen zur Lehrveranstaltung findet man im OLAT. Für den OLAT-Zugang ist eine Anmeldung zur Vorlesung bzw. Proseminar erforderlich.