Bei der diskreten Mathematik wollen wir Elemente der abstrakten Algebra und Zahlentheorie und ihre Anwendungen in der Informatik betrachten.
Hierbei werden auch Verschlüsselungsverfahren behandelt.

Inhalte

Grundlagen der Gruppentheorie, Ringtheorie und Teilbarkeit ganzer Zahlen, Euklidischer Algorithmus, Rechnen mit Divisionsresten (Modulo). Primzahlen und wichtige Sätze der Zahlentheorie, wie der kleine Satz von Fermat, Satz von Euler. Diese Ergebnisse werden auf die Informatik angewendet ins besondere bei Verschlüsselung und Hash-Verfahren. Asymmetrische Verschlüsselung mit RSA-Verfahren, Diffie-Hellman-Protokoll, Digitale Signatur.

Modulnote

Üblicherweise wird eine Klausur geschrieben. Bei kleinerer Teilnehmerzahl können auch Präsentationen gemacht werden.
Die Vorgehensweise wird zu Beginn der Veranstaltung besprochen.

Literaturempfehlungen (nicht zwingend)

Tobias Glosauer, Elementar(s)te Gruppentheorie
Sebastian Iwanowski, Diskrete Mathematik mit Grundlagen
Gerald Teschl, Mathematik für Informatiker Band 1: Diskrete Mathematik und Lineare Algebra
Alfred Beutelspacher, Diskrete Mathematik für Einsteiger
Christof Paar, Kryptographie verständlich