Prof. Dr. Jens Gamst
Prof. Dr. Michael Hortmann

Seminar der WE AℓZAGK
Wintersemester 2010/11
VAK 03-468

Faktorisierung und diskreter Logarithmus

Das Seminar richtet sich an Studierende der Mathematik und Technomathematik ab dem fünften Semester. Behandelt werden Lösungsansätze für zwei zahlentheoretische Probleme, auf deren Schwierigkeit wichtige kryptographische Protokolle beruhen.

Interessenten/innen können sich vorab in Studip unverbindlich für das Seminar anmelden.

Vorläufige Themenliste:

1. Fermat-Faktorisierung
2. Kettenbrüche
3. Glatte Zahlen
4. Zahlkörpersieb
5. Das diskrete Logarithmusproblem in verschiedenen Gruppen
6. Elliptische Kurven
7. Lösungsansätze für das diskrete Logarithmusproblem auf Elliptischen Kurven

Termin: donnerstags 8:30-10:00, MZH 7200
Vorbesprechung und Einleitung: Donnerstag 28. Oktober
Beginn der Vorträge: 4. November
Seminarschein: rein oder angewandt, je nach Themenausrichtung

Literatur:

ad 1. u. 2.
Koblitz, A Course in Number Theory and Cryptography
Forster, Algorithmische Zahlentheorie

ad 3. 4. 6.
Buhler, Stevenhagen, Algorithmic Number Theory
http://www.msri.org/communications/books/Book44/index.html

ad 5. 6. 7.
Cohen, Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography

---

Näheres bei:
Jens Gamst, MZH 7110, Di 10-12, gamst@math.uni-bremen.de
Michael Hortmann, http://Michael-Hortmann.math.uni-bremen.de