Seminar der WE AℓZAGK

– Kryptographische Anwendungen elliptischer Kurven–

Do 8:30 - 10:00 in MZH 7200

Im SS 07 werden wir die im letzten Semester erworbenen Kenntnisse benutzen, um zu sehen, wie man elliptische Kurven in der Kryptographie und für zahlentheoretische Algorithmen einsetzen kann.
Unsere Grundlage ist weiterhin:

L. Washington *"Elliptic Curves. Number Theory and Cryptography"*.
Chapman & Hall/CRC, Boca Raton 2003

VortragsPlan

I. Kryptographische Anwendungen
- I.1 Diffie-Hellman Problem (6.2)
- I.2 Massey-Omura Verschlüsselung (6.3)
- I.3 ElGamal Verschlüsselung und -Signatur (6.4, 6.5)
- I.4 RSA mit Elliptischen Kurven (6.7)

II. Faktorisierung mit Elliptischen Kurven
- II.1 Methode von H. Lenstra (7.1)
- II.2 Beispiel: Faktorisierung von F_{10}.
  cf. R. Brent: "Factorizaton of the tenth Fermat Number",
  Math. of Comp. 1998.

III. Primzahltests mit Elliptischen Kurven
- III.1 Goldwasser/Kilian Test (7.2)
- III.2 Verbesserung nach Atkin/Morain
  cf. A.O.L. Atkin/F. Morain: "Elliptic Curves and Primality Proving",
  Math. of Comp. 1993

IV. Anzahlbestimmung
- IV.1 Schoof-Algorithmus (4.5)
- IV.2 Verbesserung nach Atkin/Elkies
  cf. I.F. Blake et al: "Elliptic Curves in Cryptography",
  Cambridge Univ. Press 2000.
- IV.3 p-adischer Ansatz
  cf. T. Satoh in LN Comp. Sci. 2369, 2002.

Näheres bei J. Gamst, mail: *gamst@math.uni-bremen.de*

Di., 10:00-12:00 Uhr, in MZH 7110