Fakultät für Mathematik und Informatik

H. Kredel, W.K. Seiler

Im Frühjahrssemester 2008 veranstalten wir ein

Seminar über Computeralgebra (Kryptographie)

Ort und Zeit: Donnerstag, $15^{30} - 17^{00}$ Uhr, B6, A 1.01
Vorbesprechung: 21. Februar 2008

In den letzten beiden Jahrzehnten bewegte sich die Kryptographie immer mehr weg von kombinatorischen Verfahren hin zu algebraisch definierten Verschlüsselungsalgorithmen. Damit werden Methoden der Computeralgebra interessant sowohl zur Verschlüsselung als auch zum Knacken verschiedener Verfahren: Beispielsweise läßt sich die Kryptanalyse des *Advanced Encryption Standards* AES, der bei fast allen sicheren Internetverbindungen benutzt wird, umformulieren in die Lösung eines (riesigen) Systems von Polynomgleichungen.

Im Seminar sollen sowohl Kryptosysteme auf der Basis von Polynomen behandelt werden als auch solche Angriffe. Dazu sollen insbesondere auch GRÖBNER-Basen als eines der universellsten Werkzeuge zum Umgang mit Polynomen ausführlich behandelt werden.

Neben eher abstrakt-algebraischen Vorträgen soll es auch einige Vorträge geben, die sich gezielt mit Implementierungsfragen befassen.

Seminargebäude D7
D - 68131 Mannheim
Tel.: 0621 / 181 - 2515
Fax: 0621 / 181 - 2461
seiler@math.uni-mannheim.de