Seminar Wintersemester 2002/2003

# Zahlentheorie und Kryptographie

Di. 14.00-16.00, M HS 4

Jedem Internetnutzer ist das RSA-Verschlüsselungssystem ein Begriff. Es handelt sich um ein sogenanntes Public-Key-System und basiert im wesentlichen auf der Schwierigkeit die Primzahlzerlegung einer großen (ganzen) Zahl anzugeben. In diesem Seminar wollen wir die arithmetischen Grundlagen dieses (und anderer Verfahren) kennenlernen.
Das Seminar wird sich hauptsächlich auf das Buch *A Course in Number Theory and Cryptography* von *Neal Koblitz* stützen.

- Einführung in die relevanten Ergebnisse der elementaren Zahlentheorie und Algebra: Teilbarkeit, Euklidischer Algorithmus, Kongruenzen, Restklassenringe, Kleiner Fermatscher Satz, Chinesischer Restsatz, quadratische Reste und das quadratische Reziprozitätsgesetz.
- Definition von Verschlüsselungsverfahren (Kryptosystemen) und Beispiele für verschiedene Systeme, insbesondere symmetrische und asymmetrische Systeme.
- Das Prinzip der Public-Key-Verfahren mit den wichtigen Beispielen RSA, Diskreter Logarithmus und Knapsack-Problem.
- Primzahltests, Pseudo-Primzahlen, Carmichael-Zahlen.
- Faktorisierungsmethoden
- Elliptische Kurven über endlichen Körpern, $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ und einige Eigenschaften. Kryptosysteme, die auf elliptischen Kurven basieren.

Für dieses Seminar werden lediglich die Vorlesungen Lineare Algebra I und Analysis I vorausgesetzt. Insbesondere werden keine speziellen Kenntnisse in Zahlentheorie und/oder Algebra angenommen. Die relevanten Ergebnisse sollen in den ersten Vorträgen erarbeitet werden. Interessenten für das Seminar können sich jederzeit bei einem von uns melden melden.

Prof. K.Wingberg
Zi. 226
Tel. (54) 48 97
wingberg@mathi.uni-heidelberg.de

Sigrid Wortmann
Zi. 108
Tel. (54) 48 96
wortmann@mathi.uni-heidelberg.de