Universität Mannheim

Lehrstuhl VI für Mathematik

Wolfgang K. Seiler

Im Herbstsemester 2010 werde ich lesen

Kryptologie

Ort und Zeit: Montag, $8^{30} - 10^{00}$ und Donnerstag, $13^{45} - 15^{15}$, C 014
Übungen dazu: Donnerstag, $15^{30} - 17^{00}$, C 014

Handel über das Internet, elektronischer Zahlungsverkehr sowie jedwede andere sichere Kommunikation sind nur möglich, wenn Vertraulichkeit gewährleistet ist und die Identität der Beteiligten zweifelsfrei feststeht. Die dazu und für vieles andere notwendigen Verfahren entwickelt die Kryptologie, die Wissenschaft vom Geheimen.

Fast alle der heute wirklich verwendeten Algorithmen (RSA, DSA, AES *usw.*) beruhen auf Sätzen der Algebra und der Zahlentheorie; diese Verfahren und ihre mathematischen Grundlagen bilden den Schwerpunkt der Vorlesung. Selbstverständlich spielen auch Angriffe auf solche Verfahren eine große Rolle, denn ohne deren Kenntnis kann Sicherheit nicht seriös beurteilt werden.

Zu Beginn der Vorlesung möchte ich allerdings zunächst einige heute veraltete und unsichere klassische Verfahren vorstellen, die leider immer noch in manchen kommerziellen Office-Programmen zu finden sind. Hier geht es vor allem darum zu verstehen, daß manche Verschlüsselung auch dann schnell und einfach geknackt werden kann, wenn der Anbieter (zu Recht) behauptet, daß selbst die leistungsfähigsten heutigen Computer länger als das Alter des Universums bräuchten, um alle Schlüssel durchzuprobieren.

Am Ende der Vorlesung geht es um einen spekulativen Ausblick in die Zukunft: Möglicherweise wird sich die Kryptologie in den nächsten Jahrzehnten entscheidend verändern müssen, denn rund um die Welt arbeiten Physiker an sogenannten Quantencomputern, die – sofern sie je in hinreichender Größe gebaut werden können – alle zur Zeit gebräuchlichen Verfahren für elektronische Unterschriften und auch für Verschlüsselung ohne vorherigem Schlüsselaustausch unsicher machen. Im letzten Teil der Vorlesung wird es einerseits darum gehen, dies zu verstehen, andererseits auch um Auswege wie die (bereits existierende) Quantenkryptographie sowie um derzeit noch in der Entwicklung befindliche Verfahren, die auch gegenüber Quantencomputern sicher sind.

Literaturauswahl:

JOHANNES BUCHMANN: Einführung in die Kryptographie, *Springer Lehrbuch*, ^{5}2010

KARIN FREIERMUT, JURAJ HROMKOVIČ, LUCIA KELLER, BJÖRN STEFFEN: Einführung in die Kryptologie – Lehrbuch für Unterricht und Selbststudium, *Vieweg+Teubner*, 2010 *(vor allem für künftige Lehrer zu empfehlen)*

CHRISTIAN KARPFINGER, HUBERT KIECHLE: Kryptologie – Algebraische Methoden und Algorithmen, *Vieweg+Teubner*, 2010

Außerdem soll parallel zur Vorlesung ein Skriptum erscheinen.

Seminargebäude A5
D - 68131 Mannheim
Tel.: 0621 / 181 - 2515
Fax: 0621 / 181 - 2461
seiler@math.uni-mannheim.de
http://hilbert.math.uni-mannheim.de/∼seiler