Lehrstuhl VI für Mathematik

Wolfgang K. Seiler

Im Herbst-/Wintersemester 2007 werde ich lesen

Kryptologie

Ort und Zeit: Dienstag, $10^{15} - 11^{45}$ und Mittwoch, $12^{00} - 13^{30}$, C 015
Übungen dazu: Dienstag, $12^{00} - 13^{30}$, C 015

Kryptologie ist die Wissenschaft vom Geheimen. Zu ihren Aufgaben gehören unter anderem der Schutz von Information vor unbefugter Kenntnisnahme und Verfälschung sowie die sichere Identifikation von Personen, daneben aber auch die Entwicklung und Analyse von Verfahren zum Angriff auf solche Methoden. Hauptanwendung der Kryptologie ist heute die sichere Kommunikation im Internet sowie im Bankenbereich.

In der Vorlesung geht es vor allem um die mathematischen Algorithmen, die in der Kryptologie und der Kryptanalyse eingesetzt werden; der Schwerpunkt liegt auf algebraischen und zahlentheoretischen Verfahren, die auch in der Praxis die größte Rolle spielen.

Grundsätzlich unterscheidet die heutige Kryptologie zwischen zwei Arten von Verschlüsselungsverfahren: Bei den klassischen, symmetrischen Verfahren einigen sich Sender und Empfänger auf einen geheimen Schlüssel, den nur die beiden kennen. Für Anwendungen wie den Handel über das Internet ist dies natürlich nicht praktikabel; hierzu gibt es seit gut dreißig Jahren die sogenannten asymmetrischen Verfahren, bei den verschiedene Schlüssel zur Ver- und zur Entschlüsselung benutzt werden, wobei nur letztere geheim bleiben müssen. Leider sind diese Verfahren allerdings rechnerisch ziemlich aufwendig, so daß man sie meist nur dazu benutzt, einen Schlüssel für ein symmetrisches Kryptoverfahren zu übermitteln, mit dem dann die eigentliche Kommunikation verschlüsselt wird. Die Vorlesung wird daher beide Arten der Verschlüsselung behandelt; jedoch soll ein gewisser Schwerpunkt auf den mathematisch interessanteren asymetrischen Verfahren und den Angriffen darauf liegen. Zum Abschluß soll noch die (bereits existierende) Quantenkryptographie vorgestellt werden sowie die (noch nicht wirklich existierenden) Quantencomputer, die potentiell zu einem völligen Neubeginn der Kryptographie mit öffentlichen Schlüsseln zwingen könnten.

Literaturauswahl:

JOHANNES BUCHMANN: Einführung in die Kryptographie, *Springer Lehrbuch*, ^{3}2004
ALAN G. KONHEIM: Computer Security and Cryptography, *Wiley*, 2007
WENBO MAO: Modern cryptography, *Prentice Hall*, 2004
NIGEL SMART: Cryptography: An Introduction, *McGraw-Hill*, 2003
DOUGLAS R. STINSON: Cryptography, Theory and Practice, *Chapman & Hall/CRC*, ^{3}2005
DIETMAR WÄTJEN: Kryptographie – Grundlagen, Algorithmen, Protokolle, *Spektrum Akademischer Verlag*, 2004
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