



Im Herbstsemester 2016 werde ich lesen

## Kryptologie

**Ort und Zeit:** Dienstag 13<sup>45</sup> – 15<sup>15</sup> und Donnerstag 10<sup>15</sup> – 11<sup>45</sup>, C 015

**Übungen dazu:** Dienstag 15<sup>30</sup> – 17<sup>00</sup>, C 015

Klassischerweise war Kryptographie zwar die Lehre von den Geheimschriften, doch wird sie schon lange nicht mehr in erster Linie von Spionen und Diplomaten benutzt: Ihre heutige Hauptanwendung ist die Sicherung der Kommunikation und des Handels über das Internet, des bargeldlosen Zahlungsverkehrs, der Zugangskontrolle zu Orten und Dokumenten und zahlreiche weitere Aufgaben. Es geht auch längst nicht mehr nur um Vertraulichkeit, sondern auch um die Authentizität von Nachrichten, elektronische Unterschriften, die Sicherung von geistigem Eigentum an digitalen Medien und vieles mehr.

Da absolute Sicherheit notwendigerweise (nicht nur finanziell) einen sehr hohen Preis fordert, muß man sich meist mit weniger zufrieden geben. Daher ist es auch für einen bloßen Anwender kryptographischer Verfahren wichtig, etwas über Angriffsmöglichkeiten eines potentiellen Gegners zu wissen, d.h. über Methoden der Kryptanalyse. Kryptographie und Kryptanalyse bilden zusammen die Kryptologie.

Während frühere Verschlüsselungsverfahren meist ziemlich *ad hoc* versuchten, eine schwer durchschaubare Komplexität zu konstruieren, beruht ein Großteil der Verfahren aus den letzten Jahrzehnten auf gut untersuchten Problemen der Algebra und Zahlentheorie. Dies gilt insbesondere für die in der heutigen Praxis wohl wichtigsten Algorithmen wie AES, RSA, DSA und die Verfahren auf der Grundlage elliptischer Kurven. Gegenstand der Vorlesung sind daher in erster Linie diese Verfahren zusammen mit der zugrundeliegenden mathematischen Theorie, wobei allerdings die mathematisch deutlich anspruchsvolleren Verfahren mit elliptischen Kurven erst in einer eigenen Vorlesung im nächsten Semester fundiert behandelt werden können.

Zumindest zu Beginn der Vorlesung möchte ich auch kurz einige nach heutigem Stand längst veraltete und unsichere klassische Verfahren vorstellen, die leider immer noch in manchen kommerziellen Programmen zu finden sind. Hier soll vor allem klar werden, 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.

Bei Verfahren, die auf schwierigen mathematischen Problemen beruhen, besteht immer die Möglichkeit, daß entweder mathematisch oder rechnerisch ein Durchbruch gelingt, der das Problem deutlich vereinfacht. Viele heute gebräuchliche Verfahren würden unsicher, wenn es gelänge, sogenannte Quantencomputer zu bauen; andererseits bietet die Quantenphysik mit der bereits heute gelegentlich eingesetzten Quantenkryptographie auch eine sichere Alternative. Dieser Themenkreis soll zum Abschluß der Vorlesung diskutiert werden.

### Literaturauswahl:

JOHANNES BUCHMANN: Einführung in die Kryptographie, *Springer*, <sup>6</sup>2016 (auch elektronisch verfügbar)

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)

HANS DELFS, HELMUT KNEBEL: Introduction to Cryptography – Principles and Applications, *Springer*, <sup>3</sup>2015

NIGEL P. SMART: Cryptography made simple, *Springer*, 2016

JOSÉ LUIS GÓMEZ PARDO: Introduction to Cryptography with Maple, *Springer*, 2013

Außerdem soll parallel zur Vorlesung ein Skriptum erscheinen, das im wesentlichen eine Überarbeitung und Anpassung des 2013er Skriptums sein wird.

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>