LAUSCHEN ZWECKLOS

CLAUDIA ALFES UND ANNA VON PIPPICH

Nicht erst seit dem NSA-Skandal, der aufdeckte, dass selbst das Handy von Angela Merkel vor Abhörattacken nicht sicher ist, spielt das Verschlüsseln von Daten eine wichtige Rolle in unserem Alltag. Ohne Verschlüsselungsmethoden wäre kein sicheres Online-Banking oder der sichere Einsatz von Chipkarten möglich. Das Verschlüsseln der Daten muss dabei so clever sein, dass ein Abhören durch Unbefugte wertlos ist: Lauschen zwecklos!

Schon vor gut 350 Jahren wurden in der Zahlentheorie Resultate entwickelt, die die Grundlage für das sogenannte RSA-Verfahren bilden. Dieses asymmetrische Verschlüsselungsverfahren wurde 1977 von R. Rivest, A. Shamir und L. Adlemann entwickelt. Es benötigt zwei verschiedene Schlüssel zum Ver- und Entschlüsseln. Im Sommerschulkurs werden diese Resultate, sowie das Faktorisierungsproblem, das die Sicherheit des RSA-Verfahrens garantiert, kennengelernt.

Danach werden wir uns mit einem modernen Verfahren beschäftigen, das bei gleicher Sicherheitsleistung eine geringere Schlüssellänge benötigt. Dieses Verfahren benutzt elliptische Kurven. Diese sind kubische Kurven, die durch eine Gleichung der Form

$$y^2 = x^3 + ax^2 + bx + c, \quad \text{mit } a, b, c \in \mathbb{Q},$$

gegeben sind. Es wird untersucht, wie elliptische Kurven zur Verschlüsselung von Daten verwendet werden können.