Einführung in die Kryptographie

Kursleiter: Anna von Pippich & Insa Schreiber

Fernseher, Heizungen und Autos, die sich via Internet vom Smartphone aus bedienen lassen, eröffnen ganz neue Möglichkeiten im Alltag. Es entwickeln sich aber auch immer neue Formen der Cyber-Kriminalität, beispielsweise des Datendiebstahls oder der Datenmanipulation. Ins Zentrum rückt deshalb die Frage nach der sicheren Verschlüsselung von Daten – dies ist der Hauptgegenstand der Kryptographie.
Nach einem kurzen Einblick in klassische Verschlüsselungsverfahren werden wir in diesem Kurs einige heutzutage verwendete Public-Key-Verfahren kennenlernen und uns dabei die Mathematik, die hinter diesen steckt, erarbeiten. Hierbei werden wir uns insbesondere mit dem 1977 entwickelten RSA-Verfahren beschäftigen und mit dem sogenannten Faktorisierungsproblem, auf dem die Sicherheit des RSA-Verfahrens beruht. Darüber hinaus werden wir uns mit *elliptic curve cryptography* befassen. Hier spielen sogenannte elliptische Kurven, 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, eine wichtige Rolle.