Einführung in die Kryptographie: Die Mathematik, die das Internet sicherer macht

Kursleiter: Michalis Neururer & Róisín Neururer

Verschlüsselte Nachrichten sind schon seit tausenden Jahren Bestandteil unserer Kommunikation. Während Verschlüsselungsmethoden in der Geschichte der Menschheit oft für die Verständigung zwischen Verbündeten in Kriegszeiten entwickelt wurden, spielen Sie heute eine wichtige Rolle in unserem Alltag. Ohne Kryptographie gebe es kein Online-Banking und keine sicheren Emails.

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 lernen wir die Mathematik hinter dem RSA-Verfahren kennen: zum Beispiel den euklidschen Algorithmus, Fermat's kleinen Satz und das Faktorisierungsproblem. Parallel dazu werden wir die erlernten mathematischen Methoden in Sagemath bzw. Python programmieren, um schlussendlich unser eigenes RSA-Verschlüsselungsprogramm zu erstellen.

Kursleiter

Michalis Neururer hat Mathematik in Wien, Cambridge und Paris studiert und anschließend in Nottingham im Bereich der Zahlentheorie promoviert. Zurzeit ist er wissenschaftlicher Mitarbeiter an der TU-Darmstadt.

Róisín Neururer hat Mathematik in Dublin, Paris und Padova studiert. Danach arbeitete sie drei Jahre als Mathematiklehrerin an einem Gymnasium in Nottingham. Im Moment ist sie in Elternzeit, plant aber demnächst wieder als Lehrerin einzusteigen.