Informatik AG

Informatik ist inzwischen in vielen Bereichen des Lebens und der Wissenschaft unverzichtbar geworden. Sie hilft nicht nur wissenschaftliche Daten zugänglich und handhabbar zu machen, sondern beschäftigt sich auch mit der Berechnung einer optimalen Route oder der Kompression von Musik-Dateien. In diesem Labjahr beschäftigt sich die Informatik AG mit **Kryptographie**, der „Kunst der Verschlüsselung“. Es geht darum, wie du geheime Nachrichten so verschlüsseln kannst, dass nur deine Freunde sie lesen können.

Erst durch Kryptographie wird es möglich, online zu bezahlen oder einzukaufen. Wir werden der Frage nachgehen, was im Hintergrund vor sich geht, wenn wir uns sicher auf einer Webseite anmelden oder unsere E-Mails abrufen, ohne dass jemand auf dem Weg der Daten durch die Leitung an unser Passwort herankommt.

Kryptographie ist heute aber **weit mehr als nur Verschlüsselung**. Neben z.B. digitalen Unterschriften ermöglicht sie auch Dinge, die intuitiv unmöglich erscheinen. So kann man …

- … jemandem schlüssig nachweisen, dass man die Lösung für ein schwieriges Problem (z.B. ein Sudoku-Rätsel) kennt, ohne dass der andere dabei etwas über diese Lösung erfährt.
- … am Telefon eine „Münze werfen“, ohne dass der andere das Ergebnis anzweifeln wird.
- … gemeinsam herausfinden, wer einer Gruppe der/die Reichste ist, ohne das jemand verrät, wieviel Geld er/sie hat.
- … die Cloud auf privaten Daten rechnen lassen, ohne dass sie die Daten selber kennt.

Dabei werden wichtige Grundlagen der **theoretischen Informatik** behandelt:

- Während das Verschlüsseln einer Nachricht normalerweise sehr schnell geht, sollen sich Unbefugte an der Entschlüsselung ohne den geheimen Schlüssel die Zähne ausbeißen. Doch wann ist eine Problemstellung, wie etwa das Brechen einer Verschlüsselung, „schwierig”? Und: Gibt es überhaupt solche schwierigen Probleme, die leicht werden, wenn man den geheimen Schlüssel kennt?
- Die theoretische Informatik liefert auf solche und verwandte Fragen einige, wenn auch noch nicht vollständige Antworten, die je nach Tiefe auch sehr philosophisch werden können. So gibt es sogar Dinge, die ein Computer schon prinzipiell nicht berechnen kann.
- Wenn wir uns die Berechnungs-Komplexität von typischen Problemen, wie zum Beispiel das optimale Packen eines Rucksacks, oder das optimale Zeichnen einer Karte, sodass sich die Städte/Ortsnamen nicht überlappen, anschauen, dann stellen wir fest dass viele davon schwierig sind. Was hat es damit auf sich? Und: Kann man sie für Kryptographie nutzen?
- Gibt es Protokolle, von denen man die Sicherheit beweisen kann, egal in welcher Umgebung sie eingesetzt werden?

Natürlich darf bei einer Informatik AG auch die praktische Komponente nicht zu kurz kommen. Wir werden **Programmieren lernen** und vertiefen, je nach vorhandenen Vorkenntnissen, aber auch schon

vorhandene Verschlüsselungssoftware ausprobieren. Für diesen Anlass sind zwei Programmierwochenenden in Planung. Natürlich wird es auch um verwandte Fragen gehen: Wie schütze ich mich und meine Daten im Internet? Und was hat es mit den Sicherheitslücken und Datenlecks der letzten Zeit auf sich?

Wir treffen uns für gewöhnlich **einmal im Monat**, samstags, für 3–4 Stunden um unseren Projekten und Fragen nachzugehen. Die genauen Termine erfährst du im internen Bereich und auf der Mailingliste nach Anmeldung. Es wird kein Vorwissen vorrausgesetzt. Die Themen werden sich natürlich zentral an euren Interessen und eurem Engagement orientieren.

Die Informatik AG findet in Kooperation mit MINTmachen! der Uni Heidelberg statt. Des weiteren haben bereits Labbies der Informatik AG an dem Bundeswettbewerb Informatik erfolgreich in Gruppen an der ersten Runde teilgenommen.

Ansprechpartner/Mentoren ab dem Labjahr 2014/15:

- Alexander Koch (alexkoch_mail (at) web.de)
- Daniel Mendler (mail+lsl (at) daniel-mendler.de)