Workshop 3: Digitale Datensicherheit und die Kunst der Verschlüsselung

Wie funktioniert Verschlüsselung, was gilt als sicher und was kann man trotzdem knacken?

In den drei Workshoptagen lernen wir die wichtigsten Techniken der Verschlüsselung (Kryptographie) und des Code-Brechens (Kryptoanalyse) kennen.

Zunächst drehen wir die Zeit zurück und verschlüsseln geheime Botschaften händisch mit der Technik monoalphabetischer Verschlüsselung, die jahrhundertelang als sicher galt, aber durch einen einfachen wie genialen Trick geknackt werden kann, welcher z.B. der schottischen Königin Maria Stuart das Leben kostete.

Enigma, WikiLeaks, Edward Snowden und der NSA-Skandal zeigen, dass die Kryptographie eine immense Bedeutung für den Lauf der Weltgeschichte hatte und immer noch für heftigen politischen Zündstoff sorgt.

Heutzutage ist z.B. für die sichere Nutzung des Internets die sogenannte "asymmetrische" Verschlüsselung notwendig. Dabei ist - vereinfacht gesprochen - der Schlüssel zum Zusperren ein anderer wie der zum Aufsperren!

Diese auch "Public Key-Verfahren" genannte Technik bildet die Grundlage des Internet-Banking, von Kreditkartenzahlungen über das Internet, der Verschlüsselung von E-Mails und jeder Art digitaler Unterschriften.

Mithilfe des Computers werden wir eigenständig den RSA-Algorithmus anwenden, und dabei die überragende Bedeutung von Primzahlen für deine alltäglichen Tätigkeiten im Internet kennenlernen.

Aber auch diese - theoretisch als sicher geltende - Art der Verschlüsselung besitzt ihre Schwachstellen!
Wir zeigen, wie ein unbedachtes kurzes Ignorieren einer alltäglichen Zertifikatswarnung im Browser katastrophale Konsequenzen haben könnte, und wie durch die Rechenkraft heutiger PCs auch die beste Verschlüsselungstechnik wirkungslos werden kann, wenn sie von möglicherweise schlecht gewählten Passwörtern abhängig ist.

Schließlich wollen wir noch einen Ausblick geben, welche Zukunft Quantencomputer, Quantenkryptographie und homomorphe Verschlüsselung versprechen, und worauf die NSA hofft bzw. wovor sie Angst hat.

Leitung: DI Felix Hummel, DI Mag. Gerhard Mitterlechner