ABLAUF UND INHALT DER SCHÜLER-KRYPTO 2011

Daniel Loebenberger

Nach Ihrer Anreise wird zunächst eine kurze Vorlesung über die historisch wichtigen sowie aktuell in der Industrie angewandten asymmetrischen Verschlüsselungsverfahren, einschließlich der dazu notwendigen mathematischen Grundlagen gehalten. Die Schüler erhalten anschließend die Möglichkeit das erworbene Wissen eigenständig in einer Programmiersprache zu formulieren und Problemstellungen selbst zu lösen.

Im Detail wird neben dem unbedingt sicheren One-Time-Pad die symmetrische Caesar-Chiffre beschrieben und daran die elementaren Grundlagen der modularen Arithmetik erläutert. Darauf aufbauend werden die Ringe der Zahlen modulo n eingeführt und einige – für die modernen asymmetrischen Verfahren notwendigen – Eigenschaften dieser Ringe anschaulich dargestellt. Dies bildet dann die Grundlage für das Verständnis zu RSA, einem der wichtigsten, heute gebräuchlichen, Verschlüsselungsverfahren. Die theoretisch relativ tiefgreifenden Eigenschaften dieses Verschlüsselungssystems werden stets so dargestellt, dass es für Schüler der Ober- bzw. Mittelstufe problemlos möglich sein wird, dem Inhalt zu folgen.

Anhand eines klassischen James Bond Szenarios werden den Schülern anschließend Aufgaben gestellt, die diese (unter Aufsicht) selbständig lösen sollen. Dazu gehört eine eigenständige Formulierung von RSA sowie einige Aufgaben, die für das Verständnis der Sicherheit von RSA notwendig sind. Die technisch versierten Schüler werden die Aufgaben mit der Realisierung einer vollständigen Public-Key-Infrastruktur abschließen und die Möglichkeit erhalten, verschlüsselte Nachrichten gegenseitig auszutauschen.

Abgerundet wird die Schüler-Krypto durch ein Additionsketten-Spiel, welches Schülern auf einfache Weise erklärt, wie verschiedene Ansätze einer simplen Aufgabenstellung algorithmisch bessere Lösungen liefern können. Dies zeigt insbesondere einen wesentlichen Aspekt des Informatik-Studiums auf und gibt Schülern einen ungewöhnlich tiefen Einblick in die Informatik.

Als kleines Geschenk erhält jeder Schüler ein Kryptogramm seines eigenen Bildes in Form zweier vollkommen zufälligen Folien. Erst das Übereinanderlegen der Folien zeigt die darin verborgene Nachricht und zeigt so anschaulich die Funktionsweise des One-Time-Pads.

Die Methoden, die im Rahmen der Schüler-Krypto vorgestellt werden, sind elementare Grundlagen, welche zum Beispiel Online-Banking oder E-Commerce erst korrekt und sicher funktionieren lassen.

Daniel Loebenberger
b-it
D53012 Bonn
daniel@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de