Vorwort zur 1. und 2. Auflage

Die Kryptologie als Lehre der Geheimschriften ist eine der faszinierendsten Wissenschaftsdisziplinen der Gegenwart. Sie ist voll von spannenden Puzzle-Aufgaben und pfiffigen Lösungen. Bei der Suche nach Lösungen bringt sie unerwartete Wendungen und öffnet – ähnlich wie es uns die Physik öfters vorgeführt hat – Türen, die das Unmögliche möglich machen. Und bei allen diesen besonderen Gedankenexperimenten hat die Kryptologie keinen langen Weg vom Abstrakten zur Praxis. Die meisten Entdeckungen können direkt für den Entwurf von sicheren Kommunikationssystem verwendet werden. Der heutige elektronische Handel, Online-Shopping oder Online-Banking wären ohne die modernen Konzepte der Kryptologie unmöglich.

Dieses Gebiet zu meistern erfordert einigen Tiefgang, und insbesondere für den Unterricht an Hochschulen wurden in den letzten Jahren mehrere Lehrbücher geschrieben. Das Ziel dieses Buches ist ein anderes. Es soll für alle Anfänger im Selbststudium zugänglich sein, sogar auch ohne Vorwissen aus den Gebieten der Mathematik wie Algebra und Zahlentheorie, die maßgebend für die Entwicklung moderner Kryptosysteme sind.

Somit eignet sich das Buch für Schülerinnen, Schüler und Studierende aller Art, von der Sekundarstufe II bis zum Universitätsstudium, sowie für Lehrpersonen, die Kryptologie selber unterrichten wollen. Die Schwerpunkte des didaktischen Vorgehens sind die folgenden:

1. Präzise Begriffsbildung und konsequente Verwendung der Fachsprache, die dem aktuellen Stand der Schülerinnen und Schüler entspricht.

2. Langsames und leitprogrammartiges Vorgehen in kleinen Schritten, die sofort durch zahlreiche Aufgaben (auch mit Lösungen und Beschreibungen der Überlegungen und Strategien) gefestigt werden.

3. Fokus auf der inneren Philosophie der Disziplin mittels Schilderung der geschichtlichen Entwicklung der wichtigsten Ideen und Konzepte. Damit vermitteln wir ein tiefes Verständnis für den Kontext dieses Wissenschaftsgebiets.

4. Hinweise für die Lehrpersonen zum Umgang mit diesem Lehrmittel, dem Stoff, den möglichen Schwierigkeiten bei dessen Übermittlung sowie zusätzliche fachliche Hintergründe sind an den entsprechenden Stellen im Lehrbuch verzeichnet.

5. Mittels vielen puzzle-artigen Aufgabenstellungen und überraschenden Lösungsideen sowie Einblicken in die Geschichte unterschiedlicher Kryptosysteme wird für Spannung gesorgt und die Motivation zur weiteren Vertiefung geweckt.

Fachlich vermittelt das Lehrbuch die Grundlagen der klassischen Kryptographie und der entsprechenden Kryptoanalyse sowie die Fundamente der Public-Key-Kryptographie mit ausgewählten Anwendungen. Der rote Faden durch das ganze Buch ist die Entwicklung des Begriffes eines sicheren Kryptosystems. Wir beginnen mit den naiven Geheimschriften der Antike und des Mittelalters, fahren mit dem Kerkhoffs-Prinzip der Sicherheit und der perfekten Sicherheit im statistischen Sinn fort und enden mit dem komplexitätstheoretischen Sicherheitskonzept der modernen Kryptosysteme.

Das Buch besteht aus elf Lektionen, jede umfasst 4 bis 12 Unterrichtsstunden. Das Buch bietet Lehrpersonen eine große Auswahl. Mehrere Lektionen sind optional und können ohne Konsequenzen für das Verständnis der nachfolgenden Lektionen übersprungen werden. Jede Lektion bietet mehrere Stufen der Vertiefung, so dass auch nur gewisse Teile im Unterricht behandelt werden können. Alle diese Auswahlmöglichkeiten werden in Hinweisen an die Lehrperson angegeben.

Für ein minimales zugeschnittenes Programm braucht man kein Vorwissen. Für vertiefende Passagen setzen wir elementare Mathematikkenntnisse aus der Kombinatorik, der Wahrscheinlichkeitstheorie und die Fähigkeit lineare Gleichungssysteme zu lösen voraus. Alle anderen Kenntnisse der Algebra und der Zahlentheorie werden mittels entsprechender kryptographischer Motivation direkt im Lehrbuch vermittelt. Somit eignet sich das Lehrbuch für den Informatik- sowie den Mathematikunterricht in der Sekundarstufe II. Dasselbe gilt für die Studiengänge der Informatik und Mathematik an der Hochschule, insbesondere für das Lehramtsstudium.

Es war eine didaktische Herausforderung den Weg zur Public-Key-Kryptographie zugänglich zu machen. Er vermittelt zuerst die grundlegenden Konzepte ohne mathematisches Vorwissen und präsentiert dann in der Vertiefung ein funktionsfähiges Public-Key-Kryptosystem so, dass man es nicht nur zu verwenden versteht, sondern dass man es – es vollkommen verstehend – selber bauen und seine Sicherheit mathematisch beweisen kann. Das ist das erste Mal, dass man eine solche anspruchsvolle Zielsetzung sogar an Gymnasien zu erfüllen versucht. Wie gut uns dies gelungen ist, haben unsere Leserinnen und Leser zu beurteilen.

An dieser Stelle möchten wir uns ganz herzlich bei Frau Lea Burger für die ausgezeichnete Unterstützung bei den sprachlichen Korrekturen und bei Frau Sybille Thelen und Herrn Ulrich Sandten für deren große Geduld und die sehr konstruktive und freundliche Zusammenarbeit bedanken.

Zürich, Juni 2014

Karin Freiermuth
Juraj Hromkovič
Lucia Keller
Björn Steffen

http://www.springer.com/978-3-8348-1855-3

Einführung in die Kryptologie
Lehrbuch für Unterricht und Selbststudium
Freiermuth, K.; Hromkovič, J.; Keller, L.; Steffen, B.
2014, IX, 399 S. 86 Abb., Softcover
ISBN: 978-3-8348-1855-3