Überblick über den Inhalt des CrypTool-Buchs

Mit dem Erfolg des Internets wurden die damit verbundenen Technologien verstärkt erforscht, was auch im Bereich Kryptografie viele neue Erkenntnisse schaffte.

Dieses *Buch zu den CrypTool-Programmen* bietet einen Überblick über die klassische und moderne Kryptografie und leitet zum konkreten Ausprobieren an. Dazu werden die CrypTool-Programme benutzt und ebenso Beispielcode, geschrieben für das Computer-Algebra-System **SageMath** (siehe Anhang A.7).

Das erste Kapitel dieses Buchs beschreibt die Prinzipien der symmetrischen und asymmetrischen **Verschlüsselung** und diskutiert Definitionen und Beispiele für deren Widerstandsfähigkeit.

Im zweiten Kapitel wird – aus didaktischen Gründen – eine ausführliche Übersicht über **Papier- und Bleistiftverfahren** gegeben. Außerdem wird ein typisches Beispiel einer Vor-Computer Maschinen-Chiffre erläutert und beschrieben, wie weit fortgeschritten KI-basierte Angriffe auf diese Hagelin-Maschine sind.

Kapitel 3 gibt einen umfassenden Überblick über **Historische Kryptologie**, ein neu etabliertes Forschungsgebiet, das sich mit den praktischen Problemen bei der Entschlüsselung und Einordnung von verschlüsselten historischen Dokumenten beschäftigt.

Kapitel 4 widmet sich dem faszinierenden Thema der **Primzahlen**. Anschließend führt Kapitel 5 anhand vieler Beispiele in die **modulare Arithmetik** und die **elementare Zahlentheorie** ein. Hier bilden die Eigenschaften des **RSA-Verfahrens** einen Schwerpunkt.

Danach erhalten Sie Einblicke in die mathematischen Konzepte und Ideen hinter der **modernen asymmetrischen Kryptografie** (Kapitel 6) inkl. einer neuen geometrischen Veranschaulichung der Vorgänge bei der RSA-Verschlüsselung.

Kapitel 7 gibt einen knappen Überblick zum Stand der Attacken gegen Passworte und moderne **Hash-Algorithmen**, und widmet sich dann kurz der Authentifizierung in der Praxis und den **digitalen Signaturen und Public-Key-Infrastrukturen** – sie sind unverzichtbarer Bestandteil von E-Business-Anwendungen. Hier werden ganz aktuell die Unterschiede der verschiedenen 2FA- und MFA-Verfahren klar gegenüber gestellt und die Erwartung von NIS-2 dazu verdeutlicht.

Kapitel 8 stellt **elliptische Kurven** vor: Sie sind eine Alternative zu RSA und für die Implementierung auf Chipkarten besonders gut geeignet.

Kapitel 9 führt in die **moderne symmetrische Kryptografie** ein. Boolesche Algebra ist Grundlage der meisten modernen, symmetrischen Verschlüsselungsverfahren, da diese auf Bitströmen und Bitblöcken operieren. Prinzipielle Konstruktionsmethoden dieser Verfahren werden beschrieben und in SageMath implementiert. Dieses Kapitel ist im Vergleich relativ mathematisch.

Kapitel 10 stellt **homomorphe Kryptofunktionen** vor. Homomorphe Verschlüsselung ist ein modernes Forschungsgebiet, das im Zuge des Cloud-Computing sehr an Bedeutung gewinnt.

Kapitel 11 gibt eine sehr einfache **Einführung in die Gitterkryptografie**, ein Gebiet, das Quantencomputer-resistente Verfahren ermöglicht – verbunden mit einigen kryptografischen Rätseln.

Kapitel 12 beschreibt **Aktuelle Resultate zum Lösen diskreter Logarithmen und zur Faktorisierung** und gibt einen breiten Überblick über die zur Zeit besten Algorithmen für (a) das Berechnen diskreter Logarithmen in verschiedenen Gruppen, für (b) das Faktorisierungsproblem und für (c) elliptische Kurven. Dieser Überblick wurde zusammengestellt, nachdem ein provozierender Vortrag auf der Black Hat-Konferenz 2013 für Verunsicherung sorgte, weil er die Fortschritte bei endlichen Körpern mit kleiner Charakteristik fälschlicherweise auf Körper extrapolierte, die in der Realität verwendet werden.

Kapitel 13 **Zukünftige Kryptografie** diskutiert Bedrohungen für bestehende kryptografische Verfahren und stellt die Forschungsansätze (Post-Quantum-Kryptografie) für eine langfristige kryptografische Sicherheit vor incl. der ersten vom NIST 2024 verabschiedeten PQC-Standards.

Die einzelnen Hauptkapitel sind von verschiedenen **(Mit-)Autoren** verfasst (siehe Anhang B.3) und in sich abgeschlossen. Die behandelten Inhalte werden begleitet von zahlreichen Beispielen und SageMath-Listings. Am Ende der meisten Kapitel finden Sie Literaturangaben und Web-Links. Die Kapitel wurden reichlich mit *Fußnoten* versehen, in denen auch darauf verwiesen wird, wie man die beschriebenen Funktionen in den verschiedenen CrypTool-Programmen, in SageMath oder OpenSSL aufruft und ausprobiert.

Während die CrypTool-*E-Learning-Programme* eher den praktischen Umgang motivieren, dient das *Buch* auch dazu, dem an Kryptografie Interessierten ein tieferes Verständnis für die implementierten mathematischen Algorithmen zu vermitteln – und das möglichst gut nachvollziehbar.

Den besten Überblick, welche Funktionen in den CrypTool-Programmen insgesamt zur Verfügung stehen, liefert die ff. Webseite: `https://www.cryptool.org/de/functions/`. Siehe auch Anhang A.1 auf Seite 755.

In diesem Buch geben die Anhänge A.2, A.3, A.4 und A.5 einen Überblick über die vier verschiedenen CrypTool-Varianten via:

- der Funktionsliste und den Menüs von CrypTool 1 (CT1)
- der Funktionsliste und den CrypTool-2-Vorlagen (CT2)
- den JCrypTool-Funktionen (JCT)
- den CrypTool-Online-Anwendungen (CTO)

Zwei weitere Anhänge geben fundierte Einführungen in **SageMath** und **OpenSSL** mit vielen Beispielen. SageMath wird dabei in einen breiteren Kontext gestellt (LaTeX, Python, Jupyter).

Die Programme zu diesem Buch oder spezifische Ergänzungen finden Sie auf der CrypTool-Seite: `https://www.cryptool.org/de/ctbook/`. Zu den Ergänzungen gehört bspw. das 90-seitige Dokument „CUDA Tutorial – Cryptanalysis of Classical Ciphers Using Modern GPUs and CUDA“.[1]

Die Autoren dieses Buchs möchten sich an dieser Stelle bedanken bei den Kollegen in der jeweiligen Firma und an den Universitäten Bochum, Darmstadt, Frankfurt, Gießen, Karlsruhe, Lausanne, München, Paris und Siegen.

Wie auch bei dem E-Learning-Programm CrypTool wächst die Qualität des Buchs mit den Anregungen und Verbesserungsvorschlägen von Ihnen als Leser. Wir freuen uns auf Ihre Rückmeldungen.

Geschlechtsneutrale Formulierung: Aus Gründen der einfacheren Lesbarkeit wird auf geschlechtsspezifische Differenzierung verzichtet. Entsprechende Begriffe wie „Entwickler“ oder „Kryptologe“ gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter.

[1] Es enthält eine praktische Einführung in das Schreiben von CUDA-Programmen unter Linux und Windows.