

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 die aktuellen Unterschiede der verschiedenen 2FA- und MFA-Verfahren (incl. Passkey) 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 Abschnitt A.1 auf Seite 757.

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.

Einleitung zum CrypTool-Buch

Das CrypTool-Buch versucht, die wichtigsten Themen aus der Kryptologie genau und trotzdem möglichst verständlich darzustellen, und zum Ausprobieren anzuleiten. Dazu wurden die Themen sinnvoll in eigenständig lesbare Kapitel unterteilt, damit Entwickler/Autoren unabhängig voneinander mitarbeiten können. Natürlich gäbe es viel mehr Themen aus der Kryptografie, die man vertiefen könnte – deshalb ist diese Auswahl nicht erschöpfend.

In der anschließenden redaktionellen Arbeit wurden Querverweise ergänzt, Fußnoten hinzugefügt, Index-Einträge vereinheitlicht und sehr viele Korrekturen vorgenommen.

Dieses Buch wurde ab dem Jahr 2000 zusammen mit CrypTool 1 (CT1) ausgeliefert. Im Vergleich zur letzten in CT1 beigelegten Version aus 2018 wurden hier die TeX-Sourcen des Dokuments komplett umstrukturiert, etliche Themen neu hinzugefügt, ergänzt, korrigiert, und alles auf den aktuellen Stand gebracht, z. B.:

- ein detaillierter Vergleich zwischen theoretischem und praktischem Schlüsselraum und ein Überblick über die besten bekannten Angriffe gegen verschiedene Chiffren (neu, Kap. 1.7 und 1.9),
- eine detaillierte Erklärung der C(X)-52, der am weitesten verbreiteten mechanischen (Hagelin) Chiffriermaschine, ihre Bedeutung und die Implementierung ihrer Varianten in CT2 (neu, Kap. 2.5),
- das Forschungsgebiet [Historische Kryptologie](#) (neu, Kapitel 3 auf Seite 145),
- generell das Primzahlen-Kapitel und die Liste der größten Primzahlen (Kap. 4.5),
- RSA-2D: eine neue geometrische Veranschaulichung der Vorgänge bei der RSA-Verschlüsselung (neu, Abschnitt 6.5 auf Seite 403),
- Auflistung, in welchen Filmen und Romanen Kryptografie eine wesentliche Rolle spielt (Anhang B.1),
- die Funktionsübersichten zu CrypTool 2 (CT2), zu JCrypTool (JCT) und zu CrypTool-Online (CTO) (siehe Anhang),
- weitere SageMath-Skripte zu Kryptoverfahren, die Einführung in das Computer-Algebra-System SageMath (siehe Anhang A.7) und die Anpassung aller Skripte an die SageMath-Versionen 9.x und 10.x,
- die Einführung in das Kommandozeilen-Tool OpenSSL (neu, Abschnitt A.8 auf Seite 819),
- die Abschnitte über die Goldbach-Vermutung (siehe 4.10.5), über Primzahl-Zwillinge (siehe 4.10.6), und über Primzahl-Lücken (siehe 4.10.8),
- der Abschnitt über gemeinsame Primzahlen in real verwendeten RSA-Moduli (siehe 5.12.5.4),
- die [Grundlagen der modernen symmetrischen Verschlüsselung](#) (stark überarbeitet, Kapitel 9 auf Seite 489),
- die [Einführung in die Gitterkryptografie](#) (neu, Kapitel 11 auf Seite 631),
- das Kapitel über [Diskrete Logarithmen und Faktorisierung](#) (Kapitel 12 auf Seite 717) und
- das Kapitel über die [Zukünftige Kryptografie](#) (Kapitel 13 auf Seite 743).

Dank

An dieser Stelle möchte ich explizit folgenden Personen danken, die bisher in ganz besonderer Weise zum CrypTool-Projekt beigetragen haben. Ohne ihre besonderen Fähigkeiten und ihr großes Engagement wäre CrypTool nicht, was es heute ist:

- Hr. Henrik Koy
- Hr. Jörg-Cornelius Schneider
- Hr. Florian Marchal
- Dr. Peer Wichmann
- Hr. Dominik Schadow
- Prof. Nils Kopal
- Mitarbeiter in den Teams von Prof. Johannes Buchmann, Prof. Claudia Eckert, Prof. Alexander May, Prof. Torben Weis und insbesondere Prof. Arno Wacker.

Dank an Bart Wessel und George Lasry für Informationen über die Unterschiede zwischen den Modellvarianten der C-52/CX-52.

Zu erwähnen sind die Studenten, die durch ihre inzwischen weit über 200 Diplom-, Bachelor- und Masterarbeiten beitrugen. Auch allen hier nicht namentlich Genannten ganz herzlichen Dank für das (meist in der Freizeit) geleistete Engagement.

Danke auch an die Leser, die uns Feedback sandten, und insbesondere an Olaf Ostwald, Helmut Witten, Prof. Ralph-Hardo Schulz und Prof. Gottfried Barthel, die verschiedene Teile des Buchs konstruktiv gegengelesen haben. Und insbesondere an Herbert Voß, der uns immer dann half, wenn es in $\text{\LaTeX}$ schwierig wurde.

Ein besonderes Dankeschön geht an Dr. Doris Behrendt, die die aufwändige Aufgabe übernahm, zwei Bücher mit je 500+ Seiten nach KOMA-Script zu bringen und die TeX-Sourcen aufzuräumen und zu modernisieren, die von unterschiedlichen Autoren über die Jahre erstellt wurden – und die dabei auch noch viele Inhalte kritisch las.

Und schließlich Dank an die Mitarbeiter des Verlags und Herbert Voß, die uns vor allem am Ende halfen, fokussiert zu bleiben.

Die Bereitschaft von Christof Paar, das Vorwort zu schreiben, ist für mich eine große Ehre, und ich möchte ihm an dieser Stelle nochmals danken.

Ich hoffe, dass viele Leser mit diesem Buch mehr Interesse an und Verständnis für dieses moderne und zugleich uralte Thema finden.

Für die zweite deutsche Auflage bei Lehmanns wurden hauptsächlich kleine Fehler korrigiert.

Bernhard Esslinger

Heilbronn/Siegen, September 2025