Cryptool

Cryptool Projekt

19. März 2018

Inhaltsverzeichnis

Vorwort zur 12. Auflage des CrypTool-Buchs

Das CrypTool-Buch versucht, einzelne Themen aus der Mathematik der Kryptologie genau und trotzdem möglichst verständlich zu erläutern.

Dieses Buch wurde ab dem Jahr 2000 – zusammen mit dem CrypTool-1-Paket (CT1) in Version 1.2.01 – ausgeliefert. Seitdem ist das Buch mit fast jeder neuen Version von CT1 und CT2 ebenfalls erweitert und aktualisiert worden.

Themen aus Mathematik und Kryptographie wurden sinnvoll unterteilt und dafür wurden jeweils eigenständig lesbare Kapitel geschrieben, damit Entwickler/Autoren unabhängig voneinander mitarbeiten können. Natürlich gäbe es viel mehr Themen aus der Kryptographie, die man vertiefen könnte – deshalb ist diese Auswahl auch nur eine von vielen möglichen.

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

Im Vergleich zu Ausgabe 11 des Buchs wurden in dieser Ausgabe die TeX-Sourcen des Dokuments komplett überarbeitet (bspw. eine einzige bibtex-Datei für alle Kapitel und beide Sprachen), und etliche Themen ergänzt, korrigiert und auf den aktuellen Stand gebracht, z.B.:

- die größten Primzahlen (Kap. **??**),
- die Auflistung, in welchen Filmen und Romanen Kryptographie eine wesentliche Rolle spielt (siehe Anhang **??**),
- die Funktionsübersichten zu CrypTool 2 (CT2), zu JCrypTool (JCT) und zu CrypTool-Online (CTO) (siehe Anhang),
- weitere SageMath-Skripte zu Kryptoverfahren, und die Einführung in das Computer-Algebra-System (CAS) SageMath (siehe Anhang **??**),
- der Abschnitt über die Goldbach-Vermutung (siehe **??**) und über Primzahl-Zwillinge (siehe **??**),
- der Abschnitt über gemeinsame Primzahlen in real verwendeten RSA-Modulen (siehe **??**),
- die „**??**“ ist völlig neu (siehe Kapitel **??**),
- die Studie „**??**“ ist völlig neu (siehe Kapitel **??**). Das ist ein phantastischer und eingehender Überblick über die Grenzen der entsprechenden aktuellen kryptoanalytischen Methoden.

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
- Mitarbeiter in den Teams von Prof. Johannes Buchmann, Prof. Claudia Eckert, Prof. Alexander May, Prof. Torben Weis und insbesondere Prof. Arno Wacker.

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 ein ganz besonderer Dank für das konstruktive Gegenlesen dieser Version durch Helmut Witten und Prof. Ralph-Hardo Schulz.

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

Bernhard Esslinger

Heilbronn/Siegen, August 2016 + August 2017

PS:

Wir würden uns freuen, wenn sich weitere Autoren finden, die vorhandene Kapitel verbessern oder fundierte Kapitel z.B. zu einem der folgenden Themen ergänzen könnten:

- Riemannsche Zeta-Funktion,
- Hashverfahren und Passwort-Knacken,
- Gitter-basierte Kryptographie,
- Zufallszahlen,
- Format-erhaltende Verschlüsselung,
- Privacy-preserving Kryptographie,
- Design/Angriff auf Krypto-Protokolle (wie SSL).

PPS:

Ausstehende Todos für Edition 12 dieses Buches (bis dahin nennen wir es weiterhin Draft):

- Updaten aller Informationen zu SageMath (Kap. **??** und Appendix) und Testen des Codes gegen das neueste SageMath (Version 8.x), sowohl von der Kommandozeile als auch mit dem SageMathCloud-Notebook.
- Updaten der Funktionslisten zu den vier CT-Versionen (im Appendix).

1 Einführung – Zusammenspiel von Buch und Programmen

Das CrypTool-Buch

Dieses Buch wird zusammen mit den Open-Source-Programmen des CrypTool-Projektes ausgeliefert. Es kann auch direkt auf der Webseite des CT-Portals herunter geladen werden (`https://www.cryptool.org/de/ctp-dokumentation`).

Die Kapitel dieses Buchs sind weitgehend in sich abgeschlossen und können auch unabhängig von den CrypTool-Programmen gelesen werden.

Für das Verständnis der meisten Kapitel reicht Abiturwissen aus. Die Kapitel **??** („Moderne Kryptografie“), **??** („??“), **??** („Bitblock- und Bitstrom-Verschlüsselung“), **??** („??“) und **??** („Resultate für das Lösen diskreter Logarithmen und zur Faktorisierung“)

erfordern tiefere mathematische Kenntnisse.

Die Autoren haben sich bemüht, Kryptographie für eine möglichst breite Leserschaft darzustellen – ohne mathematisch unkorrekt zu werden. Sie wollen die Awareness für die IT-Sicherheit und den Einsatz standardisierter, moderner Kryptographie fördern.

Die Programme CrypTool 1, CrypTool 2 und JCrypTool

CrypTool 1 (CT1) ist ein Lernprogramm, mit dem Sie unter einer einheitlichen Oberfläche kryptographische Verfahren anwenden und analysieren können. Die umfangreicher Onlinehilfe in CT1 enthält nicht nur Anleitungen zur Bedienung des Programms, sondern auch Informationen zu den Verfahren selbst (aber weniger ausführlich und anders strukturiert als im CT-Buch).

CrypTool 1 und die Nachfolgeversionen CrypTool 2 (CT2) und JCrypTool (JCT) werden weltweit in Schule, Lehre, Aus- und Fortbildung eingesetzt.

CrypTool-Online

Die Webseite CrypTool-Online (CTO) (`http://www.cryptool-online.org`), auf der man im Browser oder vom Smartphone aus kryptographische Verfahren ausprobieren und anwenden kann, gehört ebenfalls zum CT-Projekt. Der Umfang von CTO ist bei weitem nicht so groß wie der der Standalone-Programme CT1, CT2 und JCT. Jedoch wird CTO mehr und mehr als Erstkontakt genutzt, weshalb wir Backbone und Frontend momentan mit moderner

Webtechnologie neu designen, um ein schnelles, konsistentes und responsives Look&Feel anzubieten.

MTC3

Der internationale Kryptographie-Wettbewerb MysteryTwister C3 (MTC3) (`http://www.mysterytwisterc3.org`) wird ebenfalls vom CT-Projekt getragen. Hier findet man kryptographische Rätsel in vier verschiedenen Kategorien, eine High-Score-Liste und ein moderiertes Forum. Stand 2016-06-16 sind über 7000 Teilnehmer dabei, und es gibt über 200 Aufgaben, von denen 162 von zumindest einem Teilnehmer gelöst wurden.

Das Computer-Algebra-Programm SageMath

SageMath ist Open-Source und ein umfangreiches Computer-Algebra-System (CAS)-Paket, mit dem sich die in diesem Buch erläuterten mathematischen Verfahren leicht Schritt-für-Schritt programmieren lassen. Eine Besonderheit dieses CAS ist, dass als Skript-Sprache Python (z.Zt. Version 2.x) benutzt wird.

Dadurch stehen einem in Sage-Skripten nach einem import-Befehl auch alle Funktionen der Sprache Pythonn zur Verfügung. SageMath wird mehr und mehr zum Standard-CAS an Hochschulen.

Die Schüler-Krypto-Kurse

Diese Initiative bietet Ein- und Zwei-Tages-Kurse in Kryptologie für Schüler und Lehrer, um zu zeigen, wie attraktiv MINT-Fächer wie Mathematik, Informatik und insbesondere Kryptologie sind. Die Kursidee ist eine virtuelle Geheimagenten-Ausbildung.

Inzwischen finden diese Kurse seit mehreren Jahren in Deutschland in unterschiedlichen Städten statt. Alle Kursunterlagen sind frei erhältlich auf `http://www.cryptool.org/schuelerkrypto/`. Alle eingesetzte Software ist ebenfalls frei (meist wird CT1 und CT2 eingesetzt). Wir würden uns freuen, wenn jemand die Kursunterlagen übersetzt und einen entsprechenden Kurs in Englisch anbieten würde.

Dank

Herzlichen Dank an alle, die mit ihrem großem Einsatz zum Erfolg und zur weiten Verbreitung dieses Projekts beigetragen haben.

Bernhard Esslinger
Heilbronn/Siegen, August 2017