

# Kurzinhaltsverzeichnis

<b>I</b>	<b>Vorbemerkungen</b>	<b>5</b>
	Vorwort von Prof. Paar	6
	Überblick über den Inhalt des CrypTool-Buchs	13
	Einleitung zum CrypTool-Buch	15
<b>II</b>	<b>Hauptteil</b>	<b>19</b>
1	Verschlüsselungen und Angriffe dagegen	21
2	P&B- und Vor-Computer-Chiffren	71
3	Historische Kryptologie	145
4	Primzahlen	191
5	Einführung in die elementare Zahlentheorie mit Beispielen	269
6	Die mathematischen Ideen hinter der modernen (asymmetrischen) Kryptografie	389
7	Hashfunktionen, Authentifizierung, Digitale Signaturen und PKIs	445
8	Elliptische-Kurven-Kryptografie	469
9	Grundlagen der modernen symmetrischen Verschlüsselung	489
10	Homomorphe Chiffren	621
11	Einführung in die Gitterkryptografie	631
12	Diskrete Logarithmen und Faktorisierung	717
13	Zukünftige Kryptografie	743
<b>III</b>	<b>Anhänge</b>	<b>753</b>
A	Software	755
B	Verschiedenes	853
C	Verzeichnisse	873
	Index	887

# Langinhaltsverzeichnis

<b>I</b>	<b>Vorbemerkungen</b>	<b>5</b>
	Vorwort von Prof. Paar	6
	Überblick über den Inhalt des CrypTool-Buchs	13
	Einleitung zum CrypTool-Buch	15
<b>II</b>	<b>Hauptteil</b>	<b>19</b>
<b>1</b>	<b>Verschlüsselungen und Angriffe dagegen</b>	<b>21</b>
1.1	Bedeutung der Kryptologie	23
1.2	Was ist ein Kryptosystem?	24
1.3	Symmetrische Verschlüsselung	24
1.4	Asymmetrische Verschlüsselung	28
1.5	Hybridverfahren	30
1.6	Kerckhoffs' Prinzip	31
1.7	Schlüsselräume – theoretische und praktische	31
1.8	Angriffs-Typen, Sicherheits-Definitionen und n-bit-Sicherheit	38
1.9	Beste bekannte Angriffe auf konkrete Verschlüsselungsverfahren	47
1.10	Algorithmen-Typen und selbstgemachte Chiffren	53
1.11	Weitere Informationsquellen / Empfohlene Bücher	54
1.12	Anhang: AES-Visualisierungen/-Implementierungen	55
1.13	Anhang: Didaktische Beispiele für symmetrische Chiffren mit SageMath	59
	Literatur zu Kapitel 1	62
<b>2</b>	<b>P&amp;B- und Vor-Computer-Chiffren</b>	<b>71</b>
2.1	Transpositionsverfahren	73
2.2	Substitutionsverfahren	78
2.3	Kombination aus Substitution und Transposition	90
2.4	Anderer P&B-Verfahren (auch neuere)	94
2.5	Hagelin-Maschinen als Beispiel für Vor-Computer-Geräte	97
2.6	Anhang: Von ACA definierte Chiffren	111
2.7	Anhang: Ciphertype Detection – Das Verfahren aus dem Geheimtext erschließen	112
2.8	Anhang: OA-Veröffentlichungen über das Knacken von klassischen Chiffren	114
2.9	Anhang: Beispiele mit SageMath	114
	Literatur zu Kapitel 2	140
<b>3</b>	<b>Historische Kryptologie</b>	<b>145</b>
3.1	Einführung und Begriffsdefinitionen	146
3.2	Die Analyse historischer Chiffren – von der Sammlung bis zur Interpretation	156
3.3	Sammlung von Manuskripten und Erstellung von Metadaten	158
3.4	Transkriptionen	160
3.5	Kryptoanalyse	169

3.6	Kontextualisierung und Interpretation: Historische und philologische Analyse . . . . .	181
3.7	Schlussfolgerung . . . . .	184
	Literatur zu Kapitel 3 . . . . .	185
<b>4</b>	<b>Primzahlen</b>	<b>191</b>
4.1	Was sind Primzahlen? . . . . .	192
4.2	Primzahlen in der Mathematik . . . . .	193
4.3	Grafische Darstellung der Primzahlen innerhalb der natürlichen Zahlen . . . . .	194
4.4	Wie viele Primzahlen gibt es? (Satz von Euklid) . . . . .	196
4.5	Die Suche nach sehr großen Primzahlen . . . . .	199
4.6	Primzahltests . . . . .	207
4.7	Spezial-Zahlentypen und die Suche nach einer Formel für Primzahlen . . . . .	217
4.8	Dichte und Verteilung der Primzahlen . . . . .	228
4.9	Ausblick . . . . .	233
4.10	Anmerkungen zu Primzahlen . . . . .	233
4.11	Anhang: Anzahl von Primzahlen in verschiedenen Intervallen . . . . .	254
4.12	Anhang: Indizierung von Primzahlen (n-te Primzahl) . . . . .	256
4.13	Anhang: Größenordnungen / Dimensionen in der Realität . . . . .	257
4.14	Anhang: Spezielle Werte des Zweier- und Zehnersystems . . . . .	258
4.15	Anhang: Visualisierung der Menge der Primzahlen in hohen Bereichen . . . . .	259
4.16	Anhang: Beispiele mit SageMath . . . . .	263
	Literatur zu Kapitel 4 . . . . .	266
<b>5</b>	<b>Einführung in die elementare Zahlentheorie mit Beispielen</b>	<b>269</b>
5.1	Mathematik und Kryptografie . . . . .	270
5.2	Einführung in die Zahlentheorie . . . . .	272
5.3	Primzahlen und der erste Hauptsatz der elementaren Zahlentheorie . . . . .	275
5.4	Teilbarkeit, Modul und Restklassen . . . . .	277
5.5	Rechnen in endlichen Mengen . . . . .	281
5.6	Beispiele für modulares Rechnen . . . . .	282
5.7	Gruppen und modulare Arithmetik über $\mathbb{Z}_n$ und $\mathbb{Z}_n^*$ . . . . .	289
5.8	Euler-Funktion, kleiner Satz von Fermat und Satz von Euler-Fermat . . . . .	292
5.9	Multiplikative Ordnung und Primitivwurzel . . . . .	298
5.10	Beweis des RSA-Verfahrens mit Euler-Fermat . . . . .	305
5.11	Sicherheitsaspekte bei praktischen RSA-Implementierungen . . . . .	309
5.12	Zur Sicherheit des RSA-Verfahrens . . . . .	309
5.13	Anwendungen asymmetrischer Kryptografie mit Zahlenbeispielen . . . . .	327
5.14	Das RSA-Verfahren mit konkreten Zahlen . . . . .	331
5.15	Anhang: Der ggT und die beiden Algorithmen von Euklid . . . . .	340
5.16	Anhang: Abschlussbildung . . . . .	343
5.17	Anhang: Didaktische Bemerkungen zur modulo Subtraktion . . . . .	344
5.18	Anhang: Basisdarstellung von Zahlen, Abschätzung der Ziffernlänge . . . . .	345
5.19	Anhang: Interaktive Präsentation zur RSA-Chiffre . . . . .	348
5.20	Anhang: Beispiele mit SageMath . . . . .	349
5.21	Anhang: Liste der in diesem Kapitel formulierten Definitionen und Sätze . . . . .	383
	Web-Links . . . . .	384
	Literatur zu Kapitel 5 . . . . .	385
<b>6</b>	<b>Die mathematischen Ideen hinter der modernen (asymmetrischen) Kryptografie</b>	<b>389</b>
6.1	Einwegfunktionen mit Falltür und Komplexitätsklassen . . . . .	390
6.2	Knapsackproblem als Basis für Public-Key-Verfahren . . . . .	392
6.3	Primfaktorzerlegung als Basis für Public-Key-Verfahren . . . . .	394

6.4	Der diskrete Logarithmus als Basis für Public-Key-Verfahren . . . . .	398
6.5	Die RSA-Ebene . . . . .	403
6.6	Ausblick . . . . .	443
	Literatur zu Kapitel 6 . . . . .	443
<b>7</b>	<b>Hashfunktionen, Authentifizierung, Digitale Signaturen und PKIs</b>	<b>445</b>
7.1	Hashfunktionen . . . . .	445
7.2	Authentisierung / Authentifizierung in der Praxis . . . . .	451
7.3	Digitale Signaturen . . . . .	457
7.4	Public-Key-Zertifizierung . . . . .	461
	Literatur zu Kapitel 7 . . . . .	465
<b>8</b>	<b>Elliptische-Kurven-Kryptografie</b>	<b>469</b>
8.1	Elliptische Kurven – Ein effizienter Ersatz für RSA? . . . . .	469
8.2	Elliptische Kurven – Historisches . . . . .	471
8.3	Elliptische Kurven – Mathematische Grundlagen . . . . .	472
8.4	Elliptische Kurven in der Kryptografie . . . . .	475
8.5	Verknüpfung auf elliptischen Kurven . . . . .	478
8.6	Sicherheit der Elliptischen-Kurven-Kryptografie: das ECDLP . . . . .	480
8.7	Verschlüsseln und Signieren mithilfe elliptischer Kurven . . . . .	481
8.8	Faktorisieren mit elliptischen Kurven . . . . .	483
8.9	Implementierung elliptischer Kurven zu Lehrzwecken . . . . .	484
8.10	Patentaspekte . . . . .	484
8.11	Elliptische Kurven im praktischen Einsatz . . . . .	486
	Literatur zu Kapitel 8 . . . . .	486
<b>9</b>	<b>Grundlagen der modernen symmetrischen Verschlüsselung</b>	<b>489</b>
9.1	Boolesche Funktionen . . . . .	491
9.2	Block-Chiffren . . . . .	513
9.3	Strom-Chiffren . . . . .	563
9.4	Anhang: Boolesche Abbildungen in SageMath . . . . .	608
9.5	Anhang: Tabelle der SageMath-Beispiele in diesem Kapitel . . . . .	618
	Literatur zu Kapitel 9 . . . . .	619
<b>10</b>	<b>Homomorphe Chiffren</b>	<b>621</b>
10.1	Ursprung und Begriff <i>homomorph</i> . . . . .	621
10.2	Entschlüsselungsfunktion ist Homomorphismus . . . . .	622
10.3	Einordnung homomorpher Verfahren . . . . .	622
10.4	Beispiele für homomorphe Prä-FHE-Chiffren . . . . .	623
10.5	Anwendungen . . . . .	625
10.6	Homomorphe Verfahren in CrypTool . . . . .	626
	Literatur zu Kapitel 10 . . . . .	630
<b>11</b>	<b>Einführung in die Gitterkryptografie</b>	<b>631</b>
11.1	Vorbemerkungen . . . . .	632
11.2	Gleichungen . . . . .	632
11.3	Lineare Gleichungssysteme . . . . .	635
11.4	Matrizen . . . . .	637
11.5	Vektoren . . . . .	641
11.6	Gleichungen – Fortsetzung . . . . .	645
11.7	Vektorräume . . . . .	653
11.8	Gitter . . . . .	658
11.9	Gitter und RSA . . . . .	669

11.10	Gitterbasenreduktion . . . . .	680
11.11	PQC-Standardisierung . . . . .	697
11.12	Anhang: Entsprechende Plugins bei den CrypTool-Programmen . . . . .	698
	Literatur zu Kapitel 11 . . . . .	714
<b>12</b>	<b>Diskrete Logarithmen und Faktorisierung</b>	<b>717</b>
12.1	Generische Algorithmen für das Dlog-Problem in beliebigen Gruppen . . . . .	718
12.2	Beste Algorithmen für Primkörper $\mathbb{F}_p$ . . . . .	721
12.3	Beste bekannte Algorithmen für Erweiterungskörper $\mathbb{F}_{p^n}$ . . . . .	724
12.4	Beste bekannte Algorithmen für die Faktorisierung natürlicher Zahlen . . . . .	729
12.5	Beste bekannte Algorithmen für elliptische Kurven $E$ . . . . .	733
12.6	Die Möglichkeit des Einbettens von Falltürren in kryptografische Schlüssel . . . . .	737
12.7	Abschluss: Vorschlag für die kryptografische Infrastruktur . . . . .	738
	Literatur zu Kapitel 12 . . . . .	740
<b>13</b>	<b>Zukünftige Kryptografie</b>	<b>743</b>
13.1	Verbreitete Verfahren . . . . .	743
13.2	Vorsorge für morgen . . . . .	744
13.3	Neue mathematische Probleme zur Verschlüsselung . . . . .	746
13.4	Neue mathematische Probleme für digitale Signaturen . . . . .	747
13.5	Quantenkryptografie (QKD) versus Post-Quanten-Kryptografie (PQC) . . . . .	747
13.6	Post-Quanten-Kryptografie (PQC) . . . . .	748
13.7	Fazit . . . . .	750
	Literatur zu Kapitel 13 . . . . .	751
<b>III</b>	<b>Anhänge</b>	<b>753</b>
<b>A</b>	<b>Software</b>	<b>755</b>
A.1	Komplett-Übersicht aller Krypto-Funktionen im CT-Projekt . . . . .	757
A.2	Menüs von CrypTool 1 . . . . .	758
A.3	CrypTool 2-Vorlagen und der WorkspaceManager . . . . .	762
A.4	JCrypTool-Funktionen . . . . .	766
A.5	CrypTool-Online-Funktionen . . . . .	768
A.6	Lernprogramm Elementare Zahlentheorie . . . . .	773
A.7	Einführung in das CAS SageMath . . . . .	778
A.8	Kurzeinführung in das CLI openssl . . . . .	819
	Literatur zu Anhang A . . . . .	852
<b>B</b>	<b>Verschiedenes</b>	<b>853</b>
B.1	Filme und belletristische Literatur mit Bezug zur Kryptografie . . . . .	853
B.2	Empfohlene Schreibweise von Begriffen im CrypTool-Buch . . . . .	868
B.3	Autoren des CrypTool-Buchs . . . . .	869
	Literatur zu Anhang B . . . . .	872
<b>C</b>	<b>Verzeichnisse</b>	<b>873</b>
C.1	Abbildungsverzeichnis . . . . .	873
C.2	Tabellenverzeichnis . . . . .	878
C.3	Verzeichnis der Zitate . . . . .	880
C.4	Verzeichnis der Krypto-Verfahren mit Pseudocode . . . . .	881
C.5	Verzeichnis der OpenSSL-Programmbeispiele . . . . .	881
C.6	Verzeichnis der Python-Programmbeispiele . . . . .	882
C.7	Verzeichnis der SageMath-Programmbeispiele . . . . .	882

---

C.8	Verzeichnis der Rätsel von Kapitel 11 . . . . .	885
<b>Index</b>		<b>887</b>