

Kurzinhaltsverzeichnis

I	Vorbemerkungen	5
	Vorwort von Prof. Paar	6
	Überblick über den Inhalt des CrypTool-Buchs	13
	Einleitung zum CrypTool-Buch	15
II	Hauptteil	19
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	267
6	Die mathematischen Ideen hinter der modernen (asymmetrischen) Kryptografie	387
7	Hashfunktionen, Authentifizierung, Digitale Signaturen und PKIs	443
8	Elliptische-Kurven-Kryptografie	467
9	Grundlagen der modernen symmetrischen Verschlüsselung	487
10	Homomorphe Chiffren	619
11	Einführung in die Gitterkryptografie	629
12	Diskrete Logarithmen und Faktorisierung	715
13	Zukünftige Kryptografie	741
III	Anhänge	751
A	Software	753
B	Verschiedenes	851
C	Verzeichnisse	871
	Index	885

Langinhaltsverzeichnis

I	Vorbemerkungen	5
	Vorwort von Prof. Paar	6
	Überblick über den Inhalt des CrypTool-Buchs	13
	Einleitung zum CrypTool-Buch	15
II	Hauptteil	19
1	Verschlüsselungen und Angriffe dagegen	21
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	Schlüsselsräume – 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
2	P&B- und Vor-Computer-Chiffren	71
2.1	Transpositionsverfahren	73
2.2	Substitutionsverfahren	78
2.3	Kombination aus Substitution und Transposition	90
2.4	Andere 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
3	Historische Kryptologie	145
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
4	Primzahlen	191
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	216
4.8	Dichte und Verteilung der Primzahlen	227
4.9	Ausblick	232
4.10	Anmerkungen zu Primzahlen	232
4.11	Anhang: Anzahl von Primzahlen in verschiedenen Intervallen	253
4.12	Anhang: Indizierung von Primzahlen (n-te Primzahl)	254
4.13	Anhang: Größenordnungen / Dimensionen in der Realität	255
4.14	Anhang: Spezielle Werte des Zweier- und Zehnersystems	256
4.15	Anhang: Visualisierung der Menge der Primzahlen in hohen Bereichen	257
4.16	Anhang: Beispiele mit SageMath	261
	Literatur zu Kapitel 4	264
5	Einführung in die elementare Zahlentheorie mit Beispielen	267
5.1	Mathematik und Kryptografie	268
5.2	Einführung in die Zahlentheorie	270
5.3	Primzahlen und der erste Hauptsatz der elementaren Zahlentheorie	273
5.4	Teilbarkeit, Modul und Restklassen	275
5.5	Rechnen in endlichen Mengen	279
5.6	Beispiele für modulares Rechnen	280
5.7	Gruppen und modulare Arithmetik über $\mathbb{Z}_n$ und $\mathbb{Z}_n^*$	287
5.8	Euler-Funktion, kleiner Satz von Fermat und Satz von Euler-Fermat	290
5.9	Multiplikative Ordnung und Primitivwurzel	296
5.10	Beweis des RSA-Verfahrens mit Euler-Fermat	303
5.11	Sicherheitsaspekte bei praktischen RSA-Implementierungen	307
5.12	Zur Sicherheit des RSA-Verfahrens	307
5.13	Anwendungen asymmetrischer Kryptografie mit Zahlenbeispielen	324
5.14	Das RSA-Verfahren mit konkreten Zahlen	329
5.15	Anhang: Der ggT und die beiden Algorithmen von Euklid	339
5.16	Anhang: Abschlussbildung	341
5.17	Anhang: Didaktische Bemerkungen zur modulo Subtraktion	342
5.18	Anhang: Basisdarstellung von Zahlen, Abschätzung der Ziffernlänge	342
5.19	Anhang: Interaktive Präsentation zur RSA-Chiffre	345
5.20	Anhang: Beispiele mit SageMath	346
5.21	Anhang: Liste der in diesem Kapitel formulierten Definitionen und Sätze	380
	Web-Links	381
	Literatur zu Kapitel 5	382
6	Die mathematischen Ideen hinter der modernen (asymmetrischen) Kryptografie	387
6.1	Einwegfunktionen mit Falltür und Komplexitätsklassen	388
6.2	Knapsackproblem als Basis für Public-Key-Verfahren	390
6.3	Primfaktorzerlegung als Basis für Public-Key-Verfahren	392

6.4	Der diskrete Logarithmus als Basis für Public-Key-Verfahren	396
6.5	Die RSA-Ebene	401
6.6	Ausblick	440
	Literatur zu Kapitel 6	440
7	Hashfunktionen, Authentifizierung, Digitale Signaturen und PKIs	443
7.1	Hashfunktionen	443
7.2	Authentisierung / Authentifizierung in der Praxis	449
7.3	Digitale Signaturen	455
7.4	Public-Key-Zertifizierung	459
	Literatur zu Kapitel 7	463
8	Elliptische-Kurven-Kryptografie	467
8.1	Elliptische Kurven – Ein effizienter Ersatz für RSA?	467
8.2	Elliptische Kurven – Historisches	469
8.3	Elliptische Kurven – Mathematische Grundlagen	470
8.4	Elliptische Kurven in der Kryptografie	473
8.5	Verknüpfung auf elliptischen Kurven	476
8.6	Sicherheit der Elliptischen-Kurven-Kryptografie: das ECDLP	478
8.7	Verschlüsseln und Signieren mithilfe elliptischer Kurven	479
8.8	Faktorisieren mit elliptischen Kurven	481
8.9	Implementierung elliptischer Kurven zu Lehrzwecken	482
8.10	Patentaspekte	482
8.11	Elliptische Kurven im praktischen Einsatz	484
	Literatur zu Kapitel 8	484
9	Grundlagen der modernen symmetrischen Verschlüsselung	487
9.1	Boolesche Funktionen	489
9.2	Block-Chiffren	511
9.3	Strom-Chiffren	561
9.4	Anhang: Boolesche Abbildungen in SageMath	606
9.5	Anhang: Tabelle der SageMath-Beispiele in diesem Kapitel	616
	Literatur zu Kapitel 9	617
10	Homomorphe Chiffren	619
10.1	Ursprung und Begriff <i>homomorph</i>	619
10.2	Entschlüsselungsfunktion ist Homomorphismus	620
10.3	Einordnung homomorpher Verfahren	620
10.4	Beispiele für homomorphe Prä-FHE-Chiffren	621
10.5	Anwendungen	623
10.6	Homomorphe Verfahren in CrypTool	624
	Literatur zu Kapitel 10	628
11	Einführung in die Gitterkryptografie	629
11.1	Vorbemerkungen	630
11.2	Gleichungen	630
11.3	Lineare Gleichungssysteme	633
11.4	Matrizen	635
11.5	Vektoren	639
11.6	Gleichungen – Fortsetzung	643
11.7	Vektorräume	651
11.8	Gitter	656
11.9	Gitter und RSA	667

11.10	Gitterbasenreduktion	678
11.11	PQC-Standardisierung	695
11.12	Anhang: Entsprechende Plugins bei den CrypTool-Programmen	696
	Literatur zu Kapitel 11	712
12	Diskrete Logarithmen und Faktorisierung	715
12.1	Generische Algorithmen für das Dlog-Problem in beliebigen Gruppen	716
12.2	Beste Algorithmen für Primkörper $\mathbb{F}_p$	719
12.3	Beste bekannte Algorithmen für Erweiterungskörper $\mathbb{F}_{p^n}$	722
12.4	Beste bekannte Algorithmen für die Faktorisierung natürlicher Zahlen	727
12.5	Beste bekannte Algorithmen für elliptische Kurven E	731
12.6	Die Möglichkeit des Einbettens von Falltüren in kryptografische Schlüssel	735
12.7	Abschluss: Vorschlag für die kryptografische Infrastruktur	736
	Literatur zu Kapitel 12	738
13	Zukünftige Kryptografie	741
13.1	Verbreitete Verfahren	741
13.2	Vorsorge für morgen	742
13.3	Neue mathematische Probleme zur Verschlüsselung	744
13.4	Neue mathematische Probleme für digitale Signaturen	745
13.5	Quantenkryptografie (QKD) – Ein Ausweg?	745
13.6	Post-Quanten-Kryptografie (PQC)	746
13.7	Fazit	748
	Literatur zu Kapitel 13	749
III	Anhänge	751
A	Software	753
A.1	Komplett-Übersicht aller Krypto-Funktionen im CT-Projekt	755
A.2	Menüs von CrypTool 1	756
A.3	CrypTool 2-Vorlagen und der WorkspaceManager	760
A.4	JCrypTool-Funktionen	764
A.5	CrypTool-Online-Funktionen	766
A.6	Lernprogramm Elementare Zahlentheorie	771
A.7	Einführung in das CAS SageMath	776
A.8	Kurzeinführung in das CLI openssl	817
	Literatur zu Anhang A	850
B	Verschiedenes	851
B.1	Filme und belletristische Literatur mit Bezug zur Kryptografie	851
B.2	Empfohlene Schreibweise von Begriffen im CrypTool-Buch	866
B.3	Autoren des CrypTool-Buchs	867
	Literatur zu Anhang B	870
C	Verzeichnisse	871
C.1	Abbildungsverzeichnis	871
C.2	Tabellenverzeichnis	876
C.3	Verzeichnis der Zitate	878
C.4	Verzeichnis der Krypto-Verfahren mit Pseudocode	879
C.5	Verzeichnis der OpenSSL-Programmbeispiele	879
C.6	Verzeichnis der Python-Programmbeispiele	880
C.7	Verzeichnis der SageMath-Programmbeispiele	880

C.8	Verzeichnis der Rätsel von Kapitel 11	883
	Index	885