

Albrecht Beutelspacher  
Heike B. Neumann  
Thomas Schwarzpaul

**Kryptografie  
in Theorie und Praxis**

## **Aus dem Programm**

### **Mathematik/Kryptografie**

#### **Diskrete Mathematik**

von M. Aigner

#### **Diskrete Mathematik für Einsteiger**

von A. Beutelspacher und M.-A. Zschiegner

#### **Lineare Algebra**

von A. Beutelspacher

#### **Lineare Algebra Interaktiv (CD-ROM)**

von A. Beutelspacher und M.-A. Zschiegner

#### **Kryptologie**

von A. Beutelspacher

#### **Moderne Verfahren der Kryptographie**

von A. Beutelspacher, J. Schwenk und K.-D. Wolfenstetter

#### **Verschlüsselungsalgorithmen**

von G. Brands

#### **Algebraische Grundlagen der Informatik**

von K.-U. Witt

#### **Mathematik für Informatiker**

von P. Hartmann

Albrecht Beutelspacher  
Heike B. Neumann  
Thomas Schwarzpaul

# **Kryptografie in Theorie und Praxis**

**Mathematische Grundlagen für elektronisches  
Geld, Internetsicherheit und Mobilfunk**



Bibliografische Information Der Deutschen Bibliothek  
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;  
detaillierte bibliografische Daten sind im Internet über <<http://dnb.ddb.de>> abrufbar.

**Prof. Dr. Albrecht Beutelspacher**

**Thomas Schwarzpaul**

Universität Gießen

Mathematisches Institut

Arndtstraße 2

35392 Gießen

E-Mail: [albrecht.beutelspacher@math.uni-giessen.de](mailto:albrecht.beutelspacher@math.uni-giessen.de)

[thomas.schwarzpaul@math.uni-giessen.de](mailto:thomas.schwarzpaul@math.uni-giessen.de)

**Dr. Heike B. Neumann**

Mühlendamm 45 a

22087 Hamburg

E-Mail: [heike.neumann@philips.com](mailto:heike.neumann@philips.com)

1. Auflage Januar 2005

Alle Rechte vorbehalten

© Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH, Wiesbaden 2005

Lektorat: Ulrike Schmickler-Hirzebruch / Petra Rußkamp

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.

[www.vieweg.de](http://www.vieweg.de)



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Umschlaggestaltung: Ulrike Weigel, [www.CorporateDesignGroup.de](http://www.CorporateDesignGroup.de)

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

ISBN 978-3-528-03168-8

ISBN 978-3-322-93902-9 (eBook)

DOI 10.1007/978-3-322-93902-9

## Vorwort

Kryptografie ist eine alte Kunst und eine moderne Wissenschaft. Die Anfänge der Kunst, geheime Nachrichten zu erzeugen, verlieren sich im Dunkel der Geschichte. Schon 500 v. Chr. haben die Spartaner die Skytala benutzt, und vor 2000 Jahren hat Julius Cäsar im Gallischen Krieg schon die Cäsar-Chiffre eingesetzt. Die Skytala war ein Zylinder, um den ein Band gewickelt wurde, auf den der Klartext längs geschrieben wurde; das Band konnte ohne Gefahr übermittelt werden, und nur ein Empfänger mit einem Zylinder richtiger Größe konnte den Text entziffern. Bei der Cäsar-Chiffre benutzt man das normale Alphabet, unter dem ein um einige Stellen verschobenes Alphabet steht. Verschlüsselt wird, indem ein Buchstabe des Klartextalphabets durch den darunter stehenden Buchstaben des Geheimentextalphabets ersetzt wird. Die Bedeutung der Skytala und der Cäsar-Chiffre liegen u.a. darin, dass sie die Prototypen einer Transpositions- bzw. einer Substitutions-Chiffre sind. Bis vor wenigen Jahrzehnten war ernsthafte Kryptografie eine Domäne der Politiker, Diplomaten und Militärs und der entsprechenden Institutionen. Das Ziel war stets, Verfahren zu entwickeln und zu verwenden, die vom Gegner nicht gebrochen werden konnten bzw. die Verfahren der Gegner zu brechen. Die Tatsache, dass heute die Kryptografie eine nie zuvor gekannte Bedeutung hat, liegt entscheidend an der Entwicklung des Computers und der Computernetze, insbesondere des Internets. Die ersten Computer wurden gegen Ende des 2. Weltkriegs entwickelt, um Geheimcodes brechen zu können, und zwar ging es um die effiziente Verarbeitung der abgefangenen Geheimentexte. Viel später, in den 70er Jahren des vergangenen Jahrhunderts wurden Rechner eingesetzt, um komplexe Verschlüsselungsverfahren realisieren zu können. Der Übergang von den mechanischen und elektromechanischen Verschlüsselungsgeräten (wie zum Beispiel ENIGMA) zu den in Soft- und Hardware ausführbaren Codes, wie etwa dem DES, stellt einen enormen Sprung in der Qualität der Kryptosysteme dar. Das Internet und andere Netze, wie etwa das Mobilfunknetz, haben diese Tendenzen noch einmal verstärkt. Zunächst sind die Angriffsmöglichkeiten durch die Möglichkeit der effizienten Zusammenarbeit von sehr vielen Rechnern enorm gestiegen. In der Tat wurden zum Beispiel einige Faktorisierungsversuche erst durch einen massiven Verbund von Rechnern im Internet möglich. Andererseits hat das Internet die Entwicklung von Algorithmen und v.a. Protokollen notwendig gemacht. Denn zunächst waren in den Internetprotokollen keinerlei Sicherheitsmechanismen vorgesehen, aber es ist klar, dass man für Anwendungen wie Abruf sensibler Daten (z.B. Passwörter, medizinischer Daten oder Konstruktionsunterlagen) oder Bezahlvorgänge Sicherheit mit sehr guter Qualität braucht. Spätestens bei solchen Anwendungen wird auch klar, dass zu dem Ziel der Geheimhaltung ein weiteres Hauptziel der Kryptografie hinzukommt, nämlich die Authentifikation, d.h. die Echtheit von Daten.

Spätestens seit den Arbeiten von Claude Shannon, mit denen er Ende des

2. Weltkriegs die Kryptografie neu begründet hat, ist diese eine mathematische Wissenschaft geworden. Natürlich gehört zu einer Realisierung einer kryptografischen Anwendung die Arbeit der Informatiker, Ingenieure usw., aber ohne die mathematische Fundierung bei der Konstruktion und Analyse von Sicherheitsverfahren stünden alle auf tönernen Füßen. Die 70er und 80er Jahre des 20. Jahrhunderts waren gekennzeichnet durch die Entdeckung und Entwicklung vieler neuer Verfahren, die die Kryptografie revolutioniert haben: Neben dem schon erwähnten DES ist dies v.a. die Entdeckung der Public-Key-Kryptografie mit den zugehörigen Algorithmen RSA und ElGamal, sowie der Zero-Knowledge-Verfahren. Heute befinden wir uns in einer Konsolidierungsphase, die gekennzeichnet ist durch systematische Aufbereitung, Klärung der Begriffsstruktur und weitgehende mathematische Durchdringung der Verfahren. Damit werden zum ersten Mal Lehrbücher der Kryptografie möglich. Die Bücher der letzten Jahrzehnte waren Forschungsberichte, stellten einzelne Teilgebiete vor oder dienten schlicht dazu, dieses Gebiet bekannt zu machen.

Dieses Buch ist ein Lehrbuch der Kryptografie, das auf vielen Vorlesungen der Autoren an der Universität Gießen beruht. Wir haben versucht, alle wesentlichen Aspekte der Kryptografie darzustellen. Dabei haben wir uns um eine Balance bemüht, die allen Aspekten der Kryptografie gerecht wird: Symmetrische und asymmetrische (public key) Kryptografie werden beide ausführlich dargestellt. Innerhalb der Gebiete werden Algorithmen ihrer Bedeutung gemäß dargestellt. Schließlich behandeln wir nicht nur Algorithmen, sondern auch Protokolle. Im Einzelnen geht es dabei um folgende Themen:

Kapitel 1 ist eine kurze Einführung in die Kryptografie und stellt die wichtigsten Begriffe, die in den folgenden Kapiteln benötigt werden, vor. Das Buch gliedert sich dann in drei Teile, wobei im ersten Teil, den Kapiteln 2 bis 8, die symmetrischen Verfahren behandelt werden. In Kapitel 2 werden historische Verfahren, wie die bereits erwähnte Cäsar-Chiffre und Vigenère-Chiffre dargestellt. Die grundlegenden Begriffe der symmetrischen Kryptografie werden in den Kapiteln 3 bis 5 dargestellt. Im Vordergrund stehen dabei das formale Modell zur Beschreibung kryptografischer Verfahren von Shannon und die Begriffe perfekte Sicherheit und effiziente Sicherheit. Kapitel 6 und 7 zeigen, wie man praktische symmetrische Verfahren konstruiert. In Kapitel 6 werden die Stromchiffren, Verfahren die etwa im Mobilfunk eingesetzt werden, vorgestellt. Ein weiterer Schwerpunkt dieses Kapitels ist die Analyse linearer Schieberegister, die man zur Konstruktion von Stromchiffren verwenden kann. Kapitel 7 behandelt die zweite Klasse symmetrischer Verfahren, die Blockchiffren. Es werden die beiden prominentesten Vertreter, der DES und sein Nachfolger der AES, ausführlich dargestellt. Abgeschlossen wird das Gebiet der symmetrischen Verfahren durch Kapitel 8, in dem die wichtigsten Betriebsmodi vorgestellt werden. Betriebsmodi beschreiben, wie man eine Blockchiffre auf lange Nachrichten anwendet.

Der zweite Teil des Buches gilt den Public-Key-Verfahren. Kapitel 9 gibt eine kurze Einführung in die Public-Key-Kryptografie, so wie einen Vergleich mit den symmetrischen Verfahren. Kapitel 10 und 11 beschäftigen sich mit den beiden

---

wichtigsten Public-Key-Verfahren, dem RSA-Algorithmus bzw. dem ElGamal-Verschlüsselungsverfahren. Im zwölften Kapitel werden weitere Public-Key-Verfahren, wie das Rabin-Verschlüsselungsverfahren vorgestellt. Um die Sicherheit von Public-Key-Verschlüsselungsverfahren formal beschreiben zu können, werden in Kapitel 13 die Begriffe polynomielle Ununterscheidbarkeit und semantische Sicherheit eingeführt. Die Sicherheit der RSA- und der ElGamal-Signatur wird in Kapitel 14 diskutiert.

Der dritte Teil des Buches beschäftigt sich mit kryptografischen Anwendungen. Kapitel 15 behandelt die Konstruktion von Hashfunktionen und das Problem der Nachrichtenauthentizität. Kapitel 16 ist von besonderer Bedeutung, da dort die Zero-Knowledge-Protokolle behandelt werden, die einen wichtigen Baustein für komplexere kryptografische Protokolle bilden. Die Schlüsselverwaltung ist das zentrale Thema des siebzehnten Kapitels, dem sich ein Kapitel über Teilnehmerauthentifikation anschließt. In Kapitel 19 werden die wichtigsten Schlüsseltablierungsprotokolle dargestellt und im zwanzigsten Kapitels geht es um Protokolle, an deren Durchführung mehr als zwei Parteien beteiligt sein können. Beispielsweise um ein Geheimnis aufzuteilen. Kapitel 21 geht der Frage nach, wie man Anonymität in kryptografischen Anwendungen erreichen kann. Zwei der wichtigsten Anwendungen, das elektronische Geld und die elektronischen Wahlen, werden hier dargestellt. Internetsicherheit ist das Thema von Kapitel 22. Hier werden das Secure Sockets Layer Protokoll und Pretty Good Privacy vorgestellt. Im abschließenden letzten Kapitel findet sich eine Einführung in das Gebiet der Quantenkryptografie und des Quantencomputing.

Das Buch ist ein Buch, das sich zum Selbststudium, aber auch zum Gebrauch neben Vorlesungen eignet. Obwohl die Kryptografie eine mathematische Disziplin ist, benötigt man nur relativ wenige explizite mathematische Vorkenntnisse. Man braucht ein bisschen Algebra und Zahlentheorie (vor allem bei den Public-Key-Algorithmen) und in manchen Kapiteln Grundkenntnisse der Stochastik. Die meisten benötigten Begriffe und Ergebnisse werden in diesem Buch noch einmal erarbeitet, aber natürlich setzen wir eine gewisse Routine bei der mathematischen Argumentation voraus. Die Übungsaufgaben dienen zur Vertiefung des Stoffes.

Gießen, im November 2004

Albrecht Beutelspacher  
Heike Neumann  
Thomas Schwarzpaul

# Inhaltsverzeichnis

<b>1</b>	<b>Aufgaben und Grundzüge der Kryptografie</b>	<b>1</b>
1.1	Geheimhaltung - Vertraulichkeit - der passive Angreifer . . . . .	3
1.2	Authentifikation und Integrität . . . . .	7
1.3	Andere Sicherheitsmechanismen: Steganographie, physikalische Sicherheit . . . . .	9
1.4	Dienste, Mechanismen, Algorithmen . . . . .	9
<b>I</b>	<b>Symmetrische Verschlüsselungen</b>	<b>11</b>
<b>2</b>	<b>Historisches</b>	<b>13</b>
2.1	Monoalphabetische Chiffren . . . . .	13
2.1.1	Transpositionen . . . . .	13
2.1.2	Cäsar-Chiffren . . . . .	13
2.1.3	Monoalphabetische Chiffren . . . . .	14
2.2	Polyalphabetische Chiffren . . . . .	15
2.2.1	Vigenère-Chiffre . . . . .	15
2.2.2	Grundidee der Kryptoanalyse . . . . .	16
2.2.3	Der Kasiski-Angriff . . . . .	16
2.2.4	Der Friedman-Angriff . . . . .	17
<b>3</b>	<b>Formalisierung und Modelle</b>	<b>22</b>
3.1	Das Modell von Shannon . . . . .	22
3.2	Mathematische Formalisierung . . . . .	23
3.3	Angriffsarten auf Verschlüsselungen . . . . .	24
3.4	Übungen . . . . .	29
<b>4</b>	<b>Perfekte Sicherheit</b>	<b>32</b>
4.1	Formalisierung der perfekten Sicherheit . . . . .	33
4.2	Perfekte Ununterscheidbarkeit . . . . .	41
4.3	Übungen . . . . .	43
<b>5</b>	<b>Effiziente Sicherheit - Computational Security</b>	<b>46</b>
5.1	Algorithmen . . . . .	46
5.2	Komplexitätstheorie . . . . .	49
5.3	Effiziente Sicherheit . . . . .	49



---

<b>6</b>	<b>Stromchiffren</b>	<b>52</b>
6.1	Pseudozufallszahlen . . . . .	53
6.2	Statistische Tests . . . . .	54
6.3	Lineare Schieberegister . . . . .	55
6.4	Vorhersagbarkeit von linearen Schieberegistern . . . . .	63
6.5	Kombinationen von linearen Schieberegistern . . . . .	64
6.6	Lineare Komplexität . . . . .	65
<b>7</b>	<b>Blockchiffren</b>	<b>68</b>
7.1	Vollständige Schlüsselsuche . . . . .	69
7.2	Wertetabellen . . . . .	70
7.3	Folgerungen . . . . .	71
7.4	Designkriterien . . . . .	72
7.5	Feistel-Chiffren . . . . .	74
7.6	Der Data Encryption Standard - DES . . . . .	76
7.6.1	Das Schema . . . . .	76
7.6.2	Die Rundenfunktion . . . . .	77
	Die Expansionsabbildung . . . . .	78
	Die S-Boxen . . . . .	78
	Permutation . . . . .	80
	Zusammenspiel der Einzelkomponenten . . . . .	80
7.6.3	Schlüsselauswahl . . . . .	81
7.6.4	Eigenschaften des DES, Ergebnisse, Bewertung . . . . .	82
7.7	Der Advanced Encryption Standard (AES) . . . . .	83
7.7.1	Das Schema des AES . . . . .	84
7.7.2	Algebraische Grundlagen . . . . .	86
7.8	Die Rundenfunktion . . . . .	87
7.8.1	Schlüsselauswahl . . . . .	89
7.8.2	Entschlüsselung . . . . .	90
7.8.3	Bewertung . . . . .	90
<b>8</b>	<b>Kaskadenverschlüsselungen und Betriebsmodi</b>	<b>92</b>
8.1	Kaskadenverschlüsselungen . . . . .	92
8.1.1	Two-Key-Triple-DES . . . . .	94
8.2	Betriebsmodi . . . . .	94
8.2.1	Der Electronic-Codebook-Modus . . . . .	95
8.2.2	Cipher-Block-Chaining-Modus . . . . .	97
8.2.3	Counter-Modus . . . . .	99
8.2.4	Cipher-Feedback-Modus . . . . .	100
8.2.5	Output-Feedback-Modus . . . . .	102

<b>II</b>	<b>Asymmetrische Kryptografie</b>	<b>105</b>
<b>9</b>	<b>Einführung in die Public-Key-Kryptografie</b>	<b>107</b>
9.1	Public-Key-Verschlüsselung . . . . .	107
9.2	Digitale Signaturen . . . . .	111
9.3	Einwegfunktionen . . . . .	114
9.4	Vergleich Symmetrische-Asymmetrische Algorithmen . . . . .	115
<b>10</b>	<b>Der RSA-Algorithmus</b>	<b>117</b>
10.1	Überblick . . . . .	117
10.2	Die Schlüsselerzeugung . . . . .	119
10.3	Verschlüsseln und Entschlüsseln . . . . .	123
10.4	Der RSA-Pseudozufallsgenerator . . . . .	127
10.5	Die Sicherheit des RSA-Algorithmus . . . . .	127
10.6	Homomorphie der RSA-Funktion . . . . .	130
10.7	Konkrete Implementierungen . . . . .	131
<b>11</b>	<b>Der diskrete Logarithmus, Diffie-Hellman-Schlüsselvereinbarung, ElGamal-Systeme</b>	<b>134</b>
11.1	Überblick über die Diffie-Hellman-Schlüsselvereinbarung . . . . .	134
11.2	Mathematische Details . . . . .	135
11.3	Das Problem des diskreten Logarithmus . . . . .	137
11.4	Der Baby-Step-Giant-Step-Algorithmus . . . . .	138
11.5	Sicherheit der Diffie-Hellman-Schlüsselvereinbarung . . . . .	139
11.6	ElGamal-Verschlüsselung . . . . .	140
11.7	ElGamal-Signatur . . . . .	141
11.8	Der Blum-Micali-Pseudozufallsgenerator . . . . .	144
<b>12</b>	<b>Weitere Public-Key-Systeme</b>	<b>147</b>
12.1	Verallgemeinerte ElGamal-Systeme - elliptische Kurven . . . . .	147
12.2	XTR . . . . .	152
12.3	Kryptosysteme auf der Basis der Faktorisierung . . . . .	153
12.3.1	Die Rabin-Verschlüsselung und -Signatur . . . . .	153
	Das Rabin-Verschlüsselungsverfahren . . . . .	154
	Das Rabin-Signaturverfahren . . . . .	155
	Der Blum-Blum-Shub-Generator . . . . .	156
12.3.2	Paillier-Verschlüsselungen und -Signaturen . . . . .	156
12.4	Kryptosysteme auf anderen schwierigen Problemen . . . . .	157
12.4.1	McEliece-Verschlüsselungen . . . . .	157
12.4.2	Knapsack-Verschlüsselungen . . . . .	157
12.4.3	NTRU . . . . .	158
12.4.4	Hidden Field Equations . . . . .	158

---

<b>13 Sicherheit von Public-Key-Verschlüsselungsverfahren</b>	<b>160</b>
13.1 Polynomielle Ununterscheidbarkeit . . . . .	161
13.2 Semantische Sicherheit . . . . .	163
13.3 Die Sicherheit des RSA- und des ElGamal-Verschlüsselungs- verfahrens . . . . .	165
<b>14 Digitale Signaturen</b>	<b>169</b>
14.1 Vergleich von RSA- und ElGamal-Signaturen . . . . .	172
 <b>III Anwendungen</b>	 <b>175</b>
<b>15 Hashfunktionen und Nachrichtenauthentizität</b>	<b>177</b>
15.1 Hashfunktionen . . . . .	178
15.2 Konstruktion von Hashfunktionen . . . . .	182
15.2.1 Hashfunktionen unter Verwendung von Blockchiffren . . . .	183
15.2.2 Maßgeschneiderte Algorithmen . . . . .	185
15.2.3 Hashfunktion mit modularer Arithmetik . . . . .	186
15.3 Hash-and-Sign-Signaturen . . . . .	187
15.4 Message Authentication Codes . . . . .	189
15.5 Konstruktion mit Blockchiffren . . . . .	191
15.6 Konstruktionen mit Hashfunktionen . . . . .	193
15.7 Sichere Kanäle . . . . .	194
<b>16 Zero-Knowledge-Protokolle</b>	<b>196</b>
16.1 Der Fiat-Shamir-Algorithmus . . . . .	198
16.2 Zero-Knowledge-Beweis für die Kenntnis eines diskreten Loga- rithmus . . . . .	200
16.3 Formalisierung . . . . .	201
16.4 Witness hiding . . . . .	205
<b>17 Schlüsselverwaltung</b>	<b>208</b>
17.1 Schlüsselerzeugung . . . . .	208
17.2 Schlüsselverteilung . . . . .	209
17.3 Speicherung von Schlüsseln . . . . .	211
17.4 Rückruf von Schlüsseln . . . . .	211
17.5 Zerstörung von Schlüsseln . . . . .	212
17.6 Public-Key-Infrastrukturen . . . . .	212
17.6.1 Public-Key-Zertifikate . . . . .	213
<b>18 Teilnehmerauthentifikation</b>	<b>217</b>
18.1 Festcode-Verfahren . . . . .	219
18.2 Wechselcode-Verfahren . . . . .	220
18.3 Challenge-and-Response-Protokolle . . . . .	222
18.4 Authentifikation mit Zero-Knowledge-Beweisen . . . . .	224

18.5	Eigenschaften von Authentifikationsprotokollen . . . . .	226
<b>19</b>	<b>Schlüsseletablierungsprotokolle</b>	<b>229</b>
19.1	Angriffe auf Protokolle . . . . .	230
19.1.1	Die Impersonation . . . . .	231
19.1.2	Die Replay-Attacke . . . . .	232
19.1.3	Reflektionsangriff . . . . .	233
19.1.4	Der Man-in-the-middle-Angriff . . . . .	234
19.2	Schlüsseltransportprotokolle . . . . .	235
19.2.1	Das Breitmaulfrosch-Protokoll . . . . .	236
19.2.2	Needham-Schroeder-Protokoll . . . . .	237
19.2.3	Otway-Rees-Protokoll . . . . .	238
19.2.4	Das TMN-Protokoll . . . . .	239
19.3	Schlüsselvereinbarungsprotokolle . . . . .	241
19.4	Sicherheit von Protokollen . . . . .	246
<b>20</b>	<b>Multiparty-Computations</b>	<b>250</b>
20.1	Modell . . . . .	250
20.2	Secret-Sharing-Verfahren . . . . .	253
20.2.1	Schwellenschemata . . . . .	255
	Das Schwellenschema von Shamir . . . . .	255
20.2.2	Verifizierbare Geheimnisaufteilung . . . . .	257
20.3	Threshold-Signaturverfahren . . . . .	258
20.4	Der Münzwurf am Telefon . . . . .	260
20.5	Oblivious-Transfer . . . . .	261
<b>21</b>	<b>Anonymität</b>	<b>266</b>
21.1	MIX-Netze . . . . .	266
21.1.1	Kryptografische Sicherheit eines MIXes . . . . .	269
21.1.2	Weitere Sicherheitsmaßnahmen . . . . .	270
21.2	Blinde Signaturen . . . . .	271
21.2.1	Elektronisches Geld . . . . .	272
21.3	Pseudonyme . . . . .	274
21.3.1	Elektronische Wahlen . . . . .	275
<b>22</b>	<b>Internetsicherheit</b>	<b>277</b>
22.1	Secure Sockets Layer (SSL) . . . . .	277
22.1.1	Das Handshake-Protokoll . . . . .	278
22.1.2	Change-Cipher-Spec-Nachricht . . . . .	282
22.1.3	Record-Layer-Protokoll . . . . .	283
22.1.4	Alert-Protokoll . . . . .	283
22.1.5	Analyse des SSL-Protokolls Version 3.0 . . . . .	284
22.2	Pretty Good Privacy . . . . .	285
22.2.1	Operationen . . . . .	285
22.2.2	Schlüsselverwaltung . . . . .	286

---

<b>23 Quantenkryptografie und Quanten Computing</b>	<b>289</b>
23.1 Quantenkryptografie . . . . .	289
23.2 Quanten Computing . . . . .	292
23.2.1 Physikalische Grundlagen . . . . .	292
23.2.2 Quantencomputer . . . . .	294
23.2.3 Faktorisierung mit Quantencomputern . . . . .	295
23.2.4 Auswirkungen auf die Kryptografie . . . . .	297
23.2.5 Ausblick . . . . .	298
<b>Literaturverzeichnis</b>	<b>299</b>
<b>Index</b>	<b>313</b>

