

APPENDIX C

UMMU
TK
5105.59
.B871
2001
bks

PR  SS

RSA Security's Official Guide to **CRYPTOGRAPHY**

Learn how secure data-encryption
techniques work

Protect confidential information
on your network

Get official current cryptography
standards on enclosed CD-ROM

Steve Burnett & Stephen Paine

RSA Security's Official Guide to Cryptography

Steve Burnett and Stephen Paine

Osborne/McGraw-Hill

New York Chicago San Francisco
Lisbon London Madrid Mexico City
Milan New Delhi San Juan
Seoul Singapore Sydney Toronto

UMRI
TK
5105.59
.B871
200f
bks

Osborne/McGraw-Hill
2600 Tenth Street
Berkeley, California 94710
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact **Osborne/McGraw-Hill** at the above address. For information on translations or book distributors outside the U.S.A., please see the International Contact Information page immediately following the index of this book.

RSA Security's Official Guide to Cryptography

Copyright © 2001 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

234567890 FGR FGR 01987654321

Book p/n 0-07-213138-1 and CD p/n 0-07-213137-3
parts of
ISBN 0-07-213139-X

Publisher

Brandon A. Nordin

**Vice President &
Associate Publisher**

Scott Rogers

Executive Editor

Steven Elliot

Senior Project Editor

LeeAnn Pickrell

Acquisitions Coordinator

Alexander Corona

Technical Editors

Blake Dournaee

Jessica Nelson

Copy Editor

Betsy Hardinger

Composition and Indexer

MacAllister Publishing Services, LLC

Illustrators

Michael Mueller

Beth Young

Lyssa Sieben-Wald

Information has been obtained by **Osborne/McGraw-Hill** from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, **Osborne/McGraw-Hill**, or others, **Osborne/McGraw-Hill** does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from use of such information.

UMMA/bks
41413416
eHY
2-7-02

To Pao-Chi, Gwen, Ray, Satomi, Michelle, Alexander,
Warren, Maria, Daniel, and Julia

—*Steve Burnett*

To Danielle, thanks for understanding while I worked on
this book

To Alexis and Elizabeth, a father could not ask for better
children

—*Stephen Paine*

Contents

Credits	xiii
Foreword	xv
Acknowledgments	xvii
Preface	xix
About the Authors	xxii
Chapter 1 Why Cryptography?	1
Security Provided by Computer Operating Systems	2
How Operating Systems Work	2
Default OS Security: Permissions	3
Attacks on Passwords	4
Attacks That Bypass Operating Systems	6
Data Recovery Attack	6
Memory Reconstruction Attack	9
Added Protection Through Cryptography	11
The Role of Cryptography in Data Security	12
Chapter 2 Symmetric-Key Cryptography	15
Some Crypto Jargon	18
What Is a Key?	20
Why Is a Key Necessary?	22
Generating a Key	22
A Random Number Generator	27
A Pseudo-Random Number Generator	28
Attacks on Encrypted Data	30
Attacking the Key	30
Breaking the Algorithm	36
Measuring the Time It Takes to Break Your Message	37
Symmetric Algorithms: The Key Table	37
Symmetric Algorithms: Block Versus Stream Ciphers	38
Block Ciphers	38
Stream Ciphers	41
Block Versus Stream: Which Is Better?	45
Digital Encryption Standard	46
Triple DES	47
Commercial DES Replacements	49
Advanced Encryption Standard	50

Summary	51
Real-World Example: Oracle Databases	51
Chapter 3 Symmetric-Key Management	53
Password-Based Encryption	54
Programming Convenience	59
Breaking PBE	63
Slowing Down an Attack on a Password	64
Good Passwords	65
Password Generators	67
Hardware-Based Key Storage	69
Tokens	69
Crypto Accelerators	73
Hardware Devices and Random Numbers	75
Biometrics	75
Summary	76
Real-World Examples	76
Keon Desktop	77
Other Products	79
Chapter 4 The Key Distribution Problem and Public-Key Cryptography	81
Sharing Keys in Advance	83
Problems With This Scheme	84
Using a Trusted Third Party	85
Problems With This Scheme	86
Public-Key Cryptography and the Digital Envelope	88
Security Issues	91
Breaking a Public-Key Algorithm	92
Some History of Public-Key Cryptography	93
How Public-Key Cryptography Works	94
The RSA Algorithm	98
The DH Algorithm	105
The ECDH Algorithm	111
Comparing the Algorithms	117
Security	117
Key Sizes	119
Performance	120
Transmission Size	122
Interoperability	122

Protecting Private Keys	122
Using the Digital Envelope for Key Recovery	123
Key Recovery via a Trusted Third Party	124
Key Recovery via a Group of Trustees	126
Key Recovery via Threshold Schemes	127
How a Threshold Scheme Works	130
Summary	132
Real-World Example	133
Chapter 5 The Digital Signature	137
The Uniqueness of a Digital Signature	138
Message Digests	141
Collisions	145
The Three Important Digest Algorithms	148
A Representative of Larger Data	149
Data Integrity	153
Back to Digital Signatures	154
Trying to Cheat	156
Implementing Authentication, Data Integrity, and Nonrepudiation	159
Understanding the Algorithms	159
RSA	160
DSA	161
ECDSA	163
Comparing the Algorithms	163
Security	163
Performance	164
Transmission Size	165
Interoperability	165
Protecting Private Keys	166
Introduction to Certificates	166
Key Recovery	169
Summary	169
Real-World Example	170
Chapter 6 Public-Key Infrastructures and the X.509 Standard	171
Public-Key Certificates	172
Unique Identifiers	174
Standard Version 3 Certificate Extensions	175
Entity Names	177

ASN.1 Notation and Encoding	179
The Components of a PKI	179
Certification Authority	180
Registration Authority	180
Certificate Directory	181
Key Recovery Server	182
Management Protocols	182
Operational Protocols	184
Registering and Issuing Certificates	184
Revoking a Certificate	185
Certificate Revocation Lists	186
Suspending a Certificate	190
Authority Revocation Lists	190
Trust Models	191
Certificate Hierarchies	192
Cross-Certification	193
X.509 Certificate Chain	194
The Push Model Versus the Pull Model	195
Managing Key Pairs	196
Generating Key Pairs	197
Protecting Private Keys	197
Managing Multiple Key Pairs	198
Updating Key Pairs	199
Keeping a History of Key Pairs	200
Deploying a PKI	201
The Future of PKI	201
Roaming Certificates	201
Attribute Certificates	203
Certificate Policies and Certification Practice Statements	204
Summary	206
Real-World Examples	206
Keon Certificate Server	207
Keon Web PassPort	207
Chapter 7 Network and Transport Security Protocols	209
Internet Protocol Security	209
IP Security Architecture	210
IPSec Services	211
The Authentication Header Protocol	211
Integrity Check Value Calculation	212

Transport and Tunnel Modes	213
The Encapsulating Security Payload Protocol	215
Encryption Algorithms	216
ESP in Transport and Tunnel Modes	217
Security Associations	218
Combining Security Associations	219
Security Databases	220
Security Policy Database	222
Security Association Database	222
Key Management	223
Internet Key Exchange	224
Secure Sockets Layer	227
The History of SSL	227
Session and Connection States	228
The Record Layer Protocol	230
The Change Cipher Spec Protocol	231
The Alert Protocol	232
The Handshake Protocol	233
The Client Hello Message	234
The Server Hello Message	235
The Server Certificate Message	236
The Server Key Exchange Message	236
The Certificate Request Message	237
The Server Hello Done Message	237
The Client Certificate Message	237
The Client Key Exchange Message	238
The Certificate Verify Message	238
The Finished Message	239
Ending a Session and Connection	239
Resuming Sessions	240
Cryptographic Computations	240
Encryption and Authentication Algorithms	240
Summary	241
Real-World Examples	242
Chapter 8 Application-Layer Security Protocols	243
S/MIME	243
Overview	244
S/MIME Functionality	245
Cryptographic Algorithms	245

S/MIME Messages	247
Enhanced Security Services	252
Interoperability	253
Secure Electronic Transaction (SET)	253
Business Requirements	254
SET Features	255
SET Participants	256
Dual Signatures	257
SET Certificates	258
Payment Processing	260
Summary	264
Real-World Examples	265
Chapter 9 Hardware Solutions: Overcoming Software Limitations	267
Cryptographic Accelerators	267
Authentication Tokens	269
Token Form Factors	270
Noncontact Tokens	270
Contact Tokens	275
Smart Cards	275
Smart Card Standards	276
Types of Smart Cards	276
Readers and Terminals	278
JavaCards	279
History and Standards	279
JavaCard Operations	280
Other Java Tokens	281
Biometrics	282
Biometric Systems Overview	282
Recognition Methods	285
Biometric Accuracy	288
Combining Authentication Methods	289
Summary	291
Vendors	291
Chapter 10 Digital Signatures: Beyond Security	293
Legislative Approaches	295
Legal Guidelines from the American Bar Association	295
Legal Concepts Related to Digital Signatures	296

Nonrepudiation	296
Authentication	298
Written Versus Digital Signatures	299
Requirements for the Use of Digital Signatures	299
Public Key Infrastructures	300
Control of Key Revocation	300
Time-Stamping	300
Current and Pending Legislation	302
The E-SIGN Act	303
Dealing with Legal Uncertainties	306
Summary	307
Real-World Examples	307
Chapter 11 Doing It Wrong: The Break-Ins	309
Measuring Losses	309
Types of Security Threats	310
Unauthorized Disclosure of Data	311
Unauthorized Modification of Data	311
Unauthorized Access	312
Disclosure of Network Traffic	313
Spoofing of Network Traffic	314
Identifying Intruders	314
Insiders	315
Hackers	315
Terrorists	315
Foreign Intelligence Services	316
Hactivists	316
Intruder Knowledge	317
Case Studies	317
Data in Transit	317
Data at Rest	318
Authentication	319
Implementation	320
Information Security: Law Enforcement	321
Summary	322
Chapter 12 Doing It Right: Following Standards	323
Security Services and Mechanisms	324
Authentication	324

Confidentiality	326
Integrity	326
Nonrepudiation	327
Standards, Guidelines, and Regulations	327
The Internet Engineering Task Force	327
ANSI X9	328
National Institute of Standards and Technology	328
Common Criteria	330
The Health Insurance Portability Act	330
Developer Assistance	331
Insurance	332
Security Research	332
Case Studies	333
Implementation	333
Authentication	334
Data at Rest	335
Data in Transit	336
Summary	336
Appendix A Bits, Bytes, Hex, and ASCII	339
Appendix B A Layman's Guide to a Subset of ASN.1, BER, and DER	347
Appendix C Further Technical Details	387
Index	407



-ROM at Back Cover

The software and information on this CD-ROM (collectively referred to as the "Product") are the property of RSA Security Inc. ("RSA Security") and are protected by both United States copyright law and international copyright treaty provision. You must treat this Product just like a book, except that you may copy it into a computer to be used and you may make archival copies of the Products for the sole purpose of backing up our software and protecting your investment from loss.

By saying "just like a book," RSA Security means, for example, that the Product may be used by any number of people and may be freely moved from one computer location to another, so long as there is no possibility of the Product (or any part of the Product) being used at one location or on one computer while it is being used at another. Just as a book cannot be read by two different people in two different places at the same time, neither can the Product be used by two different people in two different places at the same time (unless, of course, RSA Security's rights are being violated).

RSA Security reserves the right to alter or modify the contents of the Product at any time.

This agreement is effective until terminated. The Agreement will terminate automatically without notice if you fail to comply with any provisions of this Agreement. In the event of termination by reason of your breach, you will destroy or erase all copies of the Product installed on any computer system or made for backup purposes and shall expunge the Product from your data storage facilities.

LIMITED WARRANTY

RSA Security warrants the CD-ROM(s) enclosed herein to be free of defects in materials and workmanship for a period of sixty days from the purchase date. If RSA Security receives written notification within the warranty period of defects in materials or workmanship, and such notification is determined by RSA Security to be correct, RSA Security will replace the defective diskette(s). Send request to:

RSA Press
 RSA Security Inc.
 2955 Campus Drive
 Suite 400
 San Mateo, CA 94403

The entire and exclusive liability and remedy for breach of this Limited Warranty shall be limited to replacement of defective CD-ROM(s) and shall not include or extend any claim for or right to cover any other damages, including but not limited to, loss of profit, data, or use of the software, or special, incidental, or consequential damages or other similar claims, even if RSA Security or The McGraw-Hill Companies, Inc. ("McGraw-Hill") has been specifically advised as to the possibility of such damages. In no event will RSA Security's or McGraw-Hill's liability for any damages to you or any other person ever exceed the lower of suggested list price or actual price paid for the license to use the Product, regardless of any form of the claim.

RSA SECURITY INC. AND THE MCGRAW-HILL COMPANIES, INC. SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Specifically, neither RSA Security nor McGraw-Hill makes any representation or warranty that the Product is fit for any particular purpose and any implied warranty of merchantability is limited to the sixty day duration of the Limited Warranty covering the physical CD-ROM(s) only (and not the software or information) and is otherwise expressly and specifically disclaimed.

This Limited Warranty gives you specific legal rights; you may have others which may vary from state to state. Some states do not allow the exclusion of incidental or consequential damages, or the limitation on how long an implied warranty lasts, so some of the above may not apply to you.

This Agreement constitutes the entire agreement between the parties relating to use of the Product. The terms of any purchase order shall have no effect on the terms of this Agreement. Failure of RSA Security to insist at any time on strict compliance with this Agreement shall not constitute a waiver of any rights under this Agreement. This Agreement shall be construed and governed in accordance with the laws of Massachusetts, irrespective of its choice of law principles. If any provision of this Agreement is held to be contrary to law, that provision will be enforced to the maximum extent permissible and the remaining provisions will remain in force and effect.



Learn how cryptography works— from the leading authority in e-security



Cryptography is one of the smartest ways to protect the information on your network and reduce the risk of security breaches and attacks from hackers. And because implementing cryptography is a complex process, you need the practical advice and proven techniques contained inside this official guide. Written by insiders at RSA Security, this expert resource explains the differences between symmetric-key and public-key cryptography, how PKI and X.509 affect security, how the RSA algorithm works within protocols, and much more. You'll also read actual case studies detailing different types of security vulnerabilities and what types of cryptography applications would prevent attacks.

This book will show you how to:

- Distinguish different types of symmetric-key encryption algorithms and know where each is best used
- Find out how password-based encryption works
- Communicate safely over unsecure channels using public-key technology
- Use public-key technology for authentication and non-repudiation
- Recognize how corporations use cryptography to improve security through real-world case studies
- Get details on current PKI standards and technology—including vendor information
- Understand X.509 certificates and directory structures
- Get an operational overview of widely-used protocols—including IPSec, SSL, and SET
- View cryptography from different perspectives—corporations, developers, and users
- Effectively use digital signatures and hardware solutions—smart cards, tokens, key storage devices, and more

Improve security and protect your company's information with the most authoritative guide to cryptography available.

ABOUT THE AUTHORS:

STEVE BURNETT has degrees in math from Grinnell College in Iowa and The Claremont Graduate School in California. He has spent most of his career converting math into computer programs at Intergraph Corporation and now with RSA Security. A frequent speaker at industry conferences and college campuses, Steve is the lead engineer for RSA's BSAFE Crypto-C and Crypto-J products, which are general purpose cryptography software development kits in C and Java.

STEPHEN PAINE has worked in the security field throughout most of his career—formerly for the United States Marine Corps and for SUN Microsystems. He is currently a systems engineer for RSA Security, where he explains security concepts to corporations and developers worldwide and provides training to customers and RSA employees.

ONLY AVAILABLE FROM RSA SECURITY

- RSA Laboratories' complete FAQ 4.1
- Public-Key Cryptography Standards
- Crypto Bytes Technical Newsletters

OSBORNE 

REQUIRED READING for the Information Age

A Division of The McGraw-Hill Companies 

\$59.99 USA

£43.99 UK

NETWORKING/SECURITY



7 83254 03608 6

www.osborne.com

Book P/N 0-07-213138-1 of

ISBN 0-07-213139-X

90000



9 780072 131390

APPENDIX D



Search WorldCat

Search

[Advanced Search](#) [Find a Library](#)

[<< Return to Search Results](#)

[Cite/Export](#)

[Print](#)

[E-mail](#)

[Share](#)

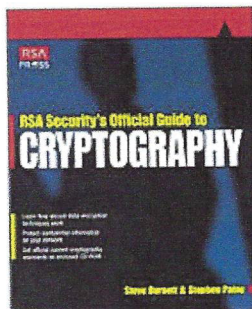
[Permalink](#)

[Add to list](#)

[Add tags](#)

[Write a review](#)

Rate this item: 1 2 3 4 5



RSA security's official guide to cryptography

Author: [Steve Burnett](#); [Stephen Paine](#)

Publisher: New York : Osborne/McGraw-Hill, cop. 2001.

Edition/Format: Print book : English [View all editions and formats](#)

Summary: Helps in implementing cryptography, the most secure form of data encryption. This work, with case studies, is written in conjunction with "RSA Security". It is a part of the "RSA Press Series".

Rating: (not yet rated) [0 with reviews - Be the first.](#)

Subjects: [Computer networks -- Security measures.](#)

[Data encryption \(Computer science\)](#)

[Cryptography.](#)

[View all subjects](#)

More like this

[Similar Items](#)

Get a Copy

[Find a copy in the library](#)

[AbeBooks](#) \$1.72

[Amazon](#) \$71.21

[Barnes & Noble](#) \$49.98

[Better World Books](#) \$4.98

[iTunes](#) \$39.99

Find a copy in the library

Finding libraries that hold this item...

Enter your location: [Find libraries](#)

Submit a complete postal address for best results.

Displaying libraries 1-6 out of 575 for all 19 editions (Washington, DC, USA)

Show libraries holding [just this edition](#)

[<< First](#) [< Prev](#) [1](#) [2](#) [3](#) [Next >](#) [Last >>](#)

Library	Held formats	Distance	
1. Library of Congress Washington, DC 20540 United States	Book	2 miles MAP IT	Library info Ask a librarian Add to favorites
2. Arlington Public Library Library Administration Arlington, VA 22201 United States	Book	4 miles MAP IT	Library info Ask a librarian Add to favorites
3. University of Maryland Libraries UMD Libraries College Park, MD 20742 United States	Book	7 miles MAP IT	Library info Search at this library. Ask a librarian Add to favorites
4. University of Maryland University College UMUC Library Adelphi, MD 20783 United States	Book	10 miles MAP IT	Library info Ask a librarian Add to favorites
5. George Mason University Fenwick Library Fairfax, VA 22030 United States	Book	16 miles MAP IT	Library info Add to favorites

6. [Bowie State University](#)
Thurgood Marshall Library
 Bowie, MD 20715 United States



17 miles
 MAP IT

[Library info](#)
[Add to favorites](#)

<< First < Prev 1 2 3 Next > Last >>

Details

Genre/Form: Handboeken (vorm)

Material Type: Internet resource

Document Type: Book, Internet Resource

All Authors / Contributors: [Steve Burnett](#); [Stephen Paine](#)

Find more information about:

ISBN: 007213139X 9780072131390 0072131381 9780072131383 0072131373 9780072131376

OCLC Number: 782997409

Notes: Includes index.

Description: xxi, 419 p. : ill. ; 24 cm + CD-ROM v.d.t.: RSA security's complete cryptography

Contents: Chapter 1: Why Cryptography? Chapter 2: Symmetric-Key Cryptography. Chapter 3: Symmetric-Key Management. Chapter 4: The Key Distribution Problem and Public-Key Cryptography. Chapter 5: The Digital Signature. Chapter 6: Public-Key Infrastructures and the X.509 Standard. Chapter 7: Network and Transport Security Protocols. Chapter 8: Application-Layer Security Protocols. Chapter 9: Hardware Solutions: Overcoming Software Limitations. Chapter 10: Digital Signatures: Beyond Security. Chapter 11: Doing It Wrong: The Break-Ins. Chapter 12: Doing It Right: Following Standards. Appendix A: Bits, Bytes, Hex, and ASCII. Appendix B: A Layman's Guide to a Subset of ASN.1, BER, and DER. Appendix C: Further Technical Details.

Other Titles: Cryptography
 RSA security's complete cryptography

Responsibility: Steve Burnett and Stephen Paine.

More information: catdir.loc.gov | catdir.loc.gov | catdir.loc.gov

Reviews

User-contributed reviews

[Add a review](#) and share your thoughts with other readers. Be the first.

Tags

[Add tags](#) for "RSA security's official guide to cryptography". Be the first.

Similar Items

[Computer networks -- Security measures.](#)

[Data encryption \(Computer science\)](#)

[Cryptography.](#)

[Cryptografie.](#)

[Computerbeveiliging.](#)

[TCP/IP.](#)

[+ Linked Data](#)