APPENDIX C

RSA PRESS

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

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

RSA Security's Official Guide to Cryptography

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

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

SOFTWARE LICENSE

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.


Security's Complete
CRYPTOGRAPHY
Reference
CD-ROM
RSA PRESS
...Because Knowledge is Security™
OSBORNE
WETATEC
UMMM TK 5105.59 .B871 2001 CD-ROM
V.3 no.1

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

RSA PRESS ...Because Knowledge is 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.

ONLY AVAILABLE FROM RSA SECURITY
- RSA Laboratories' complete FAQ 4.1
- Public-Key Cryptography Standards
- Crypto Bytes Technical Newsletters

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.

OSBORNE McGraw-Hill

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

WorldCat

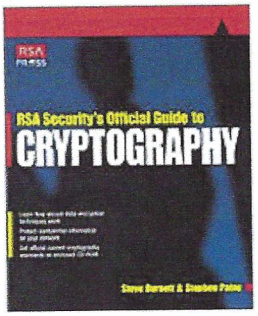
Search WorldCat

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: District of Columbia 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	Book	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: Steve Burnett ▼ Go
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

Related Subjects: (6)

Computer networks -- Security measures.

Data encryption (Computer science)

Cryptography.

Cryptografie.

Computerbeveiliging.

TCP/IP.

+ Linked Data