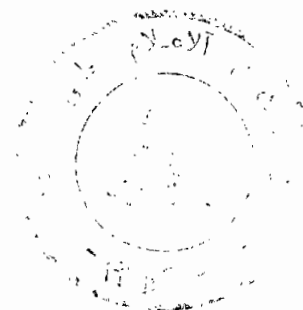


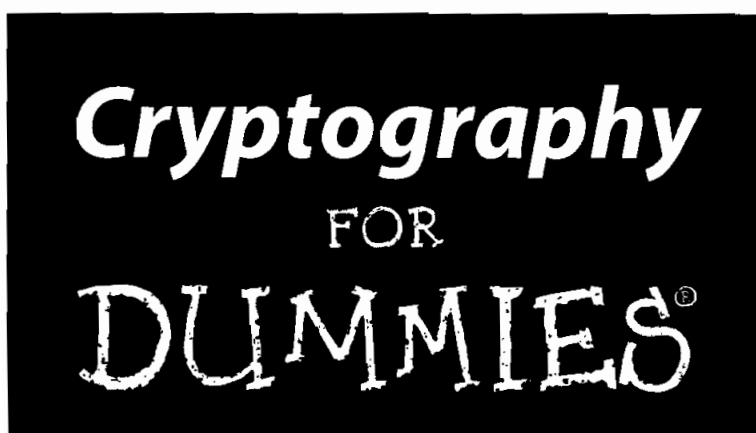
Cryptography FOR **DUMMIES®**

by Chey Cobb, CISSP



WILEY

Wiley Publishing, Inc.



BIBLIOTHEQUE DU CERIST



Cryptography For Dummies®

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

Copyright © 2004 by Wiley Publishing, Inc., Indianapolis, Indiana

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4447.
e-mail: permcoordinator@wiley.com.

Trademarks: Wiley, the Wiley Publishing logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHOR HAVE USED THEIR BEST EFFORTS IN PREPARING THIS BOOK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS BOOK AND SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A PROFESSIONAL WHERE APPROPRIATE. NEITHER THE PUBLISHER NOR AUTHOR SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at 800-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

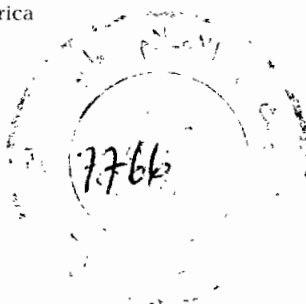
Library of Congress Control Number: 2003105686

ISBN: 0764541889

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

10/QY/QR/QU/IN



About the Author

Chey Ewertz Cobb, CISSP, began working in computer security in 1989. Since then she has managed her own computer security consulting company, Cobb Associates, working for such clients as Apple Computers and Sun Microsystems. She later worked for the government, creating a secure network at Cape Canaveral, assisting in the security at Patrick Air Force Base, and later as a technical security officer for the National Reconnaissance Office (NRO), which is more secretive than the NSA.

During her work in security, she had the opportunity to evaluate and manage cryptosystems for private industry and the U.S. Intelligence Agencies.

Chey now writes books on computer security (*Computer Security Handbook, 4th Edition* and *Network Security For Dummies*), writes articles for magazines, and speaks at computer security conferences.

BIBLIOTHEQUE DU CERIST

Dedication

To R. W. Ewertz, Jr. He was my role model and inspiration when things got tough.

BIBLIOTHEQUE DU CERIST

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

Acknowledgments

First of all, let me thank Andrea Boucher and Melody Layne who saw me through thick and thin and never lost faith in me (at least they never let on that they did!). I enjoy working with them both, and any writer who has the opportunity to work with them should count himself/herself lucky!

Secondly, I want to thank Dave Brussin, Ryan Upton, Josh Beneloh, Jon Callas, and Dave Del Torto for setting me on the correct path when my explanations strayed. Thanks so much for lending me your brainwork!

Last, but not least, Stephen. My love, my life, and my everything.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at www.dummies.com/register/.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Andrea C. Boucher

Acquisitions Editor: Melody Layne

Technical Editor: Tim Crothers

Editorial Manager: Carol Sheehan

Media Development Manager:
Laura VanWinkle

Media Development Supervisor:
Richard Graves

Editorial Assistant: Amanda Foxworth

Cartoons: Rich Tennant (www.the5thwave.com)

Production

Project Coordinator: Maridee Ennis

Layout and Graphics: Joyce Haughey,
Andrea Dahl, Stephanie D. Jumper,
Jacque Schneider, Melanee Wolven

Proofreaders: Andy Hollandbeck,
Carl William Pierce, TECHBOOKS
Production Services

Indexer: TECHBOOKS Production Services

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Joyce Pepple, Acquisitions Director

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Contents at a Glance

Introduction	1
<i>Part I: Crypto Basics & What You Really Need to Know</i>	7
Chapter 1: A Primer on Crypto Basics	9
Chapter 2: Major League Algorithms	33
Chapter 3: Deciding What You Really Need	53
Chapter 4: Locks and Keys	79
<i>Part II: Public Key Infrastructure</i>	93
Chapter 5: The PKI Primer	95
Chapter 6: PKI Bits and Pieces	107
Chapter 7: All Keyed Up!	119
<i>Part III: Putting Encryption Technologies to Work for You</i>	135
Chapter 8: Securing E-Mail from Prying Eyes	137
Chapter 9: File and Storage Strategies	167
Chapter 10: Authentication Systems	183
Chapter 11: Secure E-Commerce	197
Chapter 12: Virtual Private Network (VPN) Encryption	213
Chapter 13: Wireless Encryption Basics	223
<i>Part IV: The Part of Tens</i>	235
Chapter 14: The Ten Best Encryption Web Sites	237
Chapter 15: The Ten Most Commonly Misunderstood Encryption Terms	241
Chapter 16: Cryptography Do's and Don'ts	245
Chapter 17: Ten Principles of "Cryptiquette"	251
Chapter 18: Ten Very Useful Encryption Products	255
<i>Part V: Appendixes</i>	259
Appendix A: Cryptographic Attacks	261
Appendix B: Glossary	267
Appendix C: Encryption Export Controls	279
<i>Index</i>	283

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

[illegible]

It's Not about James Bond	9
Go with the rhythm	10
Rockin' the rhythm	11
Getting to Know the Basic Terms	12
What Makes a Cipher?	13
Concealment ciphers	13
Substitution ciphers	14
Transposition ciphers	15
Hash without the corned beef	16
XOR what?	17
Breaking Ciphers	20
Not-so-secret keys	20
Known plaintext	21
Pattern recognition	21
What a brute!	21
Cryptosystems	22
Everyday Uses of Encryption	23
Network logons and passwords	23
Secure Web transactions	25
ATMs	26
Music and DVDs	27
Communication devices	28

Why Encryption Isn't More Commonplace	28
Difficulty in understanding the technology	29
You can't do it alone	29
Sharing those ugly secrets	30
Cost may be a factor	30
Special administration requirements	31
Chapter 2: Major League Algorithms	33
Beware of "Snake Oil"	34
Symmetric Keys Are All the Same	37
The key table	37
Key generation and random numbers	38
Protecting the Key	39
Symmetric Algorithms Come in Different Flavors	40
Making a hash of it	40
Defining blocks and streams	42
Which is better: Block or stream?	44
Identifying Symmetric Algorithms	45
DES	45
Triple DES	45
IDEA	46
AES	46
Asymmetric Keys	47
RSA	48
Diffie-Hellman (& Merkle)	49
PGP	50
Elliptical Curve Cryptography	50
Working Together	52
Chapter 3: Deciding What You Really Need	53
Justifying the Costs to Management	53
Long-term versus short-term	54
Tangible versus intangible results	55
Positive ROI	55
Government due diligence	60
Insurers like it!	61
Presenting your case	61
Do You Need Secure Communications?	62
Secure e-mail	62
Instant Messaging (IM)	64
Secure e-commerce	64
Online banking	66
Virtual Private Networks (VPNs)	66
Wireless (In)security	68

Do You Need to Authenticate Users?	69
Who are your users?	70
Authentication tokens	71
Smart cards	72
Java tokens	73
Biometrics	74
Do You Need to Ensure Confidentiality and Integrity?	75
Protecting Personal Data	75
What's It Gonna Cost?	77
Chapter 4: Locks and Keys	79
The Magic Passphrase	80
The weakest link	81
Mental algorithms	82
Safety first!	84
Passphrase attacks	86
Don't forget to flush!	87
The Key Concept	88
Key generation	89
Protecting your keys	90
What to do with your old keys	91
Some cryptiquette	91
Part 11: Public Key Infrastructure	93
Chapter 5: The PKI Primer	95
What Is PKI?	96
Certificate Authorities (CAs)	97
Digital Certificates	98
Desktops, laptops, and servers	100
Key servers	102
Registration Authorities (RAs)	103
Uses for PKI Systems	103
Common PKI Problems	105
Chapter 6: PKI Bits and Pieces	107
Certificate Authorities	108
Pretenders to the throne	110
Registration Authorities	110
Certificate Policies (CPs)	111
Digital Certificates and Keys	112
D'basing Your Certificates	113
Certificate Revocation	114

Picking the PKCS	115
PKCS #1: RSA Encryption Standard	115
PKCS #3: Diffie-Hellman Key Agreement Standard	115
PKCS #5: Password-Based Cryptography Standard	115
PKCS #6: Extended-Certificate Syntax Standard	116
PKCS #7: Cryptographic Message Syntax Standard	116
PKCS #8: Private-Key Information Syntax Standard	116
PKCS #9: Selected Attribute Types	117
PKCS #10: Certification Request Syntax Standard	117
PKCS #11: Cryptographic Token Interface Standard	117
PKCS #12: Personal Information Exchange Syntax Standard	118
PKCS #13: Elliptic Curve Cryptography Standard	118
PKCS #14: Pseudo-Random Number Generation Standard	118
PKCS #15: Cryptographic Token Information Format Standard	118
Chapter 7: All Keyed Up!	119
So, What Exactly IS a Key?	120
Making a Key	120
The Long and Short of It	121
Randomness in Keys Is Good	122
Storing Your Keys Safely	123
Keys for Different Purposes	124
Keys and Algorithms	124
One Key; Two Keys	125
Public/private keys	126
The magic encryption machine	127
The magic decryption machine	128
Symmetric keys (again)	129
Trusting Those Keys	129
Key Servers	130
Keeping keys up to date	131
Policies for keys	132
Key escrow and key recovery	132
Part III: Putting Encryption Technologies to Work for You	135
Chapter 8: Securing E-Mail from Prying Eyes	137
E-Mail Encryption Basics	138
S/MIME	138
PGP	139
Digital Certificates or PGP Public/Private Key Pairs?	140
What's the diff?	140
When should you use which?	141
Sign or encrypt or both?	141
Remember that passphrase!	142

Using S/MIME	142
Setting up S/MIME in Outlook Express	143
Backing up your Digital Certificates	151
Fun and Games with PGP	153
Setting up PGP	154
Deciding on the options	156
Playing with your keyring	160
Sending and receiving PGP messages	162
PGP in the enterprise	164
Other Encryption Stuff to Try	164
Chapter 9: File and Storage Strategies	167
Why Encrypt Your Data?	168
Encrypted Storage Roulette	170
Symmetric versus asymmetric?	171
Encrypting in the air or on the ground?	173
Dealing with Integrity Issues	174
Message digest/hash	174
MACs	175
HMACs	175
Tripwire	176
Policies and Procedures	177
Examples of Encryption Storage	178
Media encryption	179
Encrypting File System	180
Secure e-mail	181
Program-specific encryption	181
Encrypted backup	181
Chapter 10: Authentication Systems	183
Common Authentication Systems	185
Kerberos	185
SSH	186
RADIUS	187
TACACS+	188
Authentication Protocols	188
How Authentication Systems Use Digital Certificates	190
Tokens, Smart Cards, and Biometrics	191
Digital Certificates on a PC	191
Time-based tokens	192
Smartcard and USB Smartkeys	193
Biometrics	194
Chapter 11: Secure E-Commerce	197
SSL Is the Standard	198
A typical SSL connection	199
Rooting around your certificates	201

Time for TLS	203
Setting Up an SSL Solution	204
What equipment do I need?	205
The e-commerce manager's checklist	206
XML Is the New Kid on the Block	209
Going for Outsourced E-Commerce	210

Chapter 12: Virtual Private Network (VPN) Encryption 213

How Do VPNs Work Their Magic?	214
Setting Up a VPN	214
What devices do I need?	215
What else should I consider?	216
Do VPNs affect performance?	216
Don't forget wireless!	217
Various VPN Encryption Schemes	217
PPP and PPTP	217
L2TP	218
IPsec	218
Which Is Best?	220
Testing, Testing, Testing	221

Chapter 13: Wireless Encryption Basics 223

Why WEP Makes Us Weep	224
No key management	225
Poor RC4 implementation	225
Authentication problems	226
Not everything is encrypted	226
WEP Attack Methods	227
Finding wireless networks	228
War chalking	228
Wireless Protection Measures	230
Look for rogue access points	230
Change the default SSIDs	230
Turn on WEP	231
Position your access points well	232
Buy special antennas	232
Use a stronger encryption scheme	232
Use a VPN for wireless networks	232
Employ an authentication system	233

Part IV: The Part of Tens 235

Chapter 14: The Ten Best Encryption Web Sites 237

Mat Blaze's Cryptography Resource on the Web	237
The Center for Democracy and Technology	237
SSL Review	238
How IPsec Works	238

Code and Cipher	238
CERIAS — Center for Education and Research in Information Assurance and Security	238
The Invisible Cryptologists — African Americans, WWII to 1956	239
Bruce Schneier	239
North American Cryptography Archives	239
RSA's Crypto FAQ	239
Chapter 15: The Ten Most Commonly Misunderstood Encryption Terms	241
Military-Grade Encryption	241
Trusted Third Party	241
X.509 Certificates	242
Rubber Hose Attack	242
Shared Secret	242
Key Escrow	242
Initialization Vector	243
Alice, Bob, Carol, and Dave	243
Secret Algorithm	243
Steganography	244
Chapter 16: Cryptography Do's and Don'ts	245
Do Be Sure the Plaintext Is Destroyed after a Document Is Encrypted	245
Do Protect Your Key Recovery Database and Other Key Servers to the Greatest Extent Possible	246
Don't Store Your Private Keys on the Hard Drive of Your Laptop or Other Personal Computing Device	246
Do Make Sure Your Servers' Operating Systems Are "Hardened" before You Install Cryptological Systems on Them	246
Do Train Your Users against Social Engineering	247
Do Create the Largest Key Size Possible	247
Do Test Your Cryptosystem after You Have It Up and Running	248
Do Check the CERT Advisories and Vendor Advisories about Flaws and Weaknesses in Cryptosystems	248
Don't Install a Cryptosystem Yourself If You're Not Sure What You Are Doing	248
Don't Use Unknown, Untested Algorithms	249
Chapter 17: Ten Principles of "Cryptiquette"	251
If Someone Sends You an Encrypted Message, Reply in Kind	251
Don't Create Too Many Keys	251
Don't Immediately Trust Someone Just Because He/She Has a Public Key.....	252
Always Back Up Your Keys and Passphrases	252

Be Wary of What You Put in the Subject Line of Encrypted Messages	252
If You Lose Your Key or Passphrase, Revoke Your Keys as Soon as Possible	253
Don't Publish Someone's Public Key to a Public Key Server without His/Her Permission	253
Don't Sign Someone's Public Key Unless You Have Reason To	253
If You Are Corresponding with Someone for the First Time, Send an Introductory Note Along with Your Public Key	254
Be Circumspect in What You Encrypt	254
Chapter 18: Ten Very Useful Encryption Products	255
PGP: Pretty Good Privacy	255
GAIM	255
madeSafe Vault	256
Password Safe	256
Kerberos	256
OpenSSL and Apache SSL	256
SafeHouse	257
WebCrypt	257
Privacy Master	257
Advanced Encryption Package	257
Part V: Appendixes	259
Appendix A: Cryptographic Attacks	261
Known Plaintext Attack	262
Chosen Ciphertext Attacks	262
Chosen Plaintext Attacks	263
The Birthday Attack	263
Man-in-the-Middle Attack	263
Timing Attacks	264
Rubber Hose Attack	264
Electrical Fluctuation Attacks	265
Major Boo-Boos	265
Appendix B: Glossary	267
Appendix C: Encryption Export Controls	279
Index	283