

# Contents

*Foreword by Whitfield Diffie* xv

*Preface* xix

HOW TO READ THIS BOOK xx

ACKNOWLEDGMENTS xxii

*About the Author* xxiii

## 1 FOUNDATIONS 1

- 1.1 TERMINOLOGY 1
- 1.2 STEGANOGRAPHY 9
- 1.3 SUBSTITUTION CIPHERS AND TRANSPOSITION CIPHERS 10
- 1.4 SIMPLE XOR 13
- 1.5 ONE-TIME PADS 15
- 1.6 COMPUTER ALGORITHMS 17
- 1.7 LARGE NUMBERS 17

## PART I CRYPTOGRAPHIC PROTOCOLS

### 2 PROTOCOL BUILDING BLOCKS 21

- 2.1 INTRODUCTION TO PROTOCOLS 21
- 2.2 COMMUNICATIONS USING SYMMETRIC CRYPTOGRAPHY 28
- 2.3 ONE-WAY FUNCTIONS 29
- 2.4 ONE-WAY HASH FUNCTIONS 30
- 2.5 COMMUNICATIONS USING PUBLIC-KEY CRYPTOGRAPHY 31
- 2.6 DIGITAL SIGNATURES 34
- 2.7 DIGITAL SIGNATURES WITH ENCRYPTION 41
- 2.8 RANDOM AND PSEUDO-RANDOM-SEQUENCE GENERATION 44



**3 BASIC PROTOCOLS 47**

- 3.1 KEY EXCHANGE 47
- 3.2 AUTHENTICATION 52
- 3.3 AUTHENTICATION AND KEY EXCHANGE 56
- 3.4 FORMAL ANALYSIS OF AUTHENTICATION AND KEY-EXCHANGE PROTOCOLS 65
- 3.5 MULTIPLE-KEY PUBLIC-KEY CRYPTOGRAPHY 68
- 3.6 SECRET SPLITTING 70
- 3.7 SECRET SHARING 71
- 3.8 CRYPTOGRAPHIC PROTECTION OF DATABASES 73

**4 INTERMEDIATE PROTOCOLS 75**

- 4.1 TIMESTAMPING SERVICES 75
- 4.2 SUBLIMINAL CHANNEL 79
- 4.3 UNDENIABLE DIGITAL SIGNATURES 81
- 4.4 DESIGNATED CONFIRMER SIGNATURES 82
- 4.5 PROXY SIGNATURES 83
- 4.6 GROUP SIGNATURES 84
- 4.7 FAIL-STOP DIGITAL SIGNATURES 85
- 4.8 COMPUTING WITH ENCRYPTED DATA 85
- 4.9 BIT COMMITMENT 86
- 4.10 FAIR COIN FLIPS 89
- 4.11 MENTAL POKER 92
- 4.12 ONE-WAY ACCUMULATORS 95
- 4.13 ALL-OR-NOTHING DISCLOSURE OF SECRETS 96
- 4.14 KEY ESCROW 97

**5 ADVANCED PROTOCOLS 101**

- 5.1 ZERO-KNOWLEDGE PROOFS 101
- 5.2 ZERO-KNOWLEDGE PROOFS OF IDENTITY 109
- 5.3 BLIND SIGNATURES 112
- 5.4 IDENTITY-BASED PUBLIC-KEY CRYPTOGRAPHY 115
- 5.5 OBLIVIOUS TRANSFER 116
- 5.6 OBLIVIOUS SIGNATURES 117
- 5.7 SIMULTANEOUS CONTRACT SIGNING 118
- 5.8 DIGITAL CERTIFIED MAIL 122
- 5.9 SIMULTANEOUS EXCHANGE OF SECRETS 123

**6 ESOTERIC PROTOCOLS 125**

- 6.1 SECURE ELECTIONS 125
- 6.2 SECURE MULTIPARTY COMPUTATION 134
- 6.3 ANONYMOUS MESSAGE BROADCAST 137
- 6.4 DIGITAL CASH 139



**PART II CRYPTOGRAPHIC TECHNIQUES****7 KEY LENGTH 151**

- 7.1 SYMMETRIC KEY LENGTH 151
- 7.2 PUBLIC-KEY KEY LENGTH 158
- 7.3 COMPARING SYMMETRIC AND PUBLIC-KEY KEY LENGTH 165
- 7.4 BIRTHDAY ATTACKS AGAINST ONE-WAY HASH FUNCTIONS 165
- 7.5 HOW LONG SHOULD A KEY BE? 166
- 7.6 CAVEAT EMPTOR 168

**8 KEY MANAGEMENT 169**

- 8.1 GENERATING KEYS 170
- 8.2 NONLINEAR KEYSACES 175
- 8.3 TRANSFERRING KEYS 176
- 8.4 VERIFYING KEYS 178
- 8.5 USING KEYS 179
- 8.6 UPDATING KEYS 180
- 8.7 STORING KEYS 180
- 8.8 BACKUP KEYS 181
- 8.9 COMPROMISED KEYS 182
- 8.10 LIFETIME OF KEYS 183
- 8.11 DESTROYING KEYS 184
- 8.12 PUBLIC-KEY KEY MANAGEMENT 185

**9 ALGORITHM TYPES AND MODES 189**

- 9.1 ELECTRONIC CODEBOOK MODE 189
- 9.2 BLOCK REPLAY 191
- 9.3 CIPHER BLOCK CHAINING MODE 193
- 9.4 STREAM CIPHERS 197
- 9.5 SELF-SYNCHRONIZING STREAM CIPHERS 198
- 9.6 CIPHER-FEEDBACK MODE 200
- 9.7 SYNCHRONOUS STREAM CIPHERS 202
- 9.8 OUTPUT-FEEDBACK MODE 203
- 9.9 COUNTER MODE 205
- 9.10 OTHER BLOCK-CIPHER MODES 206
- 9.11 CHOOSING A CIPHER MODE 208
- 9.12 INTERLEAVING 210
- 9.13 BLOCK CIPHERS VERSUS STREAM CIPHERS 210

**10 USING ALGORITHMS 213**

- 10.1 CHOOSING AN ALGORITHM 214
- 10.2 PUBLIC-KEY CRYPTOGRAPHY VERSUS SYMMETRIC CRYPTOGRAPHY 216
- 10.3 ENCRYPTING COMMUNICATIONS CHANNELS 216
- 10.4 ENCRYPTING DATA FOR STORAGE 220
- 10.5 HARDWARE ENCRYPTION VERSUS SOFTWARE ENCRYPTION 223



- 10.6 COMPRESSION, ENCODING, AND ENCRYPTION 226
- 10.7 DETECTING ENCRYPTION 226
- 10.8 HIDING CIPHERTEXT IN CIPHERTEXT 227
- 10.9 DESTROYING INFORMATION 228

### **PART III CRYPTOGRAPHIC ALGORITHMS**

#### **11 MATHEMATICAL BACKGROUND 233**

- 11.1 INFORMATION THEORY 233
- 11.2 COMPLEXITY THEORY 237
- 11.3 NUMBER THEORY 242
- 11.4 FACTORING 255
- 11.5 PRIME NUMBER GENERATION 258
- 11.6 DISCRETE LOGARITHMS IN A FINITE FIELD 261

#### **12 DATA ENCRYPTION STANDARD (DES) 265**

- 12.1 BACKGROUND 265
- 12.2 DESCRIPTION OF DES 270
- 12.3 SECURITY OF DES 278
- 12.4 DIFFERENTIAL AND LINEAR CRYPTANALYSIS 285
- 12.5 THE REAL DESIGN CRITERIA 293
- 12.6 DES VARIANTS 294
- 12.7 HOW SECURE IS DES TODAY? 300

#### **13 OTHER BLOCK CIPHERS 303**

- 13.1 LUCIFER 303
- 13.2 MADRYGA 304
- 13.3 NEWDES 306
- 13.4 FEAL 308
- 13.5 REDOC 311
- 13.6 LOKI 314
- 13.7 KHUFU AND KHAFRE 316
- 13.8 RC2 318
- 13.9 IDEA 319
- 13.10 MMB 325
- 13.11 CA-1.1 327
- 13.12 SKIPJACK 328

#### **14 STILL OTHER BLOCK CIPHERS 331**

- 14.1 GOST 331
- 14.2 CAST 334
- 14.3 BLOWFISH 336
- 14.4 SAFER 339
- 14.5 3-WAY 341



- 14.6 CRAB 342
- 14.7 SXAL8/MBAL 344
- 14.8 RC5 344
- 14.9 OTHER BLOCK ALGORITHMS 346
- 14.10 THEORY OF BLOCK CIPHER DESIGN 346
- 14.11 USING ONE-WAY HASH FUNCTIONS 351
- 14.12 CHOOSING A BLOCK ALGORITHM 354
  
- 15 COMBINING BLOCK CIPHERS 357**
  - 15.1 DOUBLE ENCRYPTION 357
  - 15.2 TRIPLE ENCRYPTION 358
  - 15.3 DOUBLING THE BLOCK LENGTH 363
  - 15.4 OTHER MULTIPLE ENCRYPTION SCHEMES 363
  - 15.5 CDMF KEY SHORTENING 366
  - 15.6 WHITENING 366
  - 15.7 CASCADING MULTIPLE BLOCK ALGORITHMS 367
  - 15.8 COMBINING MULTIPLE BLOCK ALGORITHMS 368
  
- 16 PSEUDO-RANDOM-SEQUENCE GENERATORS AND STREAM CIPHERS 369**
  - 16.1 LINEAR CONGRUENTIAL GENERATORS 369
  - 16.2 LINEAR FEEDBACK SHIFT REGISTERS 372
  - 16.3 DESIGN AND ANALYSIS OF STREAM CIPHERS 379
  - 16.4 STREAM CIPHERS USING LFSRs 381
  - 16.5 A5 389
  - 16.6 HUGHES XPD/KPD 389
  - 16.7 NANOTEQ 390
  - 16.8 RAMBUTAN 390
  - 16.9 ADDITIVE GENERATORS 390
  - 16.10 GIFFORD 392
  - 16.11 ALGORITHM M 393
  - 16.12 PKZIP 394
  
- 17 OTHER STREAM CIPHERS AND REAL RANDOM-SEQUENCE GENERATORS 397**
  - 17.1 RC4 397
  - 17.2 SEAL 398
  - 17.3 WAKE 400
  - 17.4 FEEDBACK WITH CARRY SHIFT REGISTERS 402
  - 17.5 STREAM CIPHERS USING FCSRs 405
  - 17.6 NONLINEAR-FEEDBACK SHIFT REGISTERS 412
  - 17.7 OTHER STREAM CIPHERS 413
  - 17.8 SYSTEM-THEORETIC APPROACH TO STREAM-CIPHER DESIGN 415
  - 17.9 COMPLEXITY-THEMATIC APPROACH TO STREAM-CIPHER DESIGN 416
  - 17.10 OTHER APPROACHES TO STREAM-CIPHER DESIGN 418



- 17.11 CASCADING MULTIPLE STREAM CIPHERS 419
- 17.12 CHOOSING A STREAM CIPHER 420
- 17.13 GENERATING MULTIPLE STREAMS FROM A SINGLE PSEUDO-RANDOM-SEQUENCE GENERATOR 420
- 17.14 REAL RANDOM-SEQUENCE GENERATORS 421
- 18 ONE-WAY HASH FUNCTIONS 429**
  - 18.1 BACKGROUND 429
  - 18.2 SNEFRU 431
  - 18.3 N-HASH 432
  - 18.4 MD4 435
  - 18.5 MD5 436
  - 18.6 MD2 441
  - 18.7 SECURE HASH ALGORITHM (SHA) 441
  - 18.8 RIPE-MD 445
  - 18.9 HAVAL 445
  - 18.10 OTHER ONE-WAY HASH FUNCTIONS 446
  - 18.11 ONE-WAY HASH FUNCTIONS USING SYMMETRIC BLOCK ALGORITHMS 446
  - 18.12 USING PUBLIC-KEY ALGORITHMS 455
  - 18.13 CHOOSING A ONE-WAY HASH FUNCTION 455
  - 18.14 MESSAGE AUTHENTICATION CODES 455
- 19 PUBLIC-KEY ALGORITHMS 461**
  - 19.1 BACKGROUND 461
  - 19.2 KNAPSACK ALGORITHMS 462
  - 19.3 RSA 466
  - 19.4 POHLIG-HELLMAN 474
  - 19.5 RABIN 475
  - 19.6 ELGAMAL 476
  - 19.7 McELIECE 479
  - 19.8 ELLIPTIC CURVE CRYPTOSYSTEMS 480
  - 19.9 LUC 481
  - 19.10 FINITE AUTOMATON PUBLIC-KEY CRYPTOSYSTEMS 482
- 20 PUBLIC-KEY DIGITAL SIGNATURE ALGORITHMS 483**
  - 20.1 DIGITAL SIGNATURE ALGORITHM (DSA) 483
  - 20.2 DSA VARIANTS 494
  - 20.3 GOST DIGITAL SIGNATURE ALGORITHM 495
  - 20.4 DISCRETE LOGARITHM SIGNATURE SCHEMES 496
  - 20.5 ONG-SCHNORR-SHAMIR 498
  - 20.6 ESIGN 499
  - 20.7 CELLULAR AUTOMATA 500
  - 20.8 OTHER PUBLIC-KEY ALGORITHMS 500
- 21 IDENTIFICATION SCHEMES 503**
  - 21.1 FEIGE-FIAT-SHAMIR 503



- 21.2 GUILLOU-QUISQUATER 508
- 21.3 SCHNORR 510
- 21.4 CONVERTING IDENTIFICATION SCHEMES TO SIGNATURE SCHEMES 512

## **22 KEY-EXCHANGE ALGORITHMS 513**

- 22.1 DIFFIE-HELLMAN 513
- 22.2 STATION-TO-STATION PROTOCOL 516
- 22.3 SHAMIR'S THREE-PASS PROTOCOL 516
- 22.4 COMSET 517
- 22.5 ENCRYPTED KEY EXCHANGE 518
- 22.6 FORTIFIED KEY NEGOTIATION 522
- 22.7 CONFERENCE KEY DISTRIBUTION AND SECRET BROADCASTING 523

## **23 SPECIAL ALGORITHMS FOR PROTOCOLS 527**

- 23.1 MULTIPLE-KEY PUBLIC-KEY CRYPTOGRAPHY 527
- 23.2 SECRET-SHARING ALGORITHMS 528
- 23.3 SUBLIMINAL CHANNEL 531
- 23.4 UNDENIABLE DIGITAL SIGNATURES 536
- 23.5 DESIGNATED CONFIRMER SIGNATURES 539
- 23.6 COMPUTING WITH ENCRYPTED DATA 540
- 23.7 FAIR COIN FLIPS 541
- 23.8 ONE-WAY ACCUMULATORS 543
- 23.9 ALL-OR-NOTHING DISCLOSURE OF SECRETS 543
- 23.10 FAIR AND FAILSAFE CRYPTOSYSTEMS 546
- 23.11 ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE 548
- 23.12 BLIND SIGNATURES 549
- 23.13 OBLIVIOUS TRANSFER 550
- 23.14 SECURE MULTIPARTY COMPUTATION 551
- 23.15 PROBABILISTIC ENCRYPTION 552
- 23.16 QUANTUM CRYPTOGRAPHY 554

## **PART IV THE REAL WORLD**

### **24 EXAMPLE IMPLEMENTATIONS 561**

- 24.1 IBM SECRET-KEY MANAGEMENT PROTOCOL 561
- 24.2 MITRENET 562
- 24.3 ISDN 563
- 24.4 STU-III 565
- 24.5 KERBEROS 566
- 24.6 KRYPTOKNIGHT 571
- 24.7 SESAME 572
- 24.8 IBM COMMON CRYPTOGRAPHIC ARCHITECTURE 573
- 24.9 ISO AUTHENTICATION FRAMEWORK 574
- 24.10 PRIVACY-ENHANCED MAIL (PEM) 577
- 24.11 MESSAGE SECURITY PROTOCOL (MSP) 584



- 24.12 PRETTY GOOD PRIVACY (PGP) 584
- 24.13 SMART CARDS 587
- 24.14 PUBLIC-KEY CRYPTOGRAPHY STANDARDS (PKCS) 588
- 24.15 UNIVERSAL ELECTRONIC PAYMENT SYSTEM (UEPS) 589
- 24.16 CLIPPER 591
- 24.17 CAPSTONE 593
- 24.18 AT&T MODEL 3600 TELEPHONE SECURITY DEVICE (TSD) 594
  
- 25 POLITICS 597**
- 25.1 NATIONAL SECURITY AGENCY (NSA) 597
- 25.2 NATIONAL COMPUTER SECURITY CENTER (NCSC) 599
- 25.3 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) 600
- 25.4 RSA DATA SECURITY, INC. 603
- 25.5 PUBLIC KEY PARTNERS 604
- 25.6 INTERNATIONAL ASSOCIATION FOR CRYPTOGRAPHIC RESEARCH (IACR) 605
- 25.7 RACE INTEGRITY PRIMITIVES EVALUATION (RIPE) 605
- 25.8 CONDITIONAL ACCESS FOR EUROPE (CAFE) 606
- 25.9 ISO/IEC 9979 607
- 25.10 PROFESSIONAL, CIVIL LIBERTIES, AND INDUSTRY GROUPS 608
- 25.11 SCI.CRYPT 608
- 25.12 CYPHERPUNKS 609
- 25.13 PATENTS 609
- 25.14 U.S. EXPORT RULES 610
- 25.15 FOREIGN IMPORT AND EXPORT OF CRYPTOGRAPHY 617
- 25.16 LEGAL ISSUES 618
  
- Afterword by Matt Blaze 619*

## **PART V SOURCE CODE**

*Source Code 623*

*References 675*