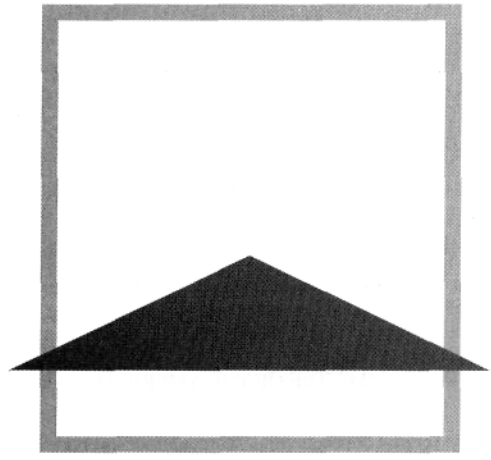
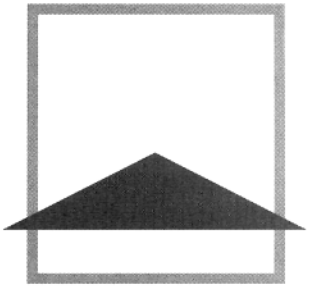


Applied Cryptography

Protocols, Algorithms, and Source Code in C

Bruce Schneier

John Wiley & Sons, Inc.
NEW YORK • CHICHESTER • BRISBANE • TORONTO • SINGAPORE



Contents

FOREWORD by Whitfield Diffie xi

PREFACE xv
How to Read This Book xvi
Acknowledgments xviii

CHAPTER 1
Foundations 1
1.1 Terminology 1
1.2 Classical Cryptography 8
1.3 Large Numbers 15

PART **ONE**
CRYPTOGRAPHIC PROTOCOLS 17

CHAPTER 2
Protocol Building Blocks 19
2.1 Introduction to Protocols 19
2.2 Communications Using Symmetric Cryptography 26
2.3 One-Way Functions 27
2.4 One-Way Hash Functions 28
2.5 Communications Using Public-Key Cryptography 29
2.6 Digital Signatures 31
2.7 Digital Signatures with Encryption 37
2.8 Random and Pseudo-Random Sequence Generation 39

CHAPTER 3
Basic Protocols **42**
3.1 Key Exchange 42
3.2 Authentication 47
3.3 Authentication and Key Exchange 51
3.4 Multiple-Key Public-Key Cryptography 56
3.5 Secret Splitting 58
3.6 Secret Sharing 59
3.7 Cryptographic Protection of Databases 61
3.8 Timestamping Services 61

CHAPTER 4
Intermediate Protocols **66**
4.1 Subliminal Channel 66
4.2 Undeniable Digital Signatures 68
4.3 Fail-Stop Digital Signatures 69
4.4 Group Signatures 70
4.5 Computing with Encrypted Data 71
4.6 Bit Commitment 71
4.7 Fair Coin Flips 74
4.8 Mental Poker 78

CHAPTER 5
Advanced Protocols **82**
5.1 Fair Cryptosystems 82
5.2 All-or-Nothing Disclosure of Secrets 83
5.3 Zero-Knowledge Proofs of Knowledge 84
5.4 Zero-Knowledge Proofs of Identity 91
5.5 Blind Signatures 93

CHAPTER 6
Esoteric Protocols **97**
6.1 Oblivious Transfer 97
6.2 Simultaneous Contract Signing 99
6.3 Digital Certified Mail 103
6.4 Simultaneous Exchange of Secrets 104
6.5 Secure Elections 105
6.6 Secure Multiparty Computation 114
6.7 Digital Cash 117
6.8 Anonymous Message Broadcast 124

PART **TWO**
CRYPTOGRAPHIC TECHNIQUES **127**

CHAPTER 7
Keys **129**
7.1 Key Length 129
7.2 Key Management 139
7.3 Public-Key Key Management 152

CHAPTER 8
Using Algorithms 154
8.1 Block Cipher Modes 154
8.2 Multiple Encryption 165
8.3 Stream Ciphers 168
8.4 Stream Ciphers vs. Block Ciphers 176
8.5 Public-Key Cryptography vs. Symmetric Cryptography 177
8.6 Encrypting Communications Networks 178
8.7 Encrypting Data for Storage 180
8.8 Hardware Encryption vs. Software Encryption 181
8.9 File Erasure 183
8.10 Choosing an Algorithm 183

PART THREE
CRYPTOGRAPHIC ALGORITHMS 187

CHAPTER 9
Mathematical Background 189
9.1 Information Theory 189
9.2 Complexity Theory 193
9.3 Number Theory 198
9.4 Factoring 211
9.5 Prime Number Generation 213
9.6 Discrete Logarithms in a Finite Field 216

CHAPTER 10
Data Encryption Standard (DES) 219
10.1 Data Encryption Standard (DES) 219
10.2 DES Variants 241

CHAPTER 11
Other Block Algorithms 244
11.1 Lucifer 244
11.2 Madryga 245
11.3 NewDES 247
11.4 FEAL-N 249
11.5 REDOC 252
11.6 LOKI 255
11.7 Khufu and Khafre 257
11.8 RC2 and RC4 259
11.9 IDEA 260
11.10 MMB 266
11.11 CA-1.1 268
11.12 Skipjack 269
11.13 Using One-Way Hash Functions 270
11.14 Other Block Algorithms 272
11.15 Which Block Algorithm Is Best? 272

CHAPTER 12
Public-Key Algorithms **273**
12.1 Background 273
12.2 Diffie-Hellman 275
12.3 Knapsack Algorithms 277
12.4 RSA 281
12.5 Pohlig-Hellman 288
12.6 Rabin 289
12.7 Feige-Fiat-Shamir 291

CHAPTER 13
More Public-Key Algorithms **297**
13.1 Guillou-Quisquater 297
13.2 Ong-Schnorr-Shamir 299
13.3 ElGamal 300
13.4 Schnorr 302
13.5 Digital Signature Algorithm (DSA) 304
13.6 ESIGN 314
13.7 McEliece 316
13.8 Okamoto 92 317
13.9 Cellular Automata 317
13.10 Elliptic Curve Cryptosystems 317
13.11 Other Public-Key Algorithms 318
13.12 Which Public-Key Algorithm Is Best? 320

CHAPTER 14
One-Way Hash Functions **321**
14.1 Background 321
14.2 Snefru 324
14.3 N-Hash 326
14.4 MD4 329
14.5 MD5 329
14.6 MD2 333
14.7 Secure Hash Algorithm (SHA) 333
14.8 RIPE-MD 336
14.9 HAVAL 336
14.10 Other One-Way Hash Functions 337
14.11 Using Symmetric Block Algorithms 338
14.12 Using Public-Key Algorithms 344
14.13 Which One-Way Hash Function Is Best? 345
14.14 Key-Dependent One-Way Hash Functions 345

CHAPTER 15
Random Sequence Generators and Stream Ciphers **347**
15.1 Pseudo-Random Sequence Generators 347
15.2 Stream Ciphers 356

15.3 Real Random Sequence Generators 368
15.4 Generating Numbers and Nonuniform Distributions 372
15.5 Generating Random Permutations 374

CHAPTER 16
Special Algorithms for Protocols **376**
16.1 Key Exchange 376
16.2 Encrypted Key Exchange 378
16.3 Multiple-Key Public-Key Cryptography 381
16.4 Secret Broadcasting 382
16.5 Secret Sharing Algorithms 383
16.6 Subliminal Channel 387
16.7 Undeniable Digital Signatures 392
16.8 Computing with Encrypted Data 395
16.9 Fair Coin Flips 395
16.10 Fair Cryptosystems 398
16.11 All-or-Nothing Disclosure of Secrets 399
16.12 Zero-Knowledge Proofs of Knowledge 401
16.13 Blind Signatures 403
16.14 Oblivious Transfer 404
16.15 Secure Multiparty Computation 404
16.16 Probabilistic Encryption 406
16.17 Quantum Cryptography 408

PART **FOUR**
THE REAL WORLD **411**

CHAPTER 17
Example Implementations **413**
17.1 IBM Secret-Key Management Protocol 413
17.2 Mitrenet 414
17.3 ISDN 415
17.4 Kerberos 417
17.5 Kryptoknight 425
17.6 ISO Authentication Framework 425
17.7 Privacy-Enhanced Mail (PEM) 428
17.8 Message Security Protocol (MSP) 436
17.9 Pretty Good Privacy (PGP) 436
17.10 Clipper 437
17.11 CAPSTONE 438

CHAPTER 18
Politics **439**
18.1 National Security Agency (NSA) 439
18.2 National Computer Security Center (NCSC) 440
18.3 National Institute of Standards and Technology (NIST) 441
18.4 RSA Data Security, Inc. 444

18.5 International Association of Cryptographic Research (IACR) 445
18.6 Sci.crypt 445
18.7 Cypherpunks 445
18.8 Research and Development in Advanced Communication Technologies in Europe (RACE) 446
18.9 Electronic Frontier Foundation (EFF) 446
18.10 Computer Professionals for Social Responsibility (CPSR) 446
18.11 Patents 447
18.12 Export Rules 448
18.13 Legal Issues 454

PART **FIVE**
SOURCE CODE

SOURCE CODE 457
VIGENERE, BEAUFORD, VARIANT BEAUFORD 457
ENIGMA 460
DES 467
LUCIFER 485
NEWDES 491
FEAL-8 495
FEAL-NX 502
REDOC III 507
LOKI 91 511
IDEA 519
N-HASH 532
MD5 542
SECURE HASH ALGORITHM 549
SECRET SHARING 557

REFERENCES 571

INDEX 605