CONTENTS

Acknowledgments xix

CHAPTER 1 **Introduction** 1

1.1 Roadmap to the Book 2
1.2 What Type of Book Is This? 3
1.3 Terminology 4
1.4 Notation 5
1.5 Primer on Networking 6
1.5.1 OSI Reference Model 6
1.5.2 Directory Service 8
1.5.3 Replicated Services 9
1.5.4 Packet Switching 9
1.5.5 Network Components 10
1.5.6 Destinations: Ultimate and Intermediate 11
1.5.7 Address Structure 12
1.6 Tempest 13
1.7 Firewalls/Security Gateways 13
1.7.1 Packet Filters 14
1.7.2 Application Level Gateway 14
1.7.3 Encrypted Tunnels 15
1.8 Key Escrow for Law Enforcement 16
1.9 Key Escrow for Careless Users 18
1.10 Viruses, Worms, Trojan Horses 18
1.10.1 Where Do They Come From? 19
1.10.2 Spreading Pests from Machine to Machine 22
1.10.3 Virus Checkers 23
1.10.4 What Can We Do Today? 23
1.10.5 Wish List for the Future 24
1.11 The Military Model of Security 26
1.11.1 Mandatory (Nondiscretionary) Access Controls 26
1.11.2 Levels of Security 27
1.11.3 Mandatory Access Control Rules 28
1.11.4 Covert Channels 29
1.11.5 The Orange Book 30
1.12 Legal Issues 33

1.12.1 Patents ... 33
1.12.2 Export Controls ... 35

CRYPTOGRAPHY

CHAPTER 2 **Introduction to Cryptography** **39**

2.1 What Is Cryptography? ... 39
2.1.1 Computational Difficulty ... 40
2.1.2 To Publish or Not to Publish ... 41
2.1.3 Secret Codes ... 42
2.2 Breaking an Encryption Scheme ... 43
2.2.1 Ciphertext Only ... 43
2.2.2 Known Plaintext ... 44
2.2.3 Chosen Plaintext ... 44
2.3 Types of Cryptographic Functions ... 45
2.4 Secret Key Cryptography ... 45
2.4.1 Security Uses of Secret Key Cryptography ... 46
2.4.2 Transmitting Over an Insecure Channel ... 46
2.4.3 Secure Storage on Insecure Media ... 46
2.4.4 Authentication ... 46
2.4.5 Integrity Check ... 47
2.5 Public Key Cryptography ... 48
2.5.1 Security Uses of Public Key Cryptography ... 50
2.5.2 Transmitting Over an Insecure Channel ... 50
2.5.3 Secure Storage on Insecure Media ... 51
2.5.4 Authentication ... 51
2.5.5 Digital Signatures ... 52
2.6 Hash Algorithms ... 53
2.6.1 Password Hashing ... 53
2.6.2 Message Integrity ... 54
2.6.3 Message Fingerprint ... 54
2.6.4 Downline Load Security ... 55
2.6.5 Digital Signature Efficiency ... 55
2.7 Homework ... 55

CHAPTER 3 **Secret Key Cryptography** **57**

3.1 Introduction ... 57
3.2 Generic Block Encryption ... 57
3.3 Data Encryption Standard (DES) ... 60
3.3.1 DES Overview ... 63
3.3.2 The Permutations of the Data ... 64
3.3.3 Generating the Per-Round Keys ... 65
3.3.4 A DES Round ... 68

3.3.5 The Mangler Function 69
3.3.6 Weak and Semi-Weak Keys 72
3.3.7 What's So Special About DES? 73
3.4 International Data Encryption Algorithm (IDEA) 74
3.4.1 Primitive Operations 75
3.4.2 Key Expansion 75
3.4.3 One Round 76
3.4.3.1 Odd Round 77
3.4.3.2 Even Round 77
3.4.4 Inverse Keys For Decryption 79
3.4.5 Does IDEA Work? 79
3.5 Using Secret Key Cryptography in Protocols 80
3.6 Encrypting a Large Message 80
3.6.1 Electronic Code Book (ECB) 80
3.6.2 Cipher Block Chaining (CBC) 82
3.6.2.1 CBC Threat 1—Modifying Ciphertext Blocks 84
3.6.2.2 CBC Threat 2—Rearranging Ciphertext Blocks 85
3.6.3 Output Feedback Mode (OFB) 86
3.6.4 Cipher Feedback Mode (CFB) 87
3.7 Generating MICs 89
3.7.1 Ensuring Privacy and Integrity Together 89
3.7.2 CBC with a Weak Cryptographic Checksum 91
3.7.3 CBC with a Cryptographic Hash 91
3.7.4 CBC Encryption and CBC Residue with Related Keys 92
3.8 Multiple Encryption DES 92
3.8.1 How Many Encryptions? 94
3.8.1.1 Encrypting Twice with the Same Key 94
3.8.1.2 Encrypting Twice with Two Keys 95
3.8.1.3 Triple Encryption 96
3.8.2 CBC Outside vs Inside 97
3.9 Homework 97
CHAPTER 4 **Hashes and Message Digests** **101**
4.1 Introduction 101
4.2 Nifty Things to Do with a Hash 105
4.2.1 Authentication 107
4.2.2 Computing a MIC with a Hash 107
4.2.3 Encryption with a Message Digest 109
4.2.3.1 Generating a One-Time Pad 109
4.2.3.2 Mixing In the Plaintext 109
4.2.4 Using Secret Key for a Hash 110
4.2.4.1 UNIX Password Hash 110

4.2.4.2 Hashing Large Messages 111

4.3 MD2 112

4.3.1 MD2 Padding 112

4.3.2 MD2 Checksum Computation 113

4.3.3 MD2 Final Pass 115

4.4 MD4 116

4.4.1 MD4 Message Padding 116

4.4.2 Overview of MD4 Message Digest Computation 117

4.4.3 MD4 Message Digest Pass 1 118

4.4.4 MD4 Message Digest Pass 2 119

4.4.5 MD4 Message Digest Pass 3 119

4.5 MD5 120

4.5.1 MD5 Message Padding 120

4.5.2 Overview of MD5 Message Digest Computation 121

4.5.3 MD5 Message Digest Pass 1 121

4.5.4 MD5 Message Digest Pass 2 121

4.5.5 MD5 Message Digest Pass 3 122

4.5.6 MD5 Message Digest Pass 4 122

4.6 SHS 123

4.6.1 SHS Message Padding 123

4.6.2 Overview of SHS Message Digest Computation 123

4.6.3 SHS Operation on a 512-bit Block 124

4.7 Homework 125

CHAPTER 5 Public Key Algorithms 129

5.1 Introduction 129

5.2 Modular Arithmetic 130

5.2.1 Modular Addition 130

5.2.2 Modular Multiplication 131

5.2.3 Modular Exponentiation 133

5.3 RSA 134

5.3.1 RSA Algorithm 134

5.3.2 Why Does RSA Work? 135

5.3.3 Why Is RSA Secure? 135

5.3.4 How Efficient Are the RSA Operations? 136

5.3.4.1 Exponentiating With Big Numbers 136

5.3.4.2 Generating RSA Keys 138

Finding Big Primes p and q 138

Finding d and e 140

5.3.4.3 Having a Small Constant e 140

5.3.4.4 Optimizing RSA Private Key Operations 142

5.3.5 Arcane RSA Threats 143

5.3.5.1 Smooth Numbers 143
5.3.5.2 The Cube Root Problem 144
5.3.6 Public-Key Cryptography Standard (PKCS) 145
5.3.6.1 Encryption 145
5.3.6.2 Signing 146
5.4 Diffie-Hellman 147
5.4.1 The Bucket Brigade Attack 149
5.4.2 Diffie-Hellman with Published Public Numbers 150
5.4.3 Encryption with Diffie-Hellman 150
5.4.4 El Gamal Signatures 151
5.4.5 Diffie-Hellman Details—Strong Primes 152
5.5 Digital Signature Standard (DSS) 152
5.5.1 The DSS Algorithm 153
5.5.2 Why Does the Verification Procedure Work? 155
5.5.3 Why Is This Secure? 155
5.5.4 The DSS Controversy 155
5.5.5 Per-Message Secret Number 157
5.6 Zero Knowledge Proof Systems 158
5.6.1 Zero Knowledge Signatures 160
5.7 Homework Problems 161

CHAPTER 6 **Number Theory** **163**

6.1 Introduction 163
6.2 Modular Arithmetic 163
6.3 Primes 164
6.4 Euclid's Algorithm 165
6.4.1 Finding Multiplicative Inverses in Modular Arithmetic 167
6.5 Chinese Remainder Theorem 168
6.6 Z_n* 170
6.7 Euler's Totient Function 171
6.8 Euler's Theorem 172
6.8.1 A Generalization of Euler's Theorem 172
6.9 Homework Problems 173

AUTHENTICATION

CHAPTER 7 **Authentication Systems** **177**

7.1 Password-Based Authentication 177
7.1.1 Off- vs On-Line Password Guessing 179
7.1.2 Storing User Passwords 179
7.2 Address-Based Authentication 181
7.2.1 Network Address Impersonation 183
7.3 Cryptographic Authentication Protocols 184

7.4 Who Is Being Authenticated? 185
7.5 Passwords as Cryptographic Keys 185
7.6 Eavesdropping and Server Database Reading 186
7.7 Trusted Intermediaries 188
7.7.1 KDCs 189
7.7.2 Certification Authorities (CAs) 190
7.7.3 Certificate Revocation 191
7.7.4 Multiple Trusted Intermediaries 193
7.7.4.1 Multiple KDC Domains 193
7.7.4.2 Multiple CA Domains 196
7.8 Session Key Establishment 196
7.9 Authorization 198
7.9.1 Groups 198
7.9.2 Hierarchical Groups 200
7.10 Delegation 201
7.11 Homework 202

CHAPTER 8 **Authentication of People** **205**

8.1 Passwords 206
8.2 On-Line Password Guessing 206
8.3 Off-Line Password Guessing 209
8.4 How Big Should a Secret Be? 211
8.5 Eavesdropping 212
8.6 Passwords and Careless Users 213
8.6.1 Using a Password in Multiple Places 213
8.6.2 Requiring Frequent Password Changes 214
8.6.3 A Login Trojan Horse to Capture Passwords 215
8.6.4 Non-Login Use of Passwords 216
8.7 Initial Password Distribution 216
8.8 Authentication Tokens 218
8.9 Physical Access 220
8.10 Biometrics 221
8.11 Homework 222

CHAPTER 9 **Security Handshake Pitfalls** **223**

9.1 Login Only 224
9.1.1 Shared Secret 224
9.1.2 One-Way Public Key 228
9.1.3 Lamport's Hash 230
9.2 Mutual Authentication 233
9.2.1 Reflection Attack 233
9.2.2 Password Guessing 235

9.2.3 Public Keys....236
9.2.4 Timestamps....237
9.3 Integrity/Encryption for Data....237
9.3.1 Shared Secret....238
9.3.2 Two-Way Public Key Based Authentication....239
9.3.3 One-Way Public Key Based Authentication....240
9.3.4 Lamport Hash....241
9.3.5 Privacy and Integrity....242
9.4 Mediated Authentication (with KDC)....243
9.4.1 Needham-Schroeder....244
9.4.2 Expanded Needham-Schroeder....246
9.4.3 Otway-Rees....247
9.5 Bellovin-Merritt....249
9.6 Network Login and Password Guessing....253
9.7 Nonce Types....254
9.8 Picking Random Numbers....256
9.9 X.509 Problem....258
9.10 Performance Considerations....258
9.11 Authentication Protocol Checklist....260
9.12 Homework....262

CHAPTER 10 Kerberos V4 265

10.1 Introduction....265
10.2 Tickets and Ticket-Granting Tickets....266
10.3 Configuration....267
10.4 Logging Into the Network....268
10.4.1 Obtaining a Session Key and TGT....268
10.4.2 Alice Asks to Talk to a Remote Node....269
10.5 Replicated KDCs....272
10.6 Realms....273
10.7 Interrealm Authentication....274
10.8 Key Version Numbers....275
10.9 Encryption for Privacy and Integrity....276
10.10 Encryption for Integrity Only....278
10.11 Network Layer Addresses in Tickets....279
10.12 Message Formats....280
10.12.1 Tickets....282
10.12.2 Authenticators....283
10.12.3 Credentials....284
10.12.4 AS_REQ....286
10.12.5 TGS_REQ....286
10.12.6 AS_REP and TGS_REP....287

10.12.7 Error Reply from KDC 289
10.12.8 AP_REQ 289
10.12.9 AP_REP 290
10.12.10 Encrypted Data (KRB_PRV) 291
10.12.11 Integrity-Checked Data (SAFE) 291
10.12.12 AP_ERR 293
10.13 Homework 294

CHAPTER 11 Kerberos V5 **295**

11.1 ASN.1 295
11.2 Names 297
11.3 Delegation of Rights 297
11.4 Ticket Lifetimes 300
11.4.1 Renewable Tickets 300
11.4.2 Postdated Tickets 301
11.5 Key Versions 302
11.6 Making Master Keys in Different Realms Different 302
11.7 Optimizations 303
11.8 Cryptographic Algorithms 303
11.8.1 Integrity-Only Algorithms 304
11.8.1.1 rsa-md5-des 304
11.8.1.2 des-mac 305
11.8.1.3 des-mac-k 306
11.8.1.4 rsa-md4-des 306
11.8.1.5 rsa-md4-des-k 306
11.8.2 Encryption for Privacy and Integrity 307
11.9 Hierarchy of Realms 307
11.10 Evading Password-Guessing Attacks 310
11.11 Key Inside Authenticator 311
11.12 Double TGT Authentication 311
11.13 KDC Database 312
11.14 Kerberos V5 Messages 313
11.14.1 Authenticator 313
11.14.2 Ticket 314
11.14.3 AS_REQ 314
11.14.4 TGS_REQ 316
11.14.5 AS_REP 318
11.14.6 TGS_REP 319
11.14.7 AP_REQ 319
11.14.8 AP_REP 320
11.14.9 KRB_SAFE 320
11.14.10 KRB_PRIV 321

11.14.11 KRB_CRED ... 321
11.14.12 KRB_ERROR ... 322
11.15 Homework ... 325

ELECTRONIC MAIL

CHAPTER 12 **Electronic Mail Security** 329
12.1 Distribution Lists ... 329
12.2 Store and Forward ... 331
12.3 Security Services for Electronic Mail ... 333
12.4 Establishing Keys ... 334
12.4.1 Establishing Public Keys ... 335
12.4.2 Establishing Secret Keys ... 336
12.5 Privacy ... 336
12.5.1 End-to-End Privacy ... 337
12.5.2 Privacy with Distribution List Exploders ... 338
12.6 Authentication of the Source ... 338
12.6.1 Source Authentication Based on Public Key Technology ... 339
12.6.2 Source Authentication Based on Secret Keys ... 340
12.6.3 Source Authentication with Distribution Lists ... 340
12.7 Message Integrity ... 341
12.7.1 Message Integrity Without Source Authentication ... 341
12.8 Non-Repudiation ... 342
12.8.1 Non-repudiation Based on Public Key Technology ... 342
12.8.2 Plausible Deniability Based on Public Key Technology ... 343
12.8.3 Non-Repudiation with Secret Keys ... 343
12.9 Proof of Submission ... 344
12.10 Proof of Delivery ... 345
12.11 Message Flow Confidentiality ... 345
12.12 Anonymity ... 346
12.13 Containment ... 347
12.14 Annoying Text Format Issues ... 348
12.14.1 Disguising Data as Text ... 349
12.15 Names and Addresses ... 351
12.16 Old Messages ... 352
12.16.1 Case 1: The Dishonest Buyer ... 352
12.16.2 Case 2: The Solution Looking for a Problem ... 353
12.17 Homework ... 353
CHAPTER 13 **Privacy Enhanced Mail (PEM)** 357
13.1 Introduction ... 357
13.1.1 Structure of a PEM Message ... 357
13.2 Establishing Keys ... 360

13.3 Some PEM History 362
13.4 Certificate Hierarchy 364
13.5 Certificate Revocation Lists (CRLs) 366
13.6 X.509 Certificates and CRLs 367
13.7 Reformatting Data to Get Through Mailers 368
13.8 General Structure of a PEM Message 369
13.9 Encryption 371
13.10 Source Authentication and Integrity Protection 372
13.11 Multiple Recipients 373
13.12 Bracketing PEM Messages 374
13.13 Remote Distribution List Exploders 377
13.13.1 Remote Exploding Using Public Keys 377
13.13.2 Remote Exploding Using Secret Keys 378
13.13.3 Mixing Key Types 380
13.14 Forwarding and Enclosures 380
13.14.1 Forwarding a Message 380
13.15 Canonicalization 382
13.16 Unprotected Information 382
13.17 Message Formats 384
13.17.1 ENCRYPTED, Public Key Variant 385
13.17.2 ENCRYPTED, Secret Key Variant 388
13.17.3 MIC-ONLY or MIC-CLEAR, Public Key Variant 390
13.17.4 MIC-ONLY and MIC-CLEAR, Secret Key Variant 391
13.17.5 CRL-RETRIEVAL-REQUEST 392
13.17.6 CRL 392
13.18 DES-CBC as MIC Doesn't Work 392
13.19 Homework 395

CHAPTER 14 **PGP (Pretty Good Privacy)** **399**

14.1 Introduction 399
14.2 Overview 400
14.3 Key Distribution 400
14.4 Efficient Encoding 401
14.5 Certificate and Key Revocation 403
14.6 Signature Types 404
14.7 Your Private Key 404
14.8 Key Rings 404
14.9 Anomalies 405
14.9.1 File Name 405
14.9.2 People Names 406
14.10 Object Formats 406
14.10.1 Message Formats 406

14.10.2 Primitive Object Formats 408

CHAPTER 15 **X.400** **413**

15.1 Overview of X.400 415
15.2 Security Functions Possible with X.400 416
15.3 Structure of an X.400 Message 417
15.3.1 Per-Message Security Fields 420
15.3.2 Per-Recipient Security Fields 421
15.3.2.1 Security Fields in the Token 422
15.3.2.2 Unencrypted Part of the Token 422
15.3.2.3 Encrypted Part of the Token 423
15.3.3 Fields for Probe Messages 423
15.3.4 Fields for Proof of Delivery 423
15.3.5 Fields for Proof of Submission 423
15.3.6 Security Fields for X.420 424

CHAPTER 16 **A Comparison of PEM, PGP, and X.400** **425**

16.1 Introduction 425
16.2 Certification Hierarchy 425
16.3 Certificate Distribution 426
16.4 Encryption 426
16.5 Encoding of Transmitted Messages 427
16.6 Cryptographic Algorithms Supported 427
16.7 Recipients with Multiple Keys 428
16.8 Mail-Intermediary-Provided Functions 428

LEFTOVERS

CHAPTER 17 **More Security Systems** **431**

17.1 NetWare V3 431
17.2 NetWare V4 433
17.2.1 NetWare's Gillou-Quisquater Authentication Scheme 436
17.3 KryptoKnight 438
17.3.1 KryptoKnight Tickets 439
17.3.2 Authenticators 440
17.3.3 Nonces vs. Timestamps 440
17.3.4 Data Encryption 441
17.4 SNMP 441
17.5 DASS/SPX 443
17.5.1 DASS Certification Hierarchy 443
17.5.2 Obtaining the User's Private Key 443
17.5.3 Login Key 444
17.5.4 DASS Authentication Handshake 444

17.5.5 DASS Authenticators 446
17.5.6 DASS Delegation 446
17.5.7 Saving Bits 447
17.6 Lotus Notes Security 448
17.6.1 ID Files 448
17.6.2 Coping with Export Controls 449
17.6.3 Certificates for Flat Names 450
17.6.4 Certificates for Hierarchical Names 451
17.6.5 Lotus Notes Authentication 452
17.6.6 Authentication Long-Term Secret 453
17.6.7 Mail 454
17.6.8 Certification Revocation 454
17.7 DCE Security 455
17.8 Microsoft Security 459
17.9 Network Denial of Service 462
17.9.1 Robust Broadcast 463
17.9.2 Robust Packet Delivery 464
17.10 Clipper 465
17.10.1 Key Escrow 469
17.11 Homework 469

Bibliography 471

Glossary 481

Index 497