## Contents

**Preface** xvi
  How to Read this Book ........................................ vii

1 **Our Design Philosophy** 1
  1.1 The Evils of Performance ........................................ 2
  1.2 The Evils of Features ........................................ 5

2 **The Context of Cryptography** 7
  2.1 The Role of Cryptography ........................................ 8
  2.2 The Weakest Link Property..................................... 9
  2.3 The Adversarial Setting ........................................ 11
  2.4 Practical Paranoia ........................................ 12
    2.4.1 Attack .................................................. 13
  2.5 Threat Model .................................................. 15
  2.6 Cryptography Is Not the Solution/ ................................ 17
  2.7 Cryptography Is Very Difficult S. ............................. 18
  2.8 Cryptography Is the Easy Part ................................ 19
  2.9 Background Reading ........................................ 20

3 **Introduction to Cryptography** 21
  3.1 Encryption/ ........................................ 21
    3.1.1 Kerckhoffs' Principle .................................... 23
  3.2 Authentication ........................................ 23
  3.3 Public-Key Encryption ........................................ 26
  3.4 Digital Signatures ........................................ 28
  3.5 PKI .................................................. 29
  3.6 Attacks ........................................ 30
8 The Secure Channel

8.1 Problem Statement

8.1.1 Roles

8.1.2 Key

8.1.3 Messages or Stream

8.1.4 Security Properties

8.2 Order of Authentication and Encryption

8.3 Outline

8.3.1 Message Numbers

8.3.2 Authentication

8.3.3 Encryption

8.3.4 Frame Format

8.4 Details

8.4.1 Initialization

8.4.2 Sending a Message

8.4.3 Receiving a Message

8.4.4 Message Order

8.5 Alternatives

8.6 Conclusion

9 Implementation Issues (I)

9.1 Creating Correct Programs

9.1.1 Specifications

9.1.2 Test and Fix

9.1.3 Lax^1 Attitude

9.1.4 So How Do We Proceed?

9.2 Creating Secure Software

9.3 Keeping Secrets

9.3.1 Wiping State

9.3.2 Swap File

9.3.3 Caches

9.3.4 Data Retention by Memory
II Key Negotiation

10 Generating Randomness

10.1 Real Random

10.1.1 Problems With Using Real Random Data

10.1.2 Pseudorandom Data

10.1.3 Real Random Data and PRNGs

10.2 Attack Models for a PRNG

10.3 Fortuna

10.4 The Generator

10.4.1 Initialization

10.4.2 Reseed

10.4.3 Generate Blocks

10.4.4 Generate Random Data

10.4.5 Generator Speed

10.5 Accumulator

10.5.1 Entropy Sources

10.5.2 Pools

10.5.3 Implementation Considerations

10.5.4 Initialization

10.5.5 Getting Random Data

10.5.6 Add an Event

10.6 Seed File Management

10.6.1 Write Seed File
10.6.2 Update Seed File ........................................... 178
10.6.3 When to Read and Write the Seed File .............. 179
10.6.4 Backups ......................................................... 179
10.6.5 Atomicity of File System Updates ..................... 180
10.6.6 First Boot ..................................................... 181
10.7 So What Should I Do? ....................................... 182
10.8 Choosing Random Elements ............................. 182

11 Primes .............................................................. 185
  11.1 Divisibility and Primes .................................... 186
  11.2 Generating Small Primes .................................. 188
  11.3 Computations Modulo a Prime ........................... 190
    11.3.1 Addition and Subtraction ............................ 191
    11.3.2 Multiplication ......................................... 192
    11.3.3 Groups and Finite Fields ............................. 192
    11.3.4 The GCD Algorithm ................................... 194
    11.3.5 The Extended Euclidean Algorithm ................ 195
    11.3.6 Working Modulo 2 ................................... 197
  11.4 Large Primes ................................................ 197
    11.4.1 Primality Testing .................................... 200
    11.4.2 Evaluating Powers ................................. 204

12 Diffie-Hellman ..................................................... 207
  12.1 Groups ....................................................... 208
  12.2 Basic DH .................................................... 210
  12.3 Man in the Middle ....................................... 211
  12.4 Pitfalls ....................................................... 212
  " 12.5 Safe Primes .............................................. 214
  12.6 Using a Smaller Subgroup ............................... 215
  12.7 The Size of $p$ ........................................... 216
  12.8 Practical Rules ......................................... 218
  12.9 What Could Go Wrong .................................... 220

13 RSA ................................................................. 223
  13.1 Introduction ............................................... 223
  13.2 The Chinese Remainder Theorem ....................... 224
    13.2.1 Garner's Formula ................................... 225
Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.2.2</td>
<td>Generalizations</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>13.2.3</td>
<td>Uses</td>
<td>227</td>
<td></td>
</tr>
<tr>
<td>13.2.4</td>
<td>Conclusion</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>13.3</td>
<td>Multiplication Modulo $n$</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>13.4</td>
<td>RSA Defined</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>13.4.1</td>
<td>Digital Signatures with RSA</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>13.4.2</td>
<td>Public Exponents</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>13.4.3</td>
<td>The Private Key</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>13.4.4</td>
<td>The Size of $n$</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>13.4.5</td>
<td>Generating RSA Keys</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>13.5</td>
<td>Pitfalls Using RSA</td>
<td>236</td>
<td></td>
</tr>
<tr>
<td>13.6</td>
<td>Encryption</td>
<td>237</td>
<td></td>
</tr>
<tr>
<td>13.7</td>
<td>Signatures</td>
<td>240</td>
<td></td>
</tr>
</tbody>
</table>

14 Introduction to Cryptographic Protocols | 245 |
| 14.1 | Roles | 245 |
| 14.2 | Trust | 246 |
| 14.2.1 | Risk | 248 |
| 14.3 | Incentive | 248 |
| 14.4 | Trust in Cryptographic Protocols | 251 |
| 14.5 | Messages and Steps | 251 |
| 14.5.1 | The Transport Layer | 252 |
| 14.5.2 | Protocol and Message Identity | 253 |
| 14.5.3 | Message Encoding and Parsing | 254 |
| 14.5.4 | Protocol Execution States | 255 |
| 14.5.5 | Errors | 255 |
| 14.5.6 | Replay and Retries | 257 |

15 Key Negotiation Protocol | 261 |
| 15.1 | The Setting | 261 |
| 15.2 | A First Try | 262 |
| 15.3 | Protocols' Live Forever | 264 |
| 15.4 | An Authentication Convention | 265 |
| 15.5 | A Second Attempt | 265 |
| 15.6 | A Third Attempt | 267 |
| 15.7 | Our Final Protocol | 268 |
| 15.8 | Different Views of the Protocol | 271 |
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.8.1 Alice's View</td>
<td>271</td>
</tr>
<tr>
<td>15.8.2 Bob's View</td>
<td>272</td>
</tr>
<tr>
<td>15.8.3 Attacker's View</td>
<td>272</td>
</tr>
<tr>
<td>15.8.4 Key Compromise</td>
<td>273</td>
</tr>
<tr>
<td>v. 15.9 Computational Complexity of the Protocol</td>
<td>274</td>
</tr>
<tr>
<td>/ 15.9.1 Optimization Tricks</td>
<td>275</td>
</tr>
<tr>
<td>15.10 Protocol Complexity</td>
<td>276</td>
</tr>
<tr>
<td>15.11 A Gentle Warning</td>
<td>277</td>
</tr>
<tr>
<td>15.12 Key Negotiation from a Password</td>
<td>277</td>
</tr>
<tr>
<td>16 Implementation Issues (II)</td>
<td>279</td>
</tr>
<tr>
<td>16.1 Large Integer Arithmetic</td>
<td>279</td>
</tr>
<tr>
<td>16.1.1 Woping</td>
<td>281</td>
</tr>
<tr>
<td>16.1.2 Checking DH Computations</td>
<td>284</td>
</tr>
<tr>
<td>16.1.3 Checking RSA Encryption</td>
<td>285</td>
</tr>
<tr>
<td>16.1.4 Checking RSA Signatures</td>
<td>286</td>
</tr>
<tr>
<td>16.1.5 Conclusion</td>
<td>286</td>
</tr>
<tr>
<td>16.2 Faster Multiplication</td>
<td>286</td>
</tr>
<tr>
<td>16.3 Side-Channel Attacks</td>
<td>288</td>
</tr>
<tr>
<td>16.3.1 Countermeasures</td>
<td>289</td>
</tr>
<tr>
<td>16.4 Protocols</td>
<td>290</td>
</tr>
<tr>
<td>16.4.1 Protocols Over a Secure Channel</td>
<td>291</td>
</tr>
<tr>
<td>16.4.2 Receiving a Message</td>
<td>291</td>
</tr>
<tr>
<td>16.4.3 Timeouts</td>
<td>293</td>
</tr>
<tr>
<td>17 Key Management</td>
<td>295</td>
</tr>
<tr>
<td>17 The Clock</td>
<td>297</td>
</tr>
<tr>
<td>17.1 Uses for a Clock</td>
<td>297</td>
</tr>
<tr>
<td>17.1.1 Expiration</td>
<td>297</td>
</tr>
<tr>
<td>17.1.2 Unique Value</td>
<td>298</td>
</tr>
<tr>
<td>17.1.3 Monotonicity</td>
<td>298</td>
</tr>
<tr>
<td>17.1.4 Real-Time Transactions</td>
<td>299</td>
</tr>
<tr>
<td>17.2 Using the Real-Time Clock Chip</td>
<td>299</td>
</tr>
<tr>
<td>17.3 Security Dangers</td>
<td>300</td>
</tr>
<tr>
<td>17.3.1 Setting the Clock Back</td>
<td>300</td>
</tr>
</tbody>
</table>

y
20.6 Credential Systems ........................................... 330
20.7 The Modified Dream ........................................ 332
20.8 Revocation ...................................................... 333
  20.8.1 Revocation List ......................................... 333
  20.8.2 Fast Expiration ......................................... 335
20.9 So What Is a PKI Good For? ............................. 336
20.10 What to Choose ............................................. 337

21 PKI Practicalities .............................................. 339
  21.1 Certificate Format ....................................... 339
    21.1.1 Permission Language ................................ 340
    21.1.2 The Root Key ........................................ 340
  21.2 The Life of a Key ......................................... 341
  21.3 Why Keys Wear Out ..................................... 343
  21.4 So What Should You Do? ............................... 345

22 Storing Secrets ................................................ 347
  22.1 Disk ........................................................ 347
  22.2 Human Memory .......................................... 348
    22.2.1 Salting and Stretching ............................ 350
  22.3 Portable Storage ........................................ 353
  22.4 Secure Token ............................................ 353
  22.5 Secure UI ................................................ 355
  22.6 Biometrics ............................................... 356
  22.7 Single Sign-On .......................................... 357
  22.8 Risk of Loss ............................................ 358
  22.9 Secret Sharing .......................................... 358
  22.10 Wiping Secrets ........................................ 360
    22.10.1 Paper .............................................. 360
    22.10.2 Magnetic Storage ................................. 360
  22.10.3 Solid-State Storage ................................ 362

IV Miscellaneous ............................................... 363

23 Standards ..................................................... 365
  23.1 The Standards Process ................................. 365
23.1.1 The Standard ........................................ 367
23.1.2 Functionality ........................................ 367
23.1.3 Security .............................................. 368
23.2 SSL ..................................................... 369
23.3 AES: Standardization by Competition ............... 370

24 Patents .................................................. 373
24.1 Prior Art ................................................ 373
24.2 Continuations ......................................... 374
24.3 Vagueness .............................................. 375
24.4 Reading Patents ........................................ 375
24.5 Licensing ............................................... 376
24.6 Defensive Patents ........................................ 377
24.7 Fixing the Patent System .............................. 378
24.8 Disclaimer .............................................. 379

25 Involving Experts ....................................... 381

Acknowledgments ........................................... 385

Bibliography ............................................... 387

Index ........................................................ 397