

CONTENTS IN DETAIL

FOREWORD TO THE FIRST EDITION	xvii
--------------------------------------	-------------

ACKNOWLEDGMENTS	xix
------------------------	------------

INTRODUCTION	xxi
---------------------	------------

This Book's Approach	xxii
Who This Book Is For	xxii
How This Book Is Organized	xxiii
On the Second Edition	xxiv

LIST OF ABBREVIATIONS	xxv
------------------------------	------------

PART I: FUNDAMENTALS **1**

1	
ENCRYPTION	3

The Basics	4
Classical Ciphers	4
The Caesar Cipher	4
The Vigenère Cipher	5
How Ciphers Work	6
The Permutation	7
The Mode of Operation	8
Why Classical Ciphers Are Insecure	8
The Perfect Cipher: The One-Time Pad	9
Encryption and Decryption	9
Why Is the One-Time Pad Secure?	10
Encryption Security	12
Attack Models	12
Security Goals	15
Security Notions	15
Asymmetric Encryption	18
When Ciphers Do More Than Encryption	18
Authenticated Encryption	18
Format-Preserving Encryption	19
Fully Homomorphic Encryption	20
Searchable Encryption	20
Tweakable Encryption	20

How Things Can Go Wrong	21
Weak Cipher	21
Wrong Model	22
Further Reading	22

2

RANDOMNESS **25**

Random or Nonrandom?	25
Randomness as a Probability Distribution	26
Entropy: A Measure of Uncertainty	27
Random and Pseudorandom Number Generators	28
How PRNGs Work	29
Security Concerns	30
The PRNG Fortuna	30
Cryptographic vs. Noncryptographic PRNGs	32
The Uselessness of Statistical Tests	33
Real-World PRNGs	34
Random Bits in Linux	34
The CryptGenRandom() Function in Windows	37
A Hardware-Based PRNG: Intel Secure Key	38
How Things Can Go Wrong	38
Poor Entropy Sources	39
Insufficient Entropy at Boot Time	39
Noncryptographic PRNG	40
Sampling Bug with Strong Randomness	41
Further Reading	41

3

CRYPTOGRAPHIC SECURITY **43**

Defining the Impossible	44
Security in Theory: Unconditional Security	44
Security in Practice: Computational Security	44
Quantifying Security	46
Measuring Security in Bits	46
Calculating the Full Attack Cost	47
Choosing and Evaluating Security Levels	49
Achieving Security	50
Provable Security	50
Heuristic Security	52
Generating Keys	53
Symmetric Keys	53
Asymmetric Keys	54
Protecting Keys	55
How Things Can Go Wrong	56
Incorrect Security Proof	56
Short Keys for Legacy Support	56
Further Reading	57

4		
BLOCK CIPHERS		61
What Is a Block Cipher?	62	
Security Goals	62	
Block Size	62	
The Codebook Attack	63	
How to Construct Block Ciphers	63	
A Block Cipher’s Rounds	64	
The Slide Attack and Round Keys	64	
Substitution–Permutation Networks	65	
Feistel Schemes	66	
The Advanced Encryption Standard	67	
AES Internals	67	
AES in Action	70	
How to Implement AES	71	
Table-Based Implementations	71	
Native Instructions	72	
AES Security	73	
Modes of Operation	74	
Electronic Codebook Mode	74	
Cipher Block Chaining Mode	76	
Message Encryption in CBC Mode	78	
Counter Mode	80	
How Things Can Go Wrong	82	
Meet-in-the-Middle Attacks	82	
Padding Oracle Attacks	83	
Further Reading	85	
5		
STREAM CIPHERS		87
How Stream Ciphers Work	88	
Hardware-Oriented Stream Ciphers	89	
Feedback Shift Registers	90	
Grain-128a	97	
A5/1	98	
Software-Oriented Stream Ciphers	101	
RC4	102	
Salsa20	106	
How Things Can Go Wrong	111	
Nonce Reuse	111	
Broken RC4 Implementation	111	
Weak Ciphers Baked into Hardware	113	
Further Reading	113	
6		
HASH FUNCTIONS		115
Secure Hash Functions	116	
Unpredictability Again	117	
Preimage Resistance	117	

Collision Resistance	119
How to Find Collisions	120
How to Build Hash Functions	122
Compression-Based Hash Functions	122
Permutation-Based Hash Functions	125
The SHA Family of Hash Functions	126
SHA-1	127
SHA-2	129
The SHA-3 Competition	131
Keccak (SHA-3)	132
The BLAKE2 and BLAKE3 Hash Functions	133
How Things Can Go Wrong	135
The Length-Extension Attack	135
Fooling Proof-of-Storage Protocols	136
Further Reading	137

7

KEYED HASHING

139

Message Authentication Codes	140
MACs in Secure Communication	140
Forgery and Chosen-Message Attacks	140
Replay Attacks	141
Pseudorandom Functions	141
PRF Security	141
PRFs Are Stronger Than MACs	141
How to Create Keyed Hashes from Unkeyed Hashes	142
The Secret-Prefix Construction	142
The Secret-Suffix Construction	143
The HMAC Construction	144
A Generic Attack Against Hash-Based MACs	145
How to Create Keyed Hashes from Block Ciphers	146
Breaking CBC-MAC	146
Fixing CBC-MAC	146
Dedicated MAC Designs	148
Poly1305	148
SipHash	151
How Things Can Go Wrong	153
Timing Attacks on MAC Verification	153
When Sponges Leak	155
Further Reading	155

8

AUTHENTICATED ENCRYPTION

157

Authenticated Encryption Using MACs	158
Encrypt-and-MAC Approach	158
MAC-Then-Encrypt Composition	159
Encrypt-Then-MAC Composition	159
Authenticated Ciphers	160
Authenticated Encryption with Associated Data	160
Predictability and Nonces	161
Criteria for a Good Authenticated Cipher	162

The AES-GCM Authenticated Cipher Standard	164
GCM Internals	164
GCM Security	166
GCM Efficiency	166
The OCB Authenticated Cipher Mode	167
OCB Internals	167
OCB Security	168
OCB Efficiency	168
The SIV Authenticated Cipher Mode	169
Permutation-Based AEAD	169
How Things Can Go Wrong	171
AES-GCM and Weak Hash Keys	171
AES-GCM and Small Tags	173
Further Reading	173

PART III: ASYMMETRIC CRYPTO **175**

9 **HARD PROBLEMS** **177**

Computational Hardness	178
Running Time	178
Polynomial vs. Superpolynomial Time	180
Complexity Classes	182
Nondeterministic Polynomial Time	182
NP-Complete Problems	183
The P vs. NP Problem	185
The Factoring Problem	186
Factoring Large Numbers	187
Factoring Is Probably Not NP-Hard	188
The Discrete Logarithm Problem	189
Groups	189
The Hard Thing	190
How Things Can Go Wrong	191
When Factoring Is Easy	191
Small Hard Problems Aren't Hard	192
Further Reading	193

10 **RSA** **195**

The Math Behind RSA	196
The RSA Trapdoor Permutation	197
RSA Key Generation and Security	198
Encrypting with RSA	199
Textbook RSA Encryption's Malleability	199
Strong RSA Encryption with OAEP	200
Signing with RSA	202
Textbook RSA Signatures	203
The PSS Signature Standard	203
Full Domain Hash Signatures	205

RSA Implementations	205
A Fast Exponentiation Algorithm	206
Small Exponents for Faster Public-Key Operations	208
The Chinese Remainder Theorem	210
How Things Can Go Wrong	211
The Bellcore Attack on RSA-CRT	211
Shared Private Exponents or Moduli	212
Further Reading	213

11

DIFFIE–HELLMAN 215

The Diffie–Hellman Function	216
The Diffie–Hellman Problems	218
The Computational Problem	218
The Decisional Problem	218
Variants of Diffie–Hellman	219
Key Agreement Protocols	219
Non-DH Key Agreement.	219
Attack Models for Key Agreement Protocols	221
Performance	222
Diffie–Hellman Protocols	223
Anonymous Diffie–Hellman.	223
Authenticated Diffie–Hellman	224
Menezes–Qu–Vanstone	227
How Things Can Go Wrong	228
Not Hashing the Shared Secret.	228
Anonymous Diffie–Hellman from TLS 1.0	229
Unsafe Group Parameters	229
Further Reading	230

12

ELLIPTIC CURVES 231

What Is an Elliptic Curve?.	232
Elliptic Curves Over Integers.	233
The Addition Law	235
Elliptic Curve Groups.	239
The ECDLP Problem	240
Diffie–Hellman Key Agreement over Elliptic Curves.	241
Signing with Elliptic Curves	241
ECDSA Signature Generation	242
ECDSA Signature Verification	242
ECDSA vs. RSA Signatures.	243
EdDSA and Ed25519	244
Encrypting with Elliptic Curves	246
Choosing a Curve	246
NIST Curves.	247
Curve25519	248
Other Curves	248

How Things Can Go Wrong	249
ECDSA with Bad Randomness	249
Invalid Curve Attacks	249
Incompatible Ed25519 Validation Rules	250
Further Reading	251

PART IV: APPLICATIONS

253

13

TLS

255

Target Applications and Requirements	256
The TLS Protocol Suite	256
The TLS and SSL Families of Protocols	257
TLS in a Nutshell	257
Certificates and Certificate Authorities	258
The Record Protocol	262
The TLS Handshake Protocol	263
TLS 1.3 Cryptographic Algorithms	265
TLS 1.3 Improvements over TLS 1.2	266
Downgrade Protection	266
Single Round-Trip Handshake	267
Session Resumption	267
The Strengths of TLS Security	268
Authentication	268
Forward Secrecy	268
How Things Can Go Wrong	269
Compromised Certificate Authority	269
Compromised Server	269
Compromised Client	270
Bugs in Implementations	270
Further Reading	271

14

QUANTUM AND POST-QUANTUM

273

How Quantum Computers Work	274
Quantum Bits	274
Quantum Gates	277
Quantum Speedup	279
Exponential Speedup and Simon’s Problem	280
The Threat of Shor’s Algorithm	281
Grover’s Algorithm	282
Why Is It So Hard to Build a Quantum Computer?	284
Post-Quantum Cryptographic Algorithms	285
Code-Based Cryptography	285
Lattice-Based Cryptography	286
Multivariate Cryptography	287
Hash-Based Cryptography	288
The NIST Standards	289

How Things Can Go Wrong	291
Unclear Security Level	291
The Eventual Existence of Large Quantum Computers.	291
Implementation Issues	292
Further Reading	293

15

CRYPTOCURRENCY CRYPTOGRAPHY 295

Hashing Applications	296
Merkle Trees	297
Proof of Work	300
Hierarchical Key Derivation	301
Algebraic Hash Functions	302
How Things Can Go Wrong.	304
Multisignature Protocols	306
Multiple Multiparty Signatures	306
Schnorr Signature Protocols	307
How Things Can Go Wrong.	309
Safer Schnorr Multisignatures	310
Aggregate Signature Protocols.	311
Pairings	312
BLS Signatures	312
How Things Can Go Wrong.	314
Threshold Signature Protocols	316
Use Cases	316
Security Model	317
Secret-Sharing Techniques	319
The Trivial Case	320
The Simple Case.	320
The Hard Case	321
How Things Can Go Wrong.	321
Zero-Knowledge Proofs	323
Security Model	324
Schnorr’s Protocol	325
Noninteractive Proofs	326
zkSNARKs	327
From Statements to Proofs.	328
How Things Can Go Wrong.	329
Really Serious Crypto	330

INDEX 333