BRIEF CONTENTS

Foreword by Matthew D. Green xv

Preface xvii

Abbreviations xxi

Chapter 1: Encryption 1

Chapter 2: Randomness 21

Chapter 3: Cryptographic Security 39

Chapter 4: Block Ciphers 53

Chapter 5: Stream Ciphers 77

Chapter 6: Hash Functions 105

Chapter 7: Keyed Hashing 127

Chapter 8: Authenticated Encryption 145

Chapter 9: Hard Problems 163

Chapter 10: RSA 181

Chapter 11: Diffie–Hellman 201

Chapter 12: Elliptic Curves 217

Chapter 13: TLS 235

Chapter 14: Quantum and Post-Quantum 251

Index 271

CONTENTS IN DETAIL

FOREWORD by Matthew D. Green **xv**

PREFACE **xvii**

This Book's Approach xviii
Who This Book Is For xviii
How This Book Is Organized xix
Fundamentals xix
Symmetric Crypto xix
Asymmetric Crypto xix
Applications xx
Acknowledgments xx

ABBREVIATIONS **xxi**

1
ENCRYPTION **1**

The Basics 2
Classical Ciphers 2
The Caesar Cipher 2
The Vigenère Cipher 3
How Ciphers Work 4
The Permutation 4
The Mode of Operation 5
Why Classical Ciphers Are Insecure 6
Perfect Encryption: The One-Time Pad 7
Encrypting with the One-Time Pad 7
Why Is the One-Time Pad Secure? 8
Encryption Security 9
Attack Models 10
Security Goals 12
Security Notions 13
Asymmetric Encryption 15
When Ciphers Do More Than Encryption 16
Authenticated Encryption 16
Format-Preserving Encryption 16
Fully Homomorphic Encryption 17
Searchable Encryption 17
Tweakable Encryption 17
How Things Can Go Wrong 18
Weak Cipher 18
Wrong Model 19
Further Reading 19

2
RANDOMNESS 21

Random or Non-Random? 22
Randomness as a Probability Distribution 22
Entropy: A Measure of Uncertainty 23
Random Number Generators (RNGs) and
Pseudorandom Number Generators (PRNGs) 24
How PRNGs Work 25
Security Concerns 26
The PRNG Fortuna 26
Cryptographic vs. Non-Cryptographic PRNGs 27
The Uselessness of Statistical Tests 29
Real-World PRNGs 29
Generating Random Bits in Unix-Based Systems 30
The CryptGenRandom() Function in Windows 33
A Hardware-Based PRNG: RDRAND in Intel Microprocessors 34
How Things Can Go Wrong 35
Poor Entropy Sources 35
Insufficient Entropy at Boot Time 35
Non-cryptographic PRNG 36
Sampling Bug with Strong Randomness 37
Further Reading 38

3
CRYPTOGRAPHIC SECURITY 39

Defining the Impossible 40
Security in Theory: Informational Security 40
Security in Practice: Computational Security 40
Quantifying Security 42
Measuring Security in Bits 42
Full Attack Cost 43
Choosing and Evaluating Security Levels 44
Achieving Security 46
Provable Security 46
Heuristic Security 48
Generating Keys 49
Generating Symmetric Keys 49
Generating Asymmetric Keys 49
Protecting Keys 50
How Things Can Go Wrong 51
Incorrect Security Proof 52
Short Keys for Legacy Support 52
Further Reading 52

4
BLOCK CIPHERS 53

What Is a Block Cipher? 54
Security Goals 54
Block Size 54
The Codebook Attack 55

How to Construct Block Ciphers 55
A Block Cipher's Rounds 56
The Slide Attack and Round Keys 56
Substitution–Permutation Networks 57
Feistel Schemes 58
The Advanced Encryption Standard (AES) 59
AES Internals 59
AES in Action 62
Implementing AES 62
Table-Based Implementations 63
Native Instructions 63
Is AES Secure? 65
Modes of Operation 65
The Electronic Codebook (ECB) Mode 65
The Cipher Block Chaining (CBC) Mode 67
How to Encrypt Any Message in CBC Mode 69
The Counter (CTR) Mode 71
How Things Can Go Wrong 72
Meet-in-the-Middle Attacks 72
Padding Oracle Attacks 74
Further Reading 75

5
STREAM CIPHERS 77
How Stream Ciphers Work 78
Stateful and Counter-Based Stream Ciphers 79
Hardware-Oriented Stream Ciphers 79
Feedback Shift Registers 80
Grain-128a 86
A5/1 88
Software-Oriented Stream Ciphers 91
RC4 92
Salsa20 95
How Things Can Go Wrong 100
Nonce Reuse 101
Broken RC4 Implementation 101
Weak Ciphers Baked Into Hardware 102
Further Reading 103

6
HASH FUNCTIONS 105
Secure Hash Functions 106
Unpredictability Again 107
Preimage Resistance 107
Collision Resistance 109
Finding Collisions 109
Building Hash Functions 111
Compression-Based Hash Functions: The Merkle–Damgård Construction 112
Permutation-Based Hash Functions: Sponge Functions 115

The SHA Family of Hash Functions 116
SHA-1 116
SHA-2 119
The SHA-3 Competition 120
Keccak (SHA-3) 121
The BLAKE2 Hash Function 123
How Things Can Go Wrong 124
The Length-Extension Attack 125
Fooling Proof-of-Storage Protocols 125
Further Reading 126

7 KEYED HASHING 127

Message Authentication Codes (MACs) 128
MACs in Secure Communication 128
Forgery and Chosen-Message Attacks 128
Replay Attacks 129
Pseudorandom Functions (PRFs) 129
PRF Security 129
Why PRFs Are Stronger Than MACs 130
Creating Keyed Hashes from Unkeyed Hashes 130
The Secret-Prefix Construction 130
The Secret-Suffix Construction 131
The HMAC Construction 132
A Generic Attack Against Hash-Based MACs 133
Creating Keyed Hashes from Block Ciphers: CMAC 134
Breaking CBC-MAC 134
Fixing CBC-MAC 134
Dedicated MAC Designs 135
Poly1305 136
SipHash 139
How Things Can Go Wrong 140
Timing Attacks on MAC Verification 140
When Sponges Leak 142
Further Reading 143

8 AUTHENTICATED ENCRYPTION 145

Authenticated Encryption Using MACs 146
Encrypt-and-MAC 146
MAC-then-Encrypt 147
Encrypt-then-MAC 147
Authenticated Ciphers 148
Authenticated Encryption with Associated Data 149
Avoiding Predictability with Nonces 149
What Makes a Good Authenticated Cipher? 150
AES-GCM: The Authenticated Cipher Standard 152
GCM Internals: CTR and GHASH 152
GCM Security 154
GCM Efficiency 154

OCB: An Authenticated Cipher Faster than GCM. 155
OCB Internals 155
OCB Security 156
OCB Efficiency 156
SIV: The Safest Authenticated Cipher? 156
Permutation-Based AEAD 157
How Things Can Go Wrong 159
AES-GCM and Weak Hash Keys 159
AES-GCM and Small Tags 161
Further Reading 161

9 HARD PROBLEMS 163

Computational Hardness. 164
Measuring Running Time 164
Polynomial vs. Superpolynomial Time 166
Complexity Classes 168
Nondeterministic Polynomial Time. 168
NP-Complete Problems 169
The P vs. NP Problem. 170
The Factoring Problem 171
Factoring Large Numbers in Practice 172
Is Factoring NP-Complete? 173
The Discrete Logarithm Problem 174
What Is a Group? 174
The Hard Thing. 175
How Things Can Go Wrong 176
When Factoring Is Easy 176
Small Hard Problems Aren't Hard 177
Further Reading 178

10 RSA 181

The Math Behind RSA. 182
The RSA Trapdoor Permutation 183
RSA Key Generation and Security 184
Encrypting with RSA 185
Breaking Textbook RSA Encryption's Malleability 185
Strong RSA Encryption: OAEP 186
Signing with RSA 188
Breaking Textbook RSA Signatures 188
The PSS Signature Standard 189
Full Domain Hash Signatures 190
RSA Implementations 191
Fast Exponentiation Algorithm: Square-and-Multiply. 192
Small Exponents for Faster Public-Key Operations 194
The Chinese Remainder Theorem 195

How Things Can Go Wrong 196
The Bellcore Attack on RSA-CRT 196
Sharing Private Exponents or Moduli 197
Further Reading 199

11 DIFFIE–HELLMAN 201

The Diffie–Hellman Function 202
The Diffie–Hellman Problems 204
The Computational Diffie–Hellman Problem 204
The Decisional Diffie–Hellman Problem 204
More Diffie–Hellman Problems 205
Key Agreement Protocols 205
An Example of Non-DH Key Agreement 205
Attack Models for Key Agreement Protocols 207
Performance 208
Diffie–Hellman Protocols 209
Anonymous Diffie–Hellman 209
Authenticated Diffie–Hellman 210
Menezes–Qu–Vanstone (MQV) 213
How Things Can Go Wrong 214
Not Hashing the Shared Secret 214
Legacy Diffie–Hellman in TLS 215
Unsafe Group Parameters 215
Further Reading 216

12 ELLIPTIC CURVES 217

What Is an Elliptic Curve? 218
Elliptic Curves over Integers 219
Adding and Multiplying Points 221
Elliptic Curve Groups 224
The ECDLP Problem 224
Diffie–Hellman Key Agreement over Elliptic Curves 225
Signing with Elliptic Curves 226
Encrypting with Elliptic Curves 228
Choosing a Curve 229
NIST Curves 230
Curve25519 230
Other Curves 231
How Things Can Go Wrong 231
ECDSA with Bad Randomness 232
Breaking ECDH Using Another Curve 232
Further Reading 233

13
TLS 235

Target Applications and Requirements . . . 236
The TLS Protocol Suite . . . 236
The TLS and SSL Family of Protocols: A Brief History . . . 237
TLS in a Nutshell . . . 237
Certificates and Certificate Authorities . . . 238
The Record Protocol . . . 240
The TLS Handshake Protocol . . . 241
TLS 1.3 Cryptographic Algorithms . . . 243
TLS 1.3 Improvements over TLS 1.2 . . . 244
Downgrade Protection . . . 244
Single Round-Trip Handshake . . . 245
Session Resumption . . . 245
The Strengths of TLS Security . . . 246
Authentication . . . 246
Forward Secrecy . . . 246
How Things Can Go Wrong . . . 247
Compromised Certificate Authority . . . 247
Compromised Server . . . 248
Compromised Client . . . 248
Bugs in Implementations . . . 248
Further Reading . . . 249

14
QUANTUM AND POST-QUANTUM 251

How Quantum Computers Work . . . 252
Quantum Bits . . . 252
Quantum Gates . . . 255
Quantum Speed-Up . . . 257
Exponential Speed-Up and Simon's Problem . . . 258
The Threat of Shor's Algorithm . . . 259
Shor's Algorithm Solves the Factoring Problem . . . 259
Shor's Algorithm and the Discrete Logarithm Problem . . . 260
Grover's Algorithm . . . 260
Why Is It So Hard to Build a Quantum Computer? . . . 261
Post-Quantum Cryptographic Algorithms . . . 263
Code-Based Cryptography . . . 263
Lattice-Based Cryptography . . . 264
Multivariate Cryptography . . . 265
Hash-Based Cryptography . . . 266
How Things Can Go Wrong . . . 267
Unclear Security Level . . . 267
Fast Forward: What Happens if It's Too Late? . . . 268
Implementation Issues . . . 269
Further Reading . . . 269

INDEX 271