

CONTENTS

Preface	xiii
Message to students	xiv
Message to teachers	xvii
Acknowledgments	xix

UNCONDITIONAL CRYPTOGRAPHY

1 One-Time Pad and the Provable Security Mindset	3
1.1 Defining the problem	4
1.2 One-time pad	6
1.3 How to formalize an attack scenario	8
1.4 How to define and prove security of OTP	12
1.5 How to interpret a security proof	13
1.6 Limitations of security proofs	15
1.7 What's so special about XOR?	17
2 Rudiments of Provable Security	25
2.1 Attack scenarios as libraries	25
2.2 Interchangeable libraries	28
2.3 How to distinguish two libraries	33
2.4 How to prove that two libraries are interchangeable	37
2.5 Abstract cryptographic primitives	42
2.6 Modular cryptographic constructions	45
2.7 ★ "Real-or-random" vs. "left-or-right"	49
3 ★ Secret Sharing	61
3.1 Defining secret sharing	62

CONTENTS

3.2	2-out-of-2 secret sharing	65
3.3	Polynomial interpolation	68
3.4	Multiplicative inverses modulo a prime	72
3.5	Shamir secret sharing	78

PSEUDORANDOMNESS

4	Modern Computational Cryptography	87
4.1	The concrete approach to provable security	88
4.2	The asymptotic approach to provable security	91
4.3	Indistinguishability	95
4.4	The bad-event technique	98
4.5	Birthday probabilities	105
5	Pseudorandom Generators	117
5.1	Defining pseudorandomness	118
5.2	Do PRGs exist?	121
5.3	Application: Pseudo-OTP	124
5.4	How to extend a PRG's stretch	127
5.5	How to attack pseudorandomness	130
6	Pseudorandom Functions	141
6.1	Motivating and defining PRFs	142
6.2	How to attack PRFs	144
6.3	An example proof involving PRFs	148
6.4	Building a PRG from a PRF: The CTR construction	153
6.5	★ Building a PRF from a PRG: The GGM construction	158
6.6	PRFs for long inputs: The CBC-MAC construction	166
7	Pseudorandom Permutations	181
7.1	Defining PRPs	182
7.2	Comparing PRPs and PRFs, and the switching lemma	184
7.3	How to construct a PRP: The Feistel construction	186
7.4	PRPs in theory and practice	194
7.5	★ Strong PRPs	198

SYMMETRIC-KEY ENCRYPTION

8	Chosen-Plaintext Attacks Against Encryption	205
8.1	Definitions and leaking the plaintext length	206
8.2	Deterministic encryption	209
8.3	A randomized encryption scheme based on PRFs	210
8.4	An example chosen-plaintext attack	214
8.5	Block cipher modes	215
8.6	Non-block-aligned plaintexts	224
8.7	★ Nonce-based encryption	228
9	Chosen-Ciphertext Attacks Against Encryption	245
9.1	Format-oracle attacks and malleability	246
9.2	Defining security against chosen-ciphertext attacks	251
9.3	Chosen-ciphertext attack strategies	255
9.4	Message authentication codes	261
9.5	Encrypt-then-MAC	267
9.6	Authenticated encryption and associated data	273

HASHING

10	Collision-Resistant Hash Functions	295
10.1	Defining collision resistance	296
10.2	Hash functions in the real world	300
10.3	Composing collision-resistant functions	303
10.4	The Merkle-Damgård construction	306
10.5	PRFs from Merkle-Damgård: Length extension, NMAC, and HMAC	310
11	★ Universal Hash Functions	325
11.1	Defining universal hash functions	326
11.2	Universal hash paradigm for PRFs	330
11.3	CBC-MAC is a UHF	333
11.4	Poly-UHF: An unconditionally secure UHF	342
12	Random Oracles and Other Idealized Models	355
12.1	Defining the random oracle model	356
12.2	Using random oracles	361
12.3	★ The ideal permutation model	367
12.4	★ The ideal cipher model	376

CONTENTS

ASYMMETRIC-KEY CRYPTOGRAPHY

13 Key Exchange	391
13.1 Cyclic groups	391
13.2 Diffie-Hellman key exchange	398
13.3 Key exchange in the abstract	403
13.4 ★ Elliptic curves	404
14 Public-Key Encryption	419
14.1 Security definitions for PKE	419
14.2 One-time vs. many-time encryption	422
14.3 El Gamal encryption	426
14.4 The Fujisaki-Okamoto construction	431
14.5 Hybrid encryption	441
14.6 Key encapsulation	444
15 RSA	457
15.1 Arithmetic modulo a composite	457
15.2 The RSA function and RSA assumption	462
15.3 Building a KEM from RSA	467
15.4 ★ Chinese remainder theorem	474
16 Digital Signatures	489
16.1 Security definitions for digital signatures	490
16.2 Signatures from RSA	492
16.3 Common signature idioms	507

ADVANCED TOPICS

17 Encrypted Messaging and Ratcheting	523
17.1 Forward secrecy and the symmetric ratchet	524
17.2 Post-compromise secrecy and the asymmetric ratchet	528
17.3 The double ratchet and the Signal protocol	530
17.4 Group messaging and MLS	535

CONTENTS

18 Authenticated Key Exchange	545
18.1 Defining the problem	546
18.2 Authenticating with signatures	550
18.3 Authenticating implicitly	557
18.4 Authenticated key exchange in practice	562
19 Zero-Knowledge Proofs	569
19.1 The Schnorr identification protocol	570
19.2 Sigma protocols	575
19.3 More examples of sigma protocols	578
19.4 Noninteractive proofs and signatures	586
20 Post-Quantum Cryptography	601
20.1 Capabilities of quantum computing	602
20.2 The learning-with-errors problem	604
20.3 Key exchange from LWE	610

APPENDIX

A Math Review	625
A.1 Strings	625
A.2 Probability	626
A.3 Modular arithmetic	630
A.4 Exponents and logarithms	635
A.5 Big- O	635
A.6 Linear algebra	636
B A Crash Course in Binary Finite Fields	641
Bibliography	647
Index	673