Jonathan Katz and Yehuda Lindell

Introduction to Modern Cryptography

CRC PRESS
Boca Raton London New York Washington, D.C.

Preface

This book presents the basic paradigms and principles of modern cryptography. It is designed to serve as a textbook for undergraduate- or graduate-level courses in cryptography (in computer science or mathematics departments), as a general introduction suitable for self-study (especially for beginning graduate students), and as a reference for students, researchers, and practitioners.

There are numerous other cryptography textbooks available today, and the reader may rightly ask whether another book on the subject is needed. We would not have written this book if the answer to that question were anything other than an unequivocal *yes*. The novelty of this book — and what, in our opinion, distinguishes it from all other books currently available — is that it provides a *rigorous* treatment of modern cryptography in an *accessible* manner appropriate for an introduction to the topic.

As mentioned, our focus is on *modern* (post-1980s) cryptography, which is distinguished from classical cryptography by its emphasis on definitions, precise assumptions, and rigorous proofs of security. We briefly discuss each of these in turn (these principles are explored in greater detail in Chapter 1):

- **The central role of definitions:** A key intellectual contribution of modern cryptography has been the recognition that *formal definitions of security are an essential first step in the design of any cryptographic primitive or protocol.* The reason, in retrospect, is simple: if you don't know what it is you are trying to achieve, how can you hope to know when you have achieved it? As we will see in this book, cryptographic definitions of security are quite strong and — at first glance — may appear impossible to achieve. One of the most amazing aspects of cryptography is that (under mild and widely-believed assumptions) efficient constructions satisfying such strong definitions can be proven to exist.

- **The importance of formal and precise assumptions:** As will be explained in Chapters 2 and 3, many cryptographic constructions cannot currently be proven secure in an unconditional sense. Security often relies, instead, on some widely-believed (albeit unproven) assumption. The modern cryptographic approach dictates that *any such assumption must be clearly stated and unambiguously defined.* This not only allows for objective evaluation of the assumption but, more importantly, enables rigorous proofs of security as described next.

- **The possibility of rigorous proofs of security:** The previous two ideas lead naturally to the current one, which is the realization that *cryp-*

tographic constructions can be proven secure with respect to a clearly-stated definition of security and relative to a well-defined cryptographic assumption. This is the essence of modern cryptography, and what has transformed cryptography from an art to a science.

The importance of this idea cannot be over-emphasized. Historically, cryptographic schemes were designed in a largely ad-hoc fashion, and were deemed to be secure if the designers themselves could not find any attacks. In contrast, modern cryptography promotes the design of schemes with formal, mathematical proofs of security in well-defined models. Such schemes are *guaranteed* to be secure unless the underlying assumption is false (or the security definition did not appropriately model the real-world security concerns). By relying on long-standing assumptions (e.g., the assumption that "factoring is hard"), it is thus possible to obtain schemes that are extremely unlikely to be broken.

A unified approach. The above contributions of modern cryptography are relevant not only to the "theory of cryptography" community. The importance of precise definitions is, by now, widely understood and appreciated by those in the security community who use cryptographic tools to build secure systems, and rigorous proofs of security have become one of the requirements for cryptographic schemes to be standardized. As such, we do not separate "applied cryptography" from "provable security"; rather, we present practical and widely-used constructions along with precise statements (and, most of the time, a proof) of what definition of security is achieved.

Guide to Using this Book

This section is intended primarily for instructors seeking to adopt this book for their course, though the student picking up this book on his or her own may also find it a useful overview of the topics that will be covered.

Required background. This book uses definitions, proofs, and mathematical concepts, and therefore requires some mathematical maturity. In particular, the reader is assumed to have had some exposure to proofs at the college level, say in an upper-level mathematics course or a course on discrete mathematics, algorithms, or computability theory. Having said this, we have made a significant effort to simplify the presentation and make it generally accessible. It is our belief that this book is not more difficult than analogous textbooks that are less rigorous. On the contrary, we believe that (to take one example) once security goals are clearly formulated, it often becomes easier to understand the design choices made in a particular construction.

We have structured the book so that the only formal prerequisites are a course in algorithms and a course in discrete mathematics. Even here we rely on very little material: specifically, we assume some familiarity with basic probability and big-$\mathcal{O}$ notation, modular arithmetic, and the idea of equating efficient algorithms with those running in polynomial time. These concepts are reviewed in Appendix A and/or when first used in the book.

Suggestions for course organization. The core material of this book, which we strongly recommend should be covered in any introductory course on cryptography, consists of the following (starred sections are excluded in what follows; see further discussion regarding starred material below):

- Chapters 1–4 (through Section 4.6), discussing classical cryptography, modern cryptography, and the basics of private-key cryptography (both private-key encryption and message authentication).
- Chapter 5, illustrating basic design principles for block ciphers and including material on the widely-used block ciphers DES and AES.[1]
- Chapter 7, introducing concrete mathematical problems believed to be "hard", and providing the number-theoretic background needed to understand the RSA, Diffie-Hellman, and El Gamal cryptosystems. This chapter also gives the first examples of how number-theoretic assumptions are used in cryptography.
- Chapters 9 and 10, motivating the public-key setting and discussing public-key encryption (including RSA-based schemes and El Gamal encryption).
- Chapter 12, describing digital signature schemes.
- Sections 13.1 and 13.3, introducing the random oracle model and the RSA-FDH signature scheme.

We believe that this core material — possibly omitting some of the more in-depth discussion and proofs — can be covered in a 30–35-hour undergraduate course. Instructors with more time available could proceed at a more leisurely pace, e.g., giving details of all proofs and going more slowly when introducing the underlying group theory and number-theoretic background. Alternatively, additional topics could be incorporated as discussed next.

Those wishing to cover additional material, in either a longer course or a faster-paced graduate course, will find that the book has been structured to allow flexible incorporation of other topics as time permits (and depending on the instructor's interests). Specifically, some of the chapters and sections are starred (*). These sections are not less important in any way, but arguably do not constitute "core material" for an introductory course in cryptography. As made evident by the course outline just given (which does not include any starred material), starred chapters and sections may be skipped — or covered at any point subsequent to their appearance in the book — without affecting

[1] Although we consider this to be core material, it is not used in the remainder of the book and so this chapter can be skipped if desired.

the flow of the course. In particular, we have taken care to ensure that none of the later un-starred material depends on any starred material. For the most part, the starred chapters also do not depend on each other (and when they do, this dependence is explicitly noted).

We suggest the following from among the starred topics for those wishing to give their course a particular flavor:

- *Theory:* A more theoretically-inclined course could include material from Section 3.2.2 (building to a definition of semantic security for encryption); Sections 4.8 and 4.9 (dealing with stronger notions of security for private-key encryption); Chapter 6 (introducing one-way functions and hard-core bits, and constructing pseudorandom generators and pseudorandom functions/permutations starting from any one-way permutation); Section 10.7 (constructing public-key encryption from trapdoor permutations); Chapter 11 (describing the Goldwasser-Micali, Rabin, and Paillier encryption schemes); and Section 12.6 (showing a signature scheme that does not rely on random oracles).

- *Applications:* An instructor wanting to emphasize practical aspects of cryptography is highly encouraged to cover Section 4.7 (describing HMAC) and all of Chapter 13 (giving cryptographic constructions in the random oracle model).

- *Mathematics:* A course directed at students with a strong mathematics background — or taught by someone who enjoys this aspect of cryptography — could incorporate some of the more advanced number theory from Chapter 7 (e.g., the Chinese remainder theorem and/or elliptic-curve groups); all of Chapter 8 (algorithms for factoring and computing discrete logarithms); and selections from Chapter 11 (describing the Goldwasser-Micali, Rabin, and Paillier encryption schemes along with the necessary number-theoretic background).

Comments and Errata

Our goal in writing this book was to make modern cryptography accessible to a wide audience outside the "theoretical computer science" community. We hope you will let us know whether we have succeeded. In particular, we are always more than happy to receive feedback on this book, especially constructive comments telling us how the book can be improved. We hope there are no errors or typos in the book; if you do find any, however, we would greatly appreciate it if you let us know. (A list of known errata will be maintained at `http://www.cs.umd.edu/~jkatz/imc.html`.) You can email your comments and errata to `jkatz@cs.umd.edu` and `lindell@cs.biu.ac.il`; please put "Introduction to Modern Cryptography" in the subject line.

Acknowledgements

Jonathan Katz: I am indebted to Zvi Galil, Moti Yung, and Rafail Ostrovsky for their help, guidance, and support throughout my career. This book would never have come to be without their contributions to my development. I would also like to thank my colleagues with whom I have enjoyed numerous discussions on the "right" approach to writing a cryptography textbook. My work on this project was supported in part by the National Science Foundation under Grants #0627306, #0447075, and #0310751. Any opinions, findings, and conclusions or recommendations expressed in this book are my own, and do not necessarily reflect the views of the National Science Foundation.

Yehuda Lindell: I wish to first and foremost thank Oded Goldreich and Moni Naor for introducing me to the world of cryptography. Their influence is felt until today and will undoubtedly continue to be felt in the future. There are many, many other people who have also had considerable influence over the years and instead of mentioning them all, I will just say *thank you* — you know who you are.

We both thank Zoe Bermant for producing the figures used in this book; David Wagner for answering questions related to block ciphers and their cryptanalysis; and Salil Vadhan and Alon Rosen for experimenting with this text in an introductory course on cryptography at Harvard University and providing us with valuable feedback. We would also like to extend our gratitude to those who read and commented on earlier drafts of this book: Adam Bender, Chiu-Yuen Koo, Yair Dombb, William Glenn, S. Dov Gordon, Carmit Hazay, Eyal Kushilevitz, Avivit Levy, Matthew Mah, Martin Paraskevov, Jason Rogers, Rui Xue, Dicky Yan, Arkady Yerukhimovich, and Hila Zarosim. Their comments have greatly improved the book and helped minimize the number of errors. We are extremely grateful to all those who encouraged us to write this book, and concurred with our feeling that a book of this nature is badly needed.

Finally, we thank our (respective) wives and children for all their support and understanding during the many hours, days, and months that we have spent on this project.

Contents

Preface **iii**

I Introduction and Classical Cryptography **1**

1 Introduction **3**
1.1 Cryptography and Modern Cryptography 3
1.2 The Setting of Private-Key Encryption 4
1.3 Historical Ciphers and Their Cryptanalysis 9
1.4 The Basic Principles of Modern Cryptography 18
1.4.1 Principle 1 – Formulation of Exact Definitions 18
1.4.2 Principle 2 – Reliance on Precise Assumptions 24
1.4.3 Principle 3 – Rigorous Proofs of Security 26
References and Additional Reading 27
Exercises 27

2 Perfectly-Secret Encryption **29**
2.1 Definitions and Basic Properties 29
2.2 The One-Time Pad (Vernam's Cipher) 34
2.3 Limitations of Perfect Secrecy 36
2.4 * Shannon's Theorem 37
2.5 Summary 40
References and Additional Reading 40
Exercises 41

II Private-Key (Symmetric) Cryptography **45**

3 Private-Key Encryption and Pseudorandomness **47**
3.1 A Computational Approach to Cryptography 47
3.1.1 The Basic Idea of Computational Security 48
3.1.2 Efficient Algorithms and Negligible Success Probability 54
3.1.3 Proofs by Reduction 58
3.2 Defining Computationally-Secure Encryption 60
3.2.1 The Basic Definition of Security 61
3.2.2 * Properties of the Definition 64
3.3 Pseudorandomness 69
3.4 Constructing Secure Encryption Schemes 72
3.4.1 A Secure Fixed-Length Encryption Scheme 72
3.4.2 Handling Variable-Length Messages 76

3.4.3 Stream Ciphers and Multiple Encryptions 77
3.5 Security Against Chosen-Plaintext Attacks (CPA) 82
3.6 Constructing CPA-Secure Encryption Schemes 85
3.6.1 Pseudorandom Functions 86
3.6.2 CPA-Secure Encryption from Pseudorandom Functions 89
3.6.3 Pseudorandom Permutations and Block Ciphers . . . 94
3.6.4 Modes of Operation 96
3.7 Security Against Chosen-Ciphertext Attacks (CCA) 103
References and Additional Reading 105
Exercises 106

4 Message Authentication Codes and Collision-Resistant Hash Functions 111
4.1 Secure Communication and Message Integrity 111
4.2 Encryption vs. Message Authentication 112
4.3 Message Authentication Codes – Definitions 114
4.4 Constructing Secure Message Authentication Codes 118
4.5 CBC-MAC 125
4.6 Collision-Resistant Hash Functions 127
4.6.1 Defining Collision Resistance 128
4.6.2 Weaker Notions of Security for Hash Functions 130
4.6.3 A Generic "Birthday" Attack 131
4.6.4 The Merkle-Damgård Transform 133
4.6.5 Collision-Resistant Hash Functions in Practice 136
4.7 * NMAC and HMAC 138
4.7.1 Nested MAC (NMAC) 138
4.7.2 HMAC 141
4.8 * Constructing CCA-Secure Encryption Schemes 144
4.9 * Obtaining Privacy and Message Authentication 148
References and Additional Reading 154
Exercises 155

5 Practical Constructions of Pseudorandom Permutations (Block Ciphers) 159
5.1 Substitution-Permutation Networks 162
5.2 Feistel Networks 170
5.3 DES – The Data Encryption Standard 173
5.3.1 The Design of DES 173
5.3.2 Attacks on Reduced-Round Variants of DES 176
5.3.3 The Security of DES 179
5.4 Increasing the Key Length of a Block Cipher 181
5.5 AES – The Advanced Encryption Standard 185
5.6 Differential and Linear Cryptanalysis – A Brief Look 187
Additional Reading and References 189
Exercises 189

6 * Theoretical Constructions of Pseudorandom Objects 193
6.1 One-Way Functions 194
6.1.1 Definitions 194
6.1.2 Candidate One-Way Functions 197
6.1.3 Hard-Core Predicates 198
6.2 Overview: From One-Way Functions to Pseudorandomness . 200
6.3 A Hard-Core Predicate for Any One-Way Function 202
6.3.1 A Simple Case 202
6.3.2 A More Involved Case 203
6.3.3 The Full Proof 208
6.4 Constructing Pseudorandom Generators 213
6.4.1 Pseudorandom Generators with Minimal Expansion . 214
6.4.2 Increasing the Expansion Factor 215
6.5 Constructing Pseudorandom Functions 221
6.6 Constructing (Strong) Pseudorandom Permutations 225
6.7 Necessary Assumptions for Private-Key Cryptography 227
6.8 A Digression – Computational Indistinguishability 232
6.8.1 Pseudorandomness and Pseudorandom Generators . . 233
6.8.2 Multiple Samples 234
References and Additional Reading 237
Exercises 237

III Public-Key (Asymmetric) Cryptography 241

7 Number Theory and Cryptographic Hardness Assumptions 243
7.1 Preliminaries and Basic Group Theory 245
7.1.1 Primes and Divisibility 246
7.1.2 Modular Arithmetic 248
7.1.3 Groups 250
7.1.4 The Group $\mathbb{Z}_N^*$ 254
7.1.5 * Isomorphisms and the Chinese Remainder Theorem 256
7.2 Primes, Factoring, and RSA 261
7.2.1 Generating Random Primes 262
7.2.2 * Primality Testing 265
7.2.3 The Factoring Assumption 271
7.2.4 The RSA Assumption 271
7.3 Assumptions in Cyclic Groups 274
7.3.1 Cyclic Groups and Generators 274
7.3.2 The Discrete Logarithm and Diffie-Hellman Assumptions 277
7.3.3 Working in (Subgroups of) $\mathbb{Z}_p^*$ 281
7.3.4 * Elliptic Curve Groups 282
7.4 Cryptographic Applications of Number-Theoretic Assumptions 287
7.4.1 One-Way Functions and Permutations 287
7.4.2 Constructing Collision-Resistant Hash Functions . . . 290

References and Additional Reading 293
Exercises 294

8 * Factoring and Computing Discrete Logarithms 297
8.1 Algorithms for Factoring 297
8.1.1 Pollard's $p-1$ Method 298
8.1.2 Pollard's Rho Method 301
8.1.3 The Quadratic Sieve Algorithm 303
8.2 Algorithms for Computing Discrete Logarithms 305
8.2.1 The Baby-Step/Giant-Step Algorithm 307
8.2.2 The Pohlig-Hellman Algorithm 309
8.2.3 The Discrete Logarithm Problem in $\mathbb{Z}_N$ 310
8.2.4 The Index Calculus Method 311
References and Additional Reading 313
Exercises 314

9 Private-Key Management and the Public-Key Revolution 315
9.1 Limitations of Private-Key Cryptography 315
9.2 A Partial Solution – Key Distribution Centers 317
9.3 The Public-Key Revolution 320
9.4 Diffie-Hellman Key Exchange 324
References and Additional Reading 330
Exercises 331

10 Public-Key Encryption 333
10.1 Public-Key Encryption – An Overview 333
10.2 Definitions 336
10.2.1 Security against Chosen-Plaintext Attacks 337
10.2.2 Multiple Encryptions 340
10.3 Hybrid Encryption 347
10.4 RSA Encryption 355
10.4.1 "Textbook RSA" and its Insecurity 355
10.4.2 Attacks on Textbook RSA 359
10.4.3 Padded RSA 362
10.5 The El Gamal Encryption Scheme 364
10.6 Security Against Chosen-Ciphertext Attacks 369
10.7 * Trapdoor Permutations 373
10.7.1 Definition 374
10.7.2 Public-Key Encryption from Trapdoor Permutations . 375
References and Additional Reading 378
Exercises 379

11 * Additional Public-Key Encryption Schemes 385
11.1 The Goldwasser-Micali Encryption Scheme 386
11.1.1 Quadratic Residues Modulo a Prime 386
11.1.2 Quadratic Residues Modulo a Composite 389
11.1.3 The Quadratic Residuosity Assumption 392
11.1.4 The Goldwasser-Micali Encryption Scheme 394
11.2 The Rabin Encryption Scheme 397
11.2.1 Computing Modular Square Roots 397
11.2.2 A Trapdoor Permutation Based on Factoring 402
11.2.3 The Rabin Encryption Scheme 406
11.3 The Paillier Encryption Scheme 408
11.3.1 The Structure of $\mathbb{Z}^*_{N^2}$ 409
11.3.2 The Paillier Encryption Scheme 411
11.3.3 Homomorphic Encryption 416
References and Additional Reading 418
Exercises 418

12 Digital Signature Schemes 421
12.1 Digital Signatures – An Overview 421
12.2 Definitions 423
12.3 RSA Signatures 426
12.3.1 "Textbook RSA" and its Insecurity 426
12.3.2 Hashed RSA 428
12.4 The "Hash-and-Sign" Paradigm 429
12.5 Lamport's One-Time Signature Scheme 432
12.6 * Signatures from Collision-Resistant Hashing 435
12.6.1 "Chain-Based" Signatures 436
12.6.2 "Tree-Based" Signatures 439
12.7 The Digital Signature Standard (DSS) 445
12.8 Certificates and Public-Key Infrastructures 446
References and Additional Reading 453
Exercises 454

13 Public-Key Cryptosystems in the Random Oracle Model 457
13.1 The Random Oracle Methodology 458
13.1.1 The Random Oracle Model in Detail 459
13.1.2 Is the Random Oracle Methodology Sound? 465
13.2 Public-Key Encryption in the Random Oracle Model 469
13.2.1 Security Against Chosen-Plaintext Attacks 469
13.2.2 Security Against Chosen-Ciphertext Attacks 473
13.2.3 OAEP 479
13.3 Signatures in the Random Oracle Model 481
References and Additional Reading 486
Exercises 486

Index of Common Notation **489**

A Mathematical Background **493**
A.1 Identities and Inequalities 493
A.2 Asymptotic Notation 493
A.3 Basic Probability 494
A.4 The “Birthday” Problem 496

B Supplementary Algorithmic Number Theory **499**
B.1 Integer Arithmetic 501
B.1.1 Basic Operations 501
B.1.2 The Euclidean and Extended Euclidean Algorithms . 502
B.2 Modular Arithmetic 504
B.2.1 Basic Operations 504
B.2.2 Computing Modular Inverses 505
B.2.3 Modular Exponentiation 505
B.2.4 Choosing a Random Group Element 508
B.3 * Finding a Generator of a Cyclic Group 512
B.3.1 Group-Theoretic Background 512
B.3.2 Efficient Algorithms 513
References and Additional Reading 515
Exercises 515

References **517**

Index

Advanced Encryption Standard (AES)
  attacks, 187
  competition, 160, 185–186
  design, 186–187
Assumptions, reliance on, 24–26
Asymmetric encryption, *see* public-key encryption
Asymptotic security, 57–58
Authenticated communication
  definition of, 151
Authentication, message, *see* message authentication
Avalanche effect, 166–168, 170, 175, 176

Birthday problem, 123, 131–133, 301, 463, **496–497**
Block cipher, *see* pseudorandom permutation
  "meet-in-the-middle" attack on, 183
  AES, *see* AES
  as strong pseudorandom permutation, 95, 159–161
  block length and security, 101, 180
  constructions, 159–172
  cryptanalysis, 168–170, 176–179, 181–184, 187–188
  DES, *see* DES
  key length and security, 179
  modes of operation, 96–102
  taxonomy of attacks, 161–162
Blum integer, 405, **405**, 406
Blum-Micali pseudorandom generator, 220

Caesar's cipher, 10
CBC mode, *see* modes of operation
CBC-MAC, 124–127, 143, 152, 154
Certificate, 446–453
  revocation, 452
Certificate authority, 447
Challenge ciphertext, 63, 82, 92, 103, 338, 339
Chinese remainder theorem, **257**, 256–261, 269, 298, 300, 301, 309, 358, 359, 389, 401, 403
Chosen-ciphertext attack, *see* private-key encryption, CCA-security, *see* public-key encryption, CCA-security, 8, **103–105**, 363
  on block cipher, 161
Chosen-plaintext attack, *see* private-key encryption, CPA-security, *see* public-key encryption, CPA-security, 8, 21, **82–85**
  on block cipher, 161, 181, 184, 188
Cipher block chaining, *see* CBC-MAC, *see* modes of operation
Ciphertext-only attack, 8, 17, 21, 61
  on block cipher, 161
Collision-resistant hash function, 127–137
  birthday attack on, 131–133, 137, 141
  construction, 290–293, 296
  definition of collision resistance, 130
  MD5, 137
  Merkle-Damgård transform, 133–136
  random oracle as, 463
  SHA-1, 137, 140, 141, 161, 429
  signature scheme based on, 435–445
  syntax, 129
Compression function, *see* collision- resistant hash function, 134, 137–140
Computational Diffie-Hellman assumption, 278
Computational indistinguishability, 232–236, 350
Computational security, 47–54

Computing discrete logarithms, algorithms for, 305–313
  baby-step/giant-step, 306–309
  general number field sieve, 307
  index calculus, 306, 311–313
  Pohlig-Hellman, 279, 306, 309–310
Concrete security, 49, 160, 161
Confusion-diffusion paradigm, 163
Counter mode, 98–101
Cryptographic hash function
  as random oracle, 459, 467, 468
  collision resistance, *see* collision-resistant hash function
  security notions, 130

Data Encryption Standard, *see* DES
Data integrity, *see* message authentication
Decisional Diffie-Hellman assumption, **278–279**, 280–281, 328–329, 385
  key exchange based on, 328
  public-key encryption based on, 365
Definitions, importance of, 18–20
DES
  avalanche effect, 175
  cryptanalysis of, 176–179, 181, 187–188
  design, 173–175
  security, 179–181
  triple-DES, 184
Differential cryptanalysis, 181, 187
Diffie-Hellman key exchange, 324–330
  insecurity against man-in-the-middle attacks, 330
Digital Signature Algorithm (DSA), *see* DSS
Discrete logarithm assumption, **277**, 279, 507
  collision resistance from, 293
Discrete logarithm problem, *see* computing discrete logarithms, algorithms for
  elliptic curve groups and, 307
  one-way permutation from, 198
  preference for prime-order groups, **279**, 281, 290, 310, 515
Division with remainder, 246
Double encryption, 182
DSS, 445–446

El Gamal encryption, 363–369, 417
Electronic code book (ECB) mode, 96
Elliptic curves, 282–287, *see* discrete logarithm problem
Encryption, *see* private-key encryption, *see* public-key encryption
Encryption, definitions of, 20–22, *see* private-key encryption, *see* public-key encryption
Euclidean algorithm, 247, 260, 361, **502–504**, 505
Euler phi function, 255
Existential unforgeability, 116, 425, 432
Exponentiation, group, 252–254
  algorithm for, 505–507
Extended Euclidean algorithm, *see* Euclidean algorithm, **503**

Factoring, algorithms for, 297–305
  general number field sieve, 298, 307
  Pollard's $p-1$, 298–301
  Pollard's rho, 298, 301–303
  quadratic sieve, 298, 303–305, 313
  trial division, 261, 298
Factoring, hardness of, 261–262, **271**
  one-way function from, 197, 288
  one-way permutation from, 402
  public-key encryption based on, 385
  relation between RSA and, 273, 397, 407
  trapdoor permutation from, 402
Feistel network, 170–173, 225
  mangler function in, 172
  round function in, 171
Frequency analysis, 12, 36
Full domain hash (FDH), 481–485

Goldreich-Levin theorem, 202
Goldwasser-Micali encryption, 394–397
Group, 250
  $\mathbb{Z}^*_{N^2}$, 409
  $\mathbb{Z}_N$, 251, 254, 504, 510
  $\mathbb{Z}^*_N$, 254, 504, 511
  cyclic, 274
  elliptic curve, 282–287

Hard-core predicate, 198–200, 202–213
definition, 199
Goldreich-Levin, 202
Hash function, *see* collision-resistant hash function
Hash-and-Mac, 140, 432
Hash-and-sign, 429–432
Historical ciphers, 9–18
Caesar's cipher, 10
shift cipher, 10, 13
substitution cipher, 11
Vigenère cipher, 14, 15
HMAC, 141–143
Homomorphic public-key encryption, 416
Hybrid argument, 218, 220, 223, 344
Hybrid encryption, 346–355
efficiency of, 348

Index of coincidence, 16
Indistinguishability of encryptions, 61, 63, 338
perfect, 32, 33
Indistinguishability, computational, *see* computational indistinguishability
Isomorphism, group, **256**, 258–259, 277

Jacobi symbol, 387–388, 390–392
computation of, 393

Kasiski's method, 15
Kerberos, 320
Kerckhoffs' principle, 6, 48, 165
Key distribution center (KDC), 317–320
Kerberos, 320
Needham-Schroeder, 319
Key-exchange protocol, 323
Diffie-Hellman, 324
Known-plaintext attack, 8, 17
on block cipher, 161, 176, 181, 188

Lamport one-time signature scheme, 432–435
Legendre symbol, 387
Linear cryptanalysis, 181, 188
Logarithm, discrete, *see* discrete logarithm problem

Mangler function
and DES, 174
definition of, 172
MD5, *see* collision-resistant hash function
Merkle-Damgård transform, *see* collision-resistant hash function, **133–136**, 137, 138, 468
Message authentication, 111–112
combined with encryption, 148–154
unsuitability of encryption for, 102, 112–113
vs. digital signatures, 422
Message authentication code
CBC-MAC, 125–127
definition of security for, 115–118
fixed-length vs. variable-length messages, 120–124, 126
HMAC, 141–143
NMAC, 138–141
replay attacks, 116–118
syntax, 114
unique tags, 144, 148, 149, 156
Message integrity, *see* message authentication
Miller-Rabin algorithm, 264, **265–271**
Modern cryptography, principles of, 18–27
Modes of operation, *see* private-key encryption, 96–102
CBC mode, 97, 113, 125, 126
CTR mode, 98–101
ECB mode, 96, 113
OFB mode, 98, 113

Negligible probability, 51, 56–57
NMAC, 138–141
Non-repudiation, 323
$\mathcal{NP}$, *see* $\mathcal{P}$ vs. $\mathcal{NP}$

OAEP, 479–481, 486
One-time pad, **34–36**, 74, 90, 113
One-time signature, 432–435
constructing signatures from, 437–445
definition of security for, 432
One-way function, 194–198, 243, **287–289**
candidates, 197
definition, 195

families, 196
necessary for cryptography, 232
random oracle as, 462
sufficient for one-time signatures, 432, 435
sufficient for private-key cryptography, 228
sufficient for signatures, 445
One-way permutation, 196, **289–290**
based on discrete logarithm assumption, 198
based on factoring, 405
used to construct pseudorandom generator, 201
Output feedback (OFB) mode, 98

$\mathcal{P}$ vs. $\mathcal{NP}$, 48, 58, 198
Paillier encryption, 411–417
Perfect secrecy
definitions of, 30–34
impossibility in the public-key setting, 339
in comparison to computational security, 48, 49, 61
limitations of, 36, 47–48
one-time pad, 34
Shannon's theorem, 37
Vernam's cipher, 34
Perfectly-secure message authentication, 40
PGP, 450, 451
$\phi(N)$, *see* Euler phi function
PKCS #1 v1.5, 363
Pohlig-Hellman algorithm, *see* computing discrete logarithms, algorithms for
Pollard's $p-1$, *see* factoring, algorithms for
Pollard's rho, *see* factoring, algorithms for
Polynomial-time computation, 50, 54, 244
Primes, 246
distribution of, 263
generation of, **264**, 262–265
strong, 265, 282, 300, 515
testing of, *see* Miller-Rabin algorithm
Private-key cryptography
summary of, 244
Private-key encryption
arbitrary-length messages and, 62, 85, 94, 96
attack scenarios, 8
CCA-security, 103–105, 144–148, 154, 474
combined with message authentication, 148–154
CPA-security, 82, 89–94
definition of security for, 63, 64, 68, 78, 82, 103
hiding message length in, 62
indistinguishability in the presence of an eavesdropper, 350
limitations of, 315–317
modes of operation, 96–102
multiple message security, 78–81, 84
semantic security, 61, 64–69
setting, 4
syntax, 5, 29, 60
vs. message authentication, 102, 112–113
vs. public-key encryption, 334
Probabilistic algorithms, 54–56
Probabilistic encryption, 79, 340
Proofs by reduction, 58–60, 75
Proofs, importance of, 26
Pseudorandom function, **86–89**, 201, 221–225
construction, 222
construction in the random oracle model, 463
definition, 87
use for message authentication, 118–120
use in constructing signatures, 444
use in private-key encryption, 90
Pseudorandom generator, **69–72**, 213–221, 233
Blum-Micali, 220
construction, 201, 214
definition, 70
increasing expansion factor, 201, 215
use in private-key encryption, 73
variable output-length, 76

Pseudorandom permutation, **94–95**, 201, 243
  block cipher as, 159–161
  construction, 225
  definition, 95
  vs. strong pseudorandom permutation, 95
Public keys, secure distribution of, 335
Public-key cryptography
  number-theoretic problems as basis for, 245
Public-key encryption
  arbitrary-length messages and, 346
  based on trapdoor permutations, 375
  CCA-security, 369–373, 457, 473
  CPA-security, 337, 469, 479
  definition of security for, 337–341
  deterministic encryption and, 340
  El Gamal, 363–369, 385, 417
  Goldwasser-Micali, 385, 394–397
  homomorphic, 416
  hybrid encryption, *see* hybrid encryption
  in the random oracle model, 469
  multiple message security, 340
  OAEP, 479–481, 486
  padded RSA, 362–363
  Paillier, 385, 411–417
  PKCS #1 v1.5, 363
  Rabin, 385, 406–408
  setting, 320, 333
  syntax, 336
  textbook RSA, 355–362, 407
  vs. private-key encryption, 334
Public-key infrastructure (PKI), 446–453

Quadratic residue
  modulo a composite, 303, **388–392**
  modulo a prime, 281, 283, **386–388**
Quadratic residuosity assumption, 392–394

Rabin encryption, 406–408
Random function, 86, 460–461
Random number generators, 55–56
Random oracle
  as collision-resistant hash function, 463
  as one-way function, 462
  programmability of, 465, 474, 483
  used to construct a pseudorandom function, 463
  used to construct a signature scheme, 429
  used to construct public-key encryption, 469
Random oracle model
  overview, 458–469
Replay attack, 116, **117–118**, 370, 425
Rijndael, *see* AES
RSA
  assumption, 271–274
  attacks on, 358
  FDH, 481–485
  OAEP, 479–481, 486
  problem, 272, 289, 290, 385
  public-key encryption, 355–358, 362–363, 457, 469–481
  signatures, 426–429, 481–485

S-box, 165, 167–168, 170, 174
Secret-key encryption, *see* private-key encryption
Secure message transmission, 150–152
  definition of security for, 151
Security parameter, 50–52, 60, 62
Semantic security, 64–69
SHA-1, *see* collision-resistant hash function
  as random oracle, 459, 461, 467, 468
Shanks' algorithm, *see* computing discrete logarithms, algorithms for
Shannon's theorem, 37–40
Shift cipher, 10
Signature scheme
  certificates, *see* certificates
  chain-based, 436
  definition of security for, 425, 432
  DSS, 445–446
  FDH, 481–485
  hashed RSA, 428–429
  in the random oracle model, 481–485
  Lamport scheme, 432–435

  one-time signature, 432–435
  overview of, 421
  properties of, 422
  stateful, 436
  syntax, 424
  textbook RSA, 426
  tree-based, 439–445
  vs. message authentication, 422
  vs. public-key encryption, 423
Square root
  modulo a composite, 401–404
  modulo a prime, 268, 397–401
Stream cipher, *see* pseudorandom generator, 220
  RC4, 77
  use for multiple encryptions, 80–81
  use in private-key encryption, 77, 350
  using block cipher as, 102
Strong primes, *see* primes
Strong pseudorandom permutation, 94–95, 154
  definition, 95
  vs. pseudorandom permutation, 95
Substitution cipher, 11
Substitution-permutation network, 162–170, 186
  attacks on, 168–170
Symmetric-key encryption, *see* private-key encryption

Trapdoor permutation, **373–375**, 402–406
  based on factoring, 406
  based on RSA assumption, 374
  public-key encryption scheme based on, 375
Triple encryption, 184
Triple-DES, 173, 184

Vernam's cipher, *see* one-time pad
Vigenère cipher, 14

$\mathbb{Z}_N$, **251**, 254, 504, 510
$\mathbb{Z}_N^*$, **254–261**, 504, 511
$\mathbb{Z}_{N^2}^*$, 409–411