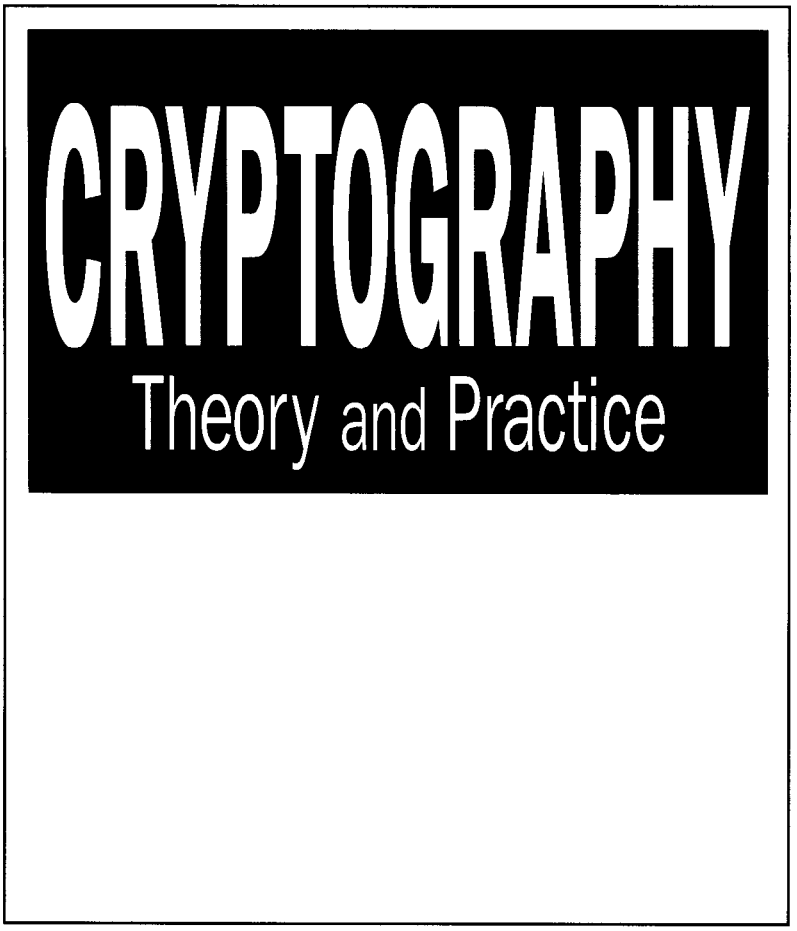
CRYPTOGRAPHY

Theory and Practice

Douglas R. Stinson


CRYPTOGRAPHY
Theory and Practice

The CRC Press Series on

DISCRETE MATHEMATICS and ITS APPLICATIONS

Series Editor

Kenneth H. Rosen, Ph.D.

AT&T Bell Laboratories

Forthcoming Handbooks

Handbook of Discrete Mathematics, *Kenneth H. Rosen*
Standard Reference of Discrete Mathematics, *Kenneth H. Rosen*
Handbook of Graph Theory, *Jonathan Gross*
Handbook of Combinatorial Designs, *Charles Colbourn and Jeffrey Dinitz*
Handbook of Cryptography, *Scott Vanstone, Paul Van Oorschot, and Alfred Menezes*
Handbook of Discrete and Computational Geometry, *Jacob E. Goodman and Joseph O'Rourke*

Forthcoming Textbooks and Monographs

Graph Theory with Computer Science Applications
Introduction to Network Reliability
Error-Correcting Codes and Algebraic Curves

CRYPTOGRAPHY

Theory and Practice

Douglas R. Stinson
Computer Science and Engineering Department
and Center for Communication and Information Science
University of Nebraska, Lincoln

CRC Press
Boca Raton New York London Tokyo

Library of Congress Cataloging-in-Publication Data

Stinson, D. R. (Douglas Robert), 1956– .
Cryptography : theory and practice / D.R. Stinson.
p. cm. -- (Discrete mathematics and its applications)
Includes bibliographical references and index.
ISBN 0-8493-8521-0
1. Coding theory. 2. Cryptography. I. Title. II. Series.
QA268.S75 1995
005.8'2--dc20 95-5237
CIP

International Standard Book Number 0-8493-8521-0
Library of Congress Card Number 95-5237
Printed in the United States of America 3 4 5 6 7 8 9 0
Printed on acid-free paper

The CRC Press Series on Discrete Mathematics and Its Applications

Discrete mathematics is becoming increasingly applied to computer science, engineering, the physical sciences, the natural sciences, and the social sciences. Moreover, there has also been an explosion of research in discrete mathematics in the past two decades. Both trends have produced a need for many types of information for people who use or study this part of the mathematical sciences. The CRC Press Series on Discrete Mathematics and Its Applications is designed to meet the needs of practitioners, students, and researchers for information in discrete mathematics. The series includes handbooks and other reference books, advanced textbooks, and selected monographs. Among the areas of discrete mathematics addressed by the series are logic, set theory, number theory, combinatorics, discrete probability theory, graph theory, algebra, linear algebra, coding theory, cryptology, discrete optimization, theoretical computer science, algorithmics, and computational geometry.

Kenneth H. Rosen, Series Editor
Distinguished Member of Technical Staff
AT&T Bell Laboratories
Holmdel, New Jersey
e-mail:krosen@arch4.ho.att.com

Advisory Board

Preface

My objective in writing this book was to produce a general, comprehensive textbook that treats all the essential core areas of cryptography. Although many books and monographs on cryptography have been written in recent years, the majority of them tend to address specialized areas of cryptography. On the other hand, many of the existing general textbooks have become out-of-date due to the rapid expansion of research in cryptography in the past 15 years.

I have taught a graduate level cryptography course at the University of Nebraska-Lincoln to computer science students, but I am aware that cryptography courses are offered at both the undergraduate and graduate levels in mathematics, computer science and electrical engineering departments. Thus, I tried to design the book to be flexible enough to be useful in a wide variety of approaches to the subject.

Of course there are difficulties in trying to appeal to such a wide audience. But basically, I tried to do things in moderation. I have provided a reasonable amount of mathematical background where it is needed. I have attempted to give informal descriptions of the various cryptosystems, along with more precise pseudo-code descriptions, since I feel that the two approaches reinforce each other. As well, there are many examples to illustrate the workings of the algorithms. And in every case I try to explain the mathematical underpinnings; I believe that it is impossible to really understand how a cryptosystem works without understanding the underlying mathematical theory.

The book is organized into three parts. The first part, Chapters 1–3, covers private-key cryptography. Chapters 4–9 concern the main topics in public-key cryptography. The remaining four chapters provide introductions to four active research areas in cryptography.

The first part consists of the following material: Chapter 1 is a fairly elementary introduction to simple "classical" cryptosystems. Chapter 2 covers the main elements of Shannon's approach to cryptography, including the concept of perfect secrecy and the use of information theory in cryptography. Chapter 3 is a lengthy discussion of the **Data Encryption Standard**; it includes a treatment of differential cryptanalysis.

The second part contains the following material: Chapter 4 concerns the **RSA Public-key Cryptosystem**, together with a considerable amount of number-

theoretic background on primality testing and factoring. Chapter 5 discusses some other public-key systems, the most important being the **ElGamal System** based on discrete logarithms. Chapter 6 deals with signature schemes, such as the **Digital Signature Standard**, and includes treatment of special types of signature schemes such as undeniable and fail-stop signature schemes. The subject of Chapter 7 is hash functions. Chapter 8 provides an overview of the numerous approaches to key distribution and key agreement protocols. Finally, Chapter 9 describes identification schemes.

The third part contains chapters on selected research-oriented topics, namely, authentication codes, secret sharing schemes, pseudo-random number generation, and zero-knowledge proofs.

Thus, I have attempted to be quite comprehensive in the "core" areas of cryptography, as well as to provide some more advanced chapters on specific research areas. Within any given area, however, I try to pick a few representative systems and discuss them in a reasonable amount of depth. Thus my coverage of cryptography is in no way encyclopedic.

Certainly there is much more material in this book than can be covered in one (or even two) semesters. But I hope that it should be possible to base several different types of courses on this book. An introductory course could cover Chapter 1, together with selected sections of Chapters 2–5. A second or graduate course could cover these chapters in a more complete fashion, as well as material from Chapters 6–9. Further, I think that any of the chapters would be a suitable basis for a "topics" course that might delve into specific areas more deeply.

But aside from its primary purpose as a textbook, I hope that researchers and practitioners in cryptography will find it useful in providing an introduction to specific areas with which they might not be familiar. With this in mind, I have tried to provide references to the literature for further reading on many of the topics discussed.

One of the most difficult things about writing this book was deciding how much mathematical background to include. Cryptography is a broad subject, and it requires knowledge of several areas of mathematics, including number theory, groups, rings and fields, linear algebra, probability and information theory. As well, some familiarity with computational complexity, algorithms and NP-completeness theory is useful. I have tried not to assume too much mathematical background, and thus I develop mathematical tools as they are needed, for the most part. But it would certainly be helpful for the reader to have some familiarity with basic linear algebra and modular arithmetic. On the other hand, a more specialized topic, such as the concept of entropy from information theory, is introduced from scratch.

I should also apologize to anyone who does not agree with the phrase "Theory and Practice" in the title. I admit that the book is more theory than practice. What I mean by this phrase is that I have tried to select the material to be included in the book both on the basis of theoretical interest and practical importance. So, I may include systems that are not of practical use if they are mathematically elegant or

illustrate an important concept or technique. But, on the other hand, I do describe the most important systems that are used in practice, e.g., **DES** and other U. S. cryptographic standards.

I would like to thank the many people who provided encouragement while I wrote this book, pointed out typos and errors, and gave me useful suggestions on material to include and how various topics should be treated. In particular, I would like to convey my thanks to Mustafa Atici, Mihir Bellare, Bob Blakley, Carlo Blundo, Gilles Brassard, Daniel Ducharme, Mike Dvorsky, Luiz Frota-Mattos, David Klarner, Don Kreher, Keith Martin, Vaclav Matyas, Alfred Menezes, Luke O'Connor, William Read, Phil Rogaway, Paul Van Oorschot, Scott Vanstone, Johan van Tilburg, Marc Vauclair and Mike Wiener. Thanks also to Mike Dvorsky for helping me prepare the index.

Douglas R. Stinson

To my children,
Michela and Aiden

Contents

1 Classical Cryptography **1**
1.1 Introduction: Some Simple Cryptosystems 1
1.1.1 The Shift Cipher 3
1.1.2 The Substitution Cipher 7
1.1.3 The Affine Cipher 8
1.1.4 The Vigenère Cipher 12
1.1.5 The Hill Cipher 14
1.1.6 The Permutation Cipher 18
1.1.7 Stream Ciphers 20
1.2 Cryptanalysis 25
1.2.1 Cryptanalysis of the Affine Cipher 26
1.2.2 Cryptanalysis of the Substitution Cipher 28
1.2.3 Cryptanalysis of the Vigenère Cipher 31
1.2.4 A Known Plaintext Attack on the Hill Cipher 37
1.2.5 Cryptanalysis of the LFSR-based Stream Cipher 37
1.3 Notes 39
Exercises 40

2 Shannon's Theory **44**
2.1 Perfect Secrecy 44
2.2 Entropy 51
2.2.1 Huffman Encodings and Entropy 53
2.3 Properties of Entropy 56
2.4 Spurious Keys and Unicity Distance 59
2.5 Product Cryptosystems 64
2.6 Notes 67
Exercises 67

3 The Data Encryption Standard **70**
3.1 Introduction . . . 70
3.2 Description of DES . . . 70
3.2.1 An Example of DES Encryption . . . 79
3.3 The DES Controversy . . . 82
3.4 DES in Practice . . . 83
3.4.1 DES Modes of Operation . . . 83
3.5 A Time-memory Trade-off . . . 86
3.6 Differential Cryptanalysis . . . 89
3.6.1 An Attack on a 3-round DES . . . 93
3.6.2 An Attack on a 6-round DES . . . 98
3.6.3 Other examples of Differential Cryptanalysis . . . 104
3.7 Notes and References . . . 110
Exercises . . . 110

4 The RSA System and Factoring **114**
4.1 Introduction to Public-key Cryptography . . . 114
4.2 More Number Theory . . . 116
4.2.1 The Euclidean Algorithm . . . 116
4.2.2 The Chinese Remainder Theorem . . . 119
4.2.3 Other Useful Facts . . . 122
4.3 The RSA Cryptosystem . . . 124
4.4 Implementing RSA . . . 125
4.5 Probabilistic Primality Testing . . . 129
4.6 Attacks On RSA . . . 138
4.6.1 The Decryption Exponent . . . 139
4.6.2 Partial Information Concerning Plaintext Bits . . . 144
4.7 The Rabin Cryptosystem . . . 145
4.8 Factoring Algorithms . . . 150
4.8.1 The $p-1$ Method . . . 151
4.8.2 Dixon's Algorithm and the Quadratic Sieve . . . 153
4.8.3 Factoring Algorithms in Practice . . . 155
4.9 Notes and References . . . 156
Exercises . . . 157

5 Other Public-key Cryptosystems **162**
5.1 The ElGamal Cryptosystem and Discrete Logs . . . 162
5.1.1 Algorithms for the Discrete Log Problem . . . 164
5.1.2 Bit Security of Discrete Logs . . . 173
5.2 Finite Field and Elliptic Curve Systems . . . 177
5.2.1 Galois Fields . . . 180
5.2.2 Elliptic Curves . . . 184
5.3 The Merkle-Hellman Knapsack System . . . 191
5.4 The McEliece System . . . 194

5.5 Notes and References . . . 199
Exercises . . . 200

6 Signature Schemes **203**
6.1 Introduction . . . 203
6.2 The ElGamal Signature Scheme . . . 206
6.3 The Digital Signature Standard . . . 210
6.4 One-time Signatures . . . 214
6.5 Undeniable Signatures . . . 218
6.6 Fail-stop Signatures . . . 225
6.7 Notes and References . . . 230
Exercises . . . 231

7 Hash Functions **233**
7.1 Signatures and Hash Functions . . . 233
7.2 Collision-free Hash Functions . . . 234
7.3 The Birthday Attack . . . 237
7.4 A Discrete Log Hash Function . . . 239
7.5 Extending Hash Functions . . . 242
7.6 Hash Functions From Cryptosystems . . . 247
7.7 The MD4 Hash Function . . . 248
7.8 Timestamping . . . 254
7.9 Notes and References . . . 256
Exercises . . . 256

8 Key Distribution and Key Agreement **259**
8.1 Introduction . . . 259
8.2 Key Predistribution . . . 261
8.2.1 Blom's Scheme . . . 261
8.2.2 Diffie-Hellman Key Predistribution . . . 264
8.3 Kerboros . . . 268
8.4 Diffie-Hellman Key Exchange . . . 271
8.4.1 The Station-to-station Protocol . . . 272
8.4.2 MTI Key Agreement Protocols . . . 274
8.4.3 Key Agreement Using Self-certifying Keys . . . 277
8.5 Notes and References . . . 281
Exercises . . . 281

9 Identification Schemes **283**
9.1 Introduction . . . 283
9.2 The Schnorr Identification Scheme . . . 285
9.3 The Okamoto Identification Scheme . . . 291
9.4 The Guillou-Quisquater Identification Scheme . . . 296
9.4.1 Identity-based Identification Schemes . . . 300

9.5 Converting Identification to Signature Schemes 302
9.6 Notes and References 302
Exercises 303

10 Authentication Codes **305**
10.1 Introduction 305
10.2 Computing Deception Probabilities 307
10.3 Combinatorial Bounds 312
10.3.1 Orthogonal Arrays 315
10.3.2 Constructions and Bounds for OAs 316
10.3.3 Characterizations of Authentication Codes 320
10.4 Entropy Bounds 322
10.5 Notes and References 324
Exercises 325

11 Secret Sharing Schemes **327**
11.1 Introduction: The Shamir Threshold Scheme 327
11.2 Access Structures and General Secret Sharing 333
11.3 The Monotone Circuit Construction 334
11.4 Formal Definitions 339
11.5 Information Rate 343
11.6 The Brickell Vector Space Construction 345
11.7 An Upper Bound on the Information Rate 350
11.8 The Decomposition Construction 355
11.9 Notes and References 359
Exercises 359

12 Pseudo-random Number Generation **361**
12.1 Introduction and Examples 361
12.2 Indistinguishable Probability Distributions 365
12.2.1 Next Bit Predictors 367
12.3 The Blum-Blum-Shub Generator 372
12.3.1 Security of the BBS Generator 375
12.4 Probabilistic Encryption 380
12.5 Notes and References 384
Exercises 385

13 Zero-knowledge Proofs **387**
13.1 Interactive Proof Systems 387
13.2 Perfect Zero-knowledge Proofs 390
13.3 Bit Commitments 400
13.4 Computational Zero-knowledge Proofs 402
13.5 Zero-knowledge Arguments 407
13.6 Notes and References 409

Exercises 410

Further Reading **412**

Bibliography **413**

Index **428**