

TEXTBOOKS IN MATHEMATICS

Cryptography

Theory and Practice

FOURTH EDITION



Douglas R. Stinson
Maura B. Paterson



CRC Press
Taylor & Francis Group

A CHAPMAN & HALL BOOK

Cryptography

Theory and Practice

Fourth Edition

Textbooks in Mathematics

Series editors:

Al Boggess and Ken Rosen

MATHEMATICAL MODELING FOR BUSINESS ANALYTICS

William P. Fox

ELEMENTARY LINEAR ALGEBRA

James R. Kirkwood and Bessie H. Kirkwood

APPLIED FUNCTIONAL ANALYSIS, THIRD EDITION

J. Tinsley Oden and Leszek Demkowicz

AN INTRODUCTION TO NUMBER THEORY WITH CRYPTOGRAPHY, SECOND EDITION

James R. Kraft and Lawrence Washington

MATHEMATICAL MODELING: BRANCHING BEYOND CALCULUS

Crista Arangala, Nicolas S. Luke and Karen A. Yokley

ELEMENTARY DIFFERENTIAL EQUATIONS, SECOND EDITION

Charles Roberts

ELEMENTARY INTRODUCTION TO THE LEBESGUE INTEGRAL

Steven G. Krantz

LINEAR METHODS FOR THE LIBERAL ARTS

David Hecker and Stephen Andrilli

CRYPTOGRAPHY: THEORY AND PRACTICE, FOURTH EDITION

Douglas R. Stinson and Maura B. Paterson

DISCRETE MATHEMATICS WITH DUCKS, SECOND EDITION

Sarah-Marie Belcastro

BUSINESS PROCESS MODELING, SIMULATION AND DESIGN, THIRD EDITION

Manual Laguna and Johan Marklund

GRAPH THEORY AND ITS APPLICATIONS, THIRD EDITION

Jonathan L. Gross, Jay Yellen and Mark Anderson

Cryptography

Theory and Practice

Fourth Edition

Douglas R. Stinson
Maura B. Paterson



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2019 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed on acid-free paper
Version Date: 20180724

International Standard Book Number-13: 978-1-1381-9701-5 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Names: Stinson, Douglas R. (Douglas Robert), 1956- author. | Paterson, Maura B., author.
Title: Cryptography : theory and practice / Douglas R. Stinson and Maura B. Paterson.
Description: Fourth edition. | Boca Raton : CRC Press, Taylor & Francis Group, 2018.
Identifiers: LCCN 2018018724 | ISBN 9781138197015
Subjects: LCSH: Coding theory. | Cryptography.
Classification: LCC QA268 .S75 2018 | DDC 005.8/2--dc23
LC record available at <https://lccn.loc.gov/2018018724>

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

To my children, Michela and Aiden

DRS

To my father, Hamish

MBP



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contents

Preface	xv
1 Introduction to Cryptography	1
1.1 Cryptosystems and Basic Cryptographic Tools	1
1.1.1 Secret-key Cryptosystems	1
1.1.2 Public-key Cryptosystems	2
1.1.3 Block and Stream Ciphers	3
1.1.4 Hybrid Cryptography	3
1.2 Message Integrity	4
1.2.1 Message Authentication Codes	6
1.2.2 Signature Schemes	6
1.2.3 Nonrepudiation	7
1.2.4 Certificates	8
1.2.5 Hash Functions	8
1.3 Cryptographic Protocols	9
1.4 Security	10
1.5 Notes and References	13
2 Classical Cryptography	15
2.1 Introduction: Some Simple Cryptosystems	15
2.1.1 The Shift Cipher	17
2.1.2 The Substitution Cipher	20
2.1.3 The Affine Cipher	22
2.1.4 The Vigenère Cipher	26
2.1.5 The Hill Cipher	27
2.1.6 The Permutation Cipher	32
2.1.7 Stream Ciphers	34
2.2 Cryptanalysis	38
2.2.1 Cryptanalysis of the Affine Cipher	40
2.2.2 Cryptanalysis of the Substitution Cipher	42
2.2.3 Cryptanalysis of the Vigenère Cipher	45
2.2.4 Cryptanalysis of the Hill Cipher	48
2.2.5 Cryptanalysis of the LFSR Stream Cipher	49
2.3 Notes and References	51
Exercises	51

3	Shannon's Theory, Perfect Secrecy, and the One-Time Pad	61
3.1	Introduction	61
3.2	Elementary Probability Theory	62
3.3	Perfect Secrecy	64
3.4	Entropy	70
3.4.1	Properties of Entropy	72
3.5	Spurious Keys and Unicity Distance	75
3.6	Notes and References	79
	Exercises	80
4	Block Ciphers and Stream Ciphers	83
4.1	Introduction	83
4.2	Substitution-Permutation Networks	84
4.3	Linear Cryptanalysis	89
4.3.1	The Piling-up Lemma	89
4.3.2	Linear Approximations of S-boxes	91
4.3.3	A Linear Attack on an SPN	94
4.4	Differential Cryptanalysis	98
4.5	The Data Encryption Standard	105
4.5.1	Description of DES	105
4.5.2	Analysis of DES	107
4.6	The Advanced Encryption Standard	109
4.6.1	Description of AES	110
4.6.2	Analysis of AES	115
4.7	Modes of Operation	116
4.7.1	Padding Oracle Attack on CBC Mode	120
4.8	Stream Ciphers	122
4.8.1	Correlation Attack on a Combination Generator	123
4.8.2	Algebraic Attack on a Filter Generator	127
4.8.3	Trivium	130
4.9	Notes and References	131
	Exercises	131
5	Hash Functions and Message Authentication	137
5.1	Hash Functions and Data Integrity	137
5.2	Security of Hash Functions	139
5.2.1	The Random Oracle Model	140
5.2.2	Algorithms in the Random Oracle Model	142
5.2.3	Comparison of Security Criteria	146
5.3	Iterated Hash Functions	148
5.3.1	The Merkle-Damgård Construction	151
5.3.2	Some Examples of Iterated Hash Functions	156
5.4	The Sponge Construction	157
5.4.1	SHA-3	160
5.5	Message Authentication Codes	161

5.5.1	Nested MACs and HMAC	163
5.5.2	CBC-MAC	166
5.5.3	Authenticated Encryption	167
5.6	Unconditionally Secure MACs	170
5.6.1	Strongly Universal Hash Families	173
5.6.2	Optimality of Deception Probabilities	175
5.7	Notes and References	177
	Exercises	178
6	The RSA Cryptosystem and Factoring Integers	185
6.1	Introduction to Public-key Cryptography	185
6.2	More Number Theory	188
6.2.1	The Euclidean Algorithm	188
6.2.2	The Chinese Remainder Theorem	191
6.2.3	Other Useful Facts	194
6.3	The RSA Cryptosystem	196
6.3.1	Implementing RSA	198
6.4	Primality Testing	200
6.4.1	Legendre and Jacobi Symbols	202
6.4.2	The Solovay-Strassen Algorithm	205
6.4.3	The Miller-Rabin Algorithm	208
6.5	Square Roots Modulo n	210
6.6	Factoring Algorithms	211
6.6.1	The Pollard $p - 1$ Algorithm	212
6.6.2	The Pollard Rho Algorithm	213
6.6.3	Dixon's Random Squares Algorithm	216
6.6.4	Factoring Algorithms in Practice	221
6.7	Other Attacks on RSA	223
6.7.1	Computing $\phi(n)$	223
6.7.2	The Decryption Exponent	223
6.7.3	Wiener's Low Decryption Exponent Attack	228
6.8	The Rabin Cryptosystem	232
6.8.1	Security of the Rabin Cryptosystem	234
6.9	Semantic Security of RSA	236
6.9.1	Partial Information Concerning Plaintext Bits	237
6.9.2	Obtaining Semantic Security	239
6.10	Notes and References	245
	Exercises	246
7	Public-Key Cryptography and Discrete Logarithms	255
7.1	Introduction	255
7.1.1	The ElGamal Cryptosystem	256
7.2	Algorithms for the Discrete Logarithm Problem	258
7.2.1	Shanks' Algorithm	258
7.2.2	The Pollard Rho Discrete Logarithm Algorithm	260