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

Printed on acid-free paper
Version Date: 20180724

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

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