

Johannes A. Buchmann

INTRODUCTION TO CRYPTOGRAPHY

Second Edition

RSA-576

=

39807508642406493739712550055
03864911990643623425267084063
85189575946388957261768583317

×

47277214610743530253622307197
30482246329146953020971164598
52171130520711256363590397527



Springer

Undergraduate Texts in Mathematics

Editors

S. Axler
F.W. Gehring
K.A. Ribet

BIBLIOTHEQUE DU CERIST

Springer

New York
Berlin
Heidelberg
Hong Kong
London
Milan
Paris
Tokyo

Undergraduate Texts in Mathematics

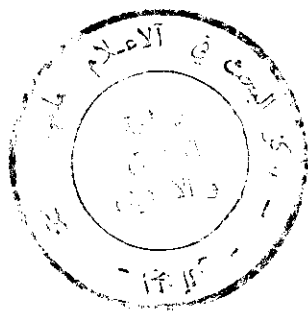
- Abbott:** Understanding Analysis.
- Anglin:** Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
- Anglin/Lambek:** The Heritage of Thales.
Readings in Mathematics.
- Apostol:** Introduction to Analytic Number Theory. Second edition.
- Armstrong:** Basic Topology.
- Armstrong:** Groups and Symmetry.
- Axler:** Linear Algebra Done Right. Second edition.
- Beardon:** Limits: A New Approach to Real Analysis.
- Bak/Newman:** Complex Analysis. Second edition.
- Banchoff/Wermer:** Linear Algebra Through Geometry. Second edition.
- Berberian:** A First Course in Real Analysis.
- Bix:** Conics and Cubics: A Concrete Introduction to Algebraic Curves.
- Brémaud:** An Introduction to Probabilistic Modeling.
- Bressoud:** Factorization and Primality Testing.
- Bressoud:** Second Year Calculus.
Readings in Mathematics.
- Brickman:** Mathematical Introduction to Linear Programming and Game Theory.
- Browder:** Mathematical Analysis: An Introduction.
- Buchmann:** Introduction to Cryptography. Second edition.
- Buskes/van Rooij:** Topological Spaces: From Distance to Neighborhood.
- Callahan:** The Geometry of Spacetime: An Introduction to Special and General Relativity.
- Carter/van Brunt:** The Lebesgue–Stieltjes Integral: A Practical Introduction.
- Cederberg:** A Course in Modern Geometries. Second edition.
- Childs:** A Concrete Introduction to Higher Algebra. Second edition.
- Chung/AitSahlia:** Elementary Probability Theory: With Stochastic Processes and an Introduction to Mathematical Finance. Fourth edition.
- Cox/Little/O'Shea:** Ideals, Varieties, and Algorithms. Second edition.
- Croom:** Basic Concepts of Algebraic Topology.
- Curtis:** Linear Algebra: An Introductory Approach. Fourth edition.
- Daep/Gorkin:** Reading, Writing, and Proving: A Closer Look at Mathematics.
- Devlin:** The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
- Dixmier:** General Topology.
- Driver:** Why Math?
- Ebbinghaus/Flum/Thomas:** Mathematical Logic. Second edition.
- Edgar:** Measure, Topology, and Fractal Geometry.
- Elaydi:** An Introduction to Difference Equations. Second edition.
- Erdős/Surányi:** Topics in the Theory of Numbers.
- Estep:** Practical Analysis in One Variable.
- Exner:** An Accompaniment to Higher Mathematics.
- Exner:** Inside Calculus.
- Fine/Rosenberger:** The Fundamental Theory of Algebra.
- Fischer:** Intermediate Real Analysis.
- Flanigan/Kazdan:** Calculus Two: Linear and Nonlinear Functions. Second edition.
- Fleming:** Functions of Several Variables. Second edition.
- Foulds:** Combinatorial Optimization for Undergraduates.
- Foulds:** Optimization Techniques: An Introduction.

(continued after index)

Johannes Buchmann

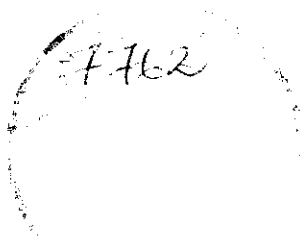
Introduction to Cryptography

Second Edition



Springer

Johannes A. Buchmann
 Department of Computer Science
 Technical University, Darmstadt
 Hochschulstr. 10
 64289 Darmstadt
 Germany



Editorial Board

S. Axler
 Mathematics Department
 San Francisco State
 University
 San Francisco, CA 94132
 USA
 axler@sfsu.edu

F.W. Gehring
 Mathematics Department
 East Hall
 University of Michigan
 Ann Arbor, MI 48109
 USA
 gehring@math.lsa.umich.edu

K.A. Ribet
 Mathematics Department
 University of California
 Berkeley
 Berkeley, CA 94720-3840
 USA
 ribet@math.berkeley.edu

Cover: The factorization of RSA-576, a 576-bit or 174-digit prime number, was the goal of an open challenge sponsored by RSA Laboratories (Bedford, Mass.). RSA-576 was factored by a team of researchers in Germany and other countries in December, 2003.

Mathematics Subject Classification (2000): 94-01, 94A60, 11T71

Library of Congress Cataloging in Publication Data
 Buchmann, Johannes.

Introduction to cryptography / Johannes Buchmann. – [2nd ed.].

p. cm. – (Undergraduate texts in mathematics)

Includes bibliographical references and index.

ISBN 0-387-21156-X (hard cover: alk. paper) – ISBN 0-387-20756-2 (soft cover: alk. paper)

1. Coding theory. 2. Cryptography. I. Title. II Series.

QA268.B83 2004

003'.54—dc22

2004041657

ISBN 0-387-21156-X

Printed on acid-free paper.

German edition: Einführung in die Kryptographie © Springer-Verlag, Heidelberg, 1999. ©2004, 2001 Springer-Verlag NY, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, LLC, 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America

(BP/EB)

9 8 6 5 4 3 2 1 SPIN 10991503 (hard cover) – SPIN 10963999 (soft cover)

Springer-Verlag is a part of *Springer Science + Business Media*

springeronline.com

For Almut, Daniel, and Jan

BIBLIOTHEQUE DU CERIST

Contents



Preface for the Second Edition	xiii
Preface	xv
1 Integers	1
1.1 Basics	1
1.2 Divisibility	3
1.3 Representation of Integers	4
1.4 O- and Ω -Notation	6
1.5 Cost of Addition, Multiplication, and Division with Remainder	7
1.6 Polynomial Time	9
1.7 Greatest Common Divisor	9
1.8 Euclidean Algorithm	12
1.9 Extended Euclidean Algorithm	16
1.10 Analysis of the Extended Euclidean Algorithm	18
1.11 Factoring into Primes	22
1.12 Exercises	24
2 Congruences and Residue Class Rings	29
2.1 Congruences	29

2.2	Semigroups	32
2.3	Groups	34
2.4	Residue Class Ring	35
2.5	Fields	36
2.6	Division in the Residue Class Ring	36
2.7	Analysis of the Operations in the Residue Class Ring	38
2.8	Multiplicative Group of Residues mod m	39
2.9	Order of Group Elements	41
2.10	Subgroups	42
2.11	Fermat's Little Theorem	44
2.12	Fast Exponentiation	45
2.13	Fast Evaluation of Power Products	48
2.14	Computation of Element Orders	49
2.15	The Chinese Remainder Theorem	51
2.16	Decomposition of the Residue Class Ring	53
2.17	A Formula for the Euler φ -Function	55
2.18	Polynomials	56
2.19	Polynomials over Fields	58
2.20	Construction of Finite Fields	61
2.21	The Structure of the Unit Group of Finite Fields	65
2.22	Structure of the Multiplicative Group of Residues Modulo a Prime Number	66
2.23	Exercises	67
3	Encryption	71
3.1	Encryption Schemes	71
3.2	Symmetric and Asymmetric Cryptosystems	73
3.3	Cryptanalysis	74
3.4	Alphabets and Words	77
3.5	Permutations	80
3.6	Block Ciphers	81
3.7	Multiple Encryption	82
3.8	The Use of Block Ciphers	83
3.9	Stream Ciphers	93
3.10	The Affine Cipher	95
3.11	Matrices and Linear Maps	97
3.12	Affine Linear Block Ciphers	102
3.13	Vigenère, Hill, and Permutation Ciphers	103

3.14	Cryptanalysis of Affine Linear Block Ciphers	104
3.15	Secure Cryptosystems	105
3.16	Exercises	111
4	Probability and Perfect Secrecy	115
4.1	Probability	115
4.2	Conditional Probability	117
4.3	Birthday Paradox	118
4.4	Perfect Secrecy	119
4.5	Vernam One-Time Pad	123
4.6	Random Numbers	124
4.7	Pseudorandom Numbers	124
4.8	Exercises	125
5	DES	127
5.1	Feistel Ciphers	127
5.2	DES Algorithm	128
5.3	An Example	134
5.4	Security of DES	136
5.5	Exercises	137
6	AES	139
6.1	Notation	139
6.2	Cipher	140
6.3	KeyExpansion	145
6.4	An Example	146
6.5	InvCipher	148
6.6	Exercises	148
7	Prime Number Generation	151
7.1	Trial Division	151
7.2	Fermat Test	153
7.3	Carmichael Numbers	154
7.4	Miller-Rabin Test	156
7.5	Random Primes	159
7.6	Exercises	160

8	Public-Key Encryption	163
8.1	Idea	163
8.2	Security	165
8.3	RSA Cryptosystem	167
8.4	Rabin Encryption	181
8.5	Diffie-Hellman Key Exchange	186
8.6	ElGamal Encryption	191
8.7	Exercises	196
9	Factoring	199
9.1	Trial Division	199
9.2	$p - 1$ Method	200
9.3	Quadratic sieve	201
9.4	Analysis of the Quadratic Sieve	206
9.5	Efficiency of Other Factoring Algorithms	210
9.6	Exercises	211
10	Discrete Logarithms	213
10.1	The DL Problem	213
10.2	Enumeration	214
10.3	Shanks Baby-Step Giant-Step Algorithm	214
10.4	The Pollard ρ -Algorithm	217
10.5	The Pohlig-Hellman Algorithm	221
10.6	Index Calculus	226
10.7	Other Algorithms	230
10.8	Generalization of the Index Calculus Algorithm	231
10.9	Exercises	232
11	Cryptographic Hash Functions	235
11.1	Hash Functions and Compression Functions	235
11.2	Birthday Attack	238
11.3	Compression Functions from Encryption Functions	239
11.4	Hash Functions from Compression Functions	239
11.5	SHA-1	242
11.6	Other Hash Functions	244
11.7	An Arithmetic Compression Function	245
11.8	Message Authentication Codes	247
11.9	Exercises	248

12 Digital Signatures	249
12.1 Idea	249
12.2 Security	250
12.3 RSA Signatures	251
12.4 Signatures from Public-Key Systems	257
12.5 ElGamal Signature	257
12.6 The Digital Signature Algorithm (DSA)	263
12.7 Undeniable Signatures	266
12.8 Blind Signatures	271
12.9 Exercises	274
13 Other Systems	277
13.1 Finite Fields	278
13.2 Elliptic Curves	278
13.3 Quadratic Forms	282
13.4 Exercises	283
14 Identification	285
14.1 Passwords	286
14.2 One-Time Passwords	287
14.3 Challenge-Response Identification	287
14.4 Exercises	292
15 Secret Sharing	293
15.1 The Principle	293
15.2 The Shamir Secret Sharing Protocol	294
15.3 Exercises	297
16 Public-Key Infrastructures	299
16.1 Personal Security Environments	299
16.2 Certification Authorities	301
16.3 Certificate Chains	306
Solutions of the exercises	307
References	325
Index	331