

Algorithms and Computation in Mathematics • Volume 3

Editors

Manuel Bronstein Arjeh M. Cohen

Henri Cohen David Eisenbud

Bernd Sturmfels

Springer-Verlag Berlin Heidelberg GmbH

Neal Koblitz

Algebraic Aspects of Cryptography

With an Appendix on
Hyperelliptic Curves by
Alfred J. Menezes,
Yi-Hong Wu, and
Robert J. Zuccherato

With 7 Figures



Springer

Neal Koblitz
Department of Mathematics
University of Washington
Seattle, WA 98195, USA
e-mail:
koblitz@math.washington.edu

Yi-Hong Wu
Department of Discrete and
Statistical Sciences
Auburn University
Auburn, AL 36849, USA

Alfred J. Menezes
Department of Combinatorics
and Optimization
University of Waterloo
Waterloo, Ontario
Canada N2L3G1
e-mail:
ajmenez@math.uwaterloo.ca

Robert J. Zuccherato
Entrust Technologies
750 Heron Road
Ottawa, Ontario
Canada K1V1A7
e-mail:
robert.zuccherato@entrust.com

1st ed. 1998. Corr. 2nd printing 1999, 3rd printing 2004

Mathematics Subject Classification (2000): 11T71, 94A60, 68P25, 11Y16, 11Y40

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>

ISSN 1431-1550

ISBN 978-3-642-08332-7 ISBN 978-3-662-03642-6 (eBook)
DOI 10.1007/978-3-662-03642-6

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

springeronline.com

© Springer-Verlag Berlin Heidelberg 1998
Originally published by Springer-Verlag Berlin Heidelberg New York in 1998
Softcover reprint of the hardcover 1st edition 1998

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typeset by the author using a Springer \LaTeX macro package
Cover design: *design & production* GmbH, Heidelberg

Printed on acid-free paper 46/3142db - 5 4 3 2 -

Preface

This book is intended as a text for a course on cryptography with emphasis on algebraic methods. It is written so as to be accessible to graduate or advanced undergraduate students, as well as to scientists in other fields. The first three chapters form a self-contained introduction to basic concepts and techniques. Here my approach is intuitive and informal. For example, the treatment of computational complexity in Chapter 2, while lacking formalistic rigor, emphasizes the aspects of the subject that are most important in cryptography.

Chapters 4–6 and the Appendix contain material that for the most part has not previously appeared in textbook form. A novel feature is the inclusion of three types of cryptography – “hidden monomial” systems, combinatorial–algebraic systems, and hyperelliptic systems – that are at an early stage of development. It is too soon to know which, if any, of these cryptosystems will ultimately be of practical use. But in the rapidly growing field of cryptography it is worthwhile to continually explore new one-way constructions coming from different areas of mathematics. Perhaps some of the readers will contribute to the research that still needs to be done.

This book is designed not as a comprehensive reference work, but rather as a selective textbook. The many exercises (with answers at the back of the book) make it suitable for use in a math or computer science course or in a program of independent study.

I wish to thank the participants in the Mathematical Sciences Research Institute’s Summer Graduate Student Program in Algebraic Aspects of Cryptography (Berkeley, 16–27 June 1997) for giving me the opportunity to test-teach parts of the manuscript of this book and for finding errors and unclarities that needed fixing. I am especially grateful to Alfred Menezes for carefully reading the manuscript and making many valuable corrections and suggestions. Finally, I would like to thank Jacques Patarin for letting me report on his work (some of it not yet published) in Chapter 4; and Alfred Menezes, Yi-Hong Wu, and Robert Zuccherato for agreeing to let me include their elementary treatment of hyperelliptic curves as an Appendix.

Seattle, September 1997

Neal Koblitz

Contents

Chapter 1. Cryptography	1
§1. Early History	1
§2. The Idea of Public Key Cryptography	2
§3. The RSA Cryptosystem	5
§4. Diffie–Hellman and the Digital Signature Algorithm	8
§5. Secret Sharing, Coin Flipping, and Time Spent on Homework	10
§6. Passwords, Signatures, and Ciphers	12
§7. Practical Cryptosystems and Useful Impractical Ones	13
Exercises	17
Chapter 2. Complexity of Computations	18
§1. The Big- O Notation	18
Exercises	21
§2. Length of Numbers	22
Exercises	23
§3. Time Estimates	24
Exercises	31
§4. P, NP, and NP-Completeness	34
Exercises	41
§5. Promise Problems	44
§6. Randomized Algorithms and Complexity Classes	45
Exercises	48
§7. Some Other Complexity Classes	48
Exercises	52
Chapter 3. Algebra	53
§1. Fields	53
Exercises	55
§2. Finite Fields	55
Exercises	61
§3. The Euclidean Algorithm for Polynomials	63
Exercises	64
§4. Polynomial Rings	65
Exercises	70

§5. Gröbner Bases	70
Exercises	78
Chapter 4. Hidden Monomial Cryptosystems	80
§1. The Imai–Matsumoto System	80
Exercises	86
§2. Patarin’s Little Dragon	87
Exercises	95
§3. Systems That Might Be More Secure	96
Exercises	102
Chapter 5. Combinatorial–Algebraic Cryptosystems	103
§1. History	103
§2. Irrelevance of Brassard’s Theorem	104
Exercises	105
§3. Concrete Combinatorial–Algebraic Systems	105
Exercises	109
§4. The Basic Computational Algebra Problem	111
Exercises	112
§5. Cryptographic Version of Ideal Membership	112
§6. Linear Algebra Attacks	113
§7. Designing a Secure System	114
Chapter 6. Elliptic and Hyperelliptic Cryptosystems	117
§1. Elliptic Curves	117
Exercises	129
§2. Elliptic Curve Cryptosystems	131
Exercises	136
§3. Elliptic Curve Analogues of Classical Number Theory Problems	137
Exercises	139
§4. Cultural Background: Conjectures on Elliptic Curves and Surprising Relations with Other Problems	139
§5. Hyperelliptic Curves	144
Exercises	148
§6. Hyperelliptic Cryptosystems	148
Exercises	154
Appendix. An Elementary Introduction to Hyperelliptic Curves <i>by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato</i>	155
§1. Basic Definitions and Properties	156
§2. Polynomial and Rational Functions	159
§3. Zeros and Poles	161
§4. Divisors	167

§5. Representing Semi-Reduced Divisors	169
§6. Reduced Divisors	171
§7. Adding Reduced Divisors	172
Exercises	178
Answers to Exercises	179
Bibliography	193
Subject Index	201