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 Combinatrics
and Optimization
University of Waterloo
Waterloo, Ontario
Canada N2L3G1
e-mail:
ajmeneze@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

springeronline.com

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

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