Proceedings of Symposia in
APPLIED MATHEMATICS

Volume 62

Public-Key Cryptography

American Mathematical Society
Short Course
January 13–14, 2003
Baltimore, Maryland

Paul Garrett
Daniel Lieman
Editors

American Mathematical Society

http://dx.doi.org/10.1090/psapm/062

AMS SHORT COURSE LECTURE NOTES

Introductory Survey Lectures

published as a subseries of

Proceedings of Symposia in Applied Mathematics

Proceedings of Symposia in
APPLIED MATHEMATICS

Volume 62

Public-Key Cryptography

American Mathematical Society
Short Course
January 13–14, 2003
Baltimore, Maryland

Paul Garrett
Daniel Lieman
Editors

American Mathematical Society
Providence, Rhode Island

LECTURE NOTES PREPARED FOR THE
AMERICAN MATHEMATICAL SOCIETY SHORT COURSE
PUBLIC-KEY CRYPTOGRAPHY
HELD IN BALTIMORE, MARYLAND
JANUARY 13–14, 2003

The AMS Short Course Series is sponsored by the Society's Program Committee for National Meetings. The series is under the direction of the Short Course Subcommittee of the Program Committee for National Meetings.

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20, 14G50, 11G20, 11T71, 11Yxx, 94Axx, 46E25, 20C20.

Library of Congress Cataloging-in-Publication Data

Public-key cryptography / Paul Garrett, Daniel Lieman, editors.
p. cm. — (Proceedings of symposia in applied mathematics ; v. 62)
Papers from a conference held at the 2003 Baltimore meeting of the American Mathematical Society.
Includes bibliographical references and index.
ISBN 0-8218-3365-0 (alk. paper)
1. Computers—Access control—Congresses. 2. Public key cryptography—Congresses. I. Garrett, Paul, 1952– II. Lieman, Daniel, 1965– III. American Mathematical Society. IV. Series.

QA76.9.A25P82 2005
005.8′2—dc22 2005048178

---

10 9 8 7 6 5 4 3 2 1 10 09 08 07 06 05

Contents

Preface

For the Baltimore 2003 meeting of the A.M.S. Daniel Lieman organized an expository and tutorial conference on public-key cryptography for mathematicians. This volume is the collection of papers that grew out of that conference.

By contrast to a number of lower-level introductory texts aimed at undergraduates, and which therefore necessarily dilute discussion of specific cryptographic issues with discussion of elementary mathematics, the aim here was to provide a survey and introduction to public-key cryptography assuming considerable mathematical maturity and considerable general mathematical knowledge. Thus, we hoped to make clearer the cryptographic issues that fall outside the scope of standard or typical mathematics.

The papers are mostly expository, with the mathematical level of the exposition meant to be palatable to experienced mathematicians not already too much acquainted with this subject.

An important part of the context is the extra-mathematical aspect. That is, many motivations and crucial issues for genuine cryptography are difficult or impossible to understood purely in terms of formal algorithmic or other mathematical notions. (And the very validity of that last assertion is a subject of debate.) It is necessary to have some idea of the complications entailed by real-life implementations of cryptographic systems. In particular, and in considerable contrast to formal mathematics, we cannot assume that everyone plays by the rules. Further, indeed, by contrast to most mathematical and scientific research contexts wherein there is no antagonist other than a merely disinterested Nature, the presence of an *active antagonist* is a singular aspect of the practice of cryptography.

Some of the authors of the papers are academic mathematicians, some are professional cryptographers outside academe, and some have been in both situations. All the papers were reviewed for literal correctness and for aptness for our espoused purposes.

Paul Garrett

Index

ISBN 0-8218-3365-0