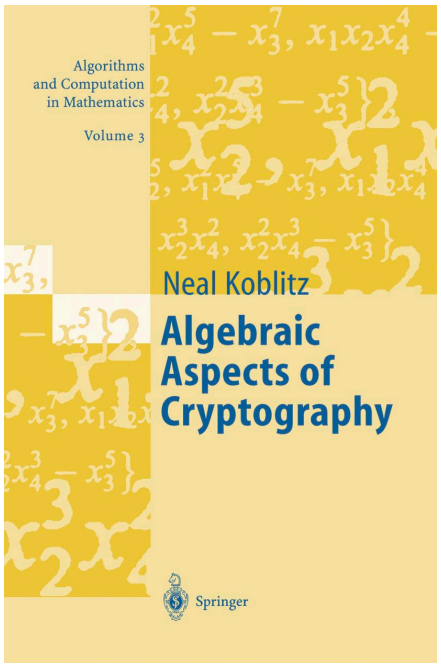

Springer

1st edition

1998, IX, 206 p.

Printed book
Hardcover

Printed book
Hardcover
ISBN 978-3-540-63446-1
£ 129,99 | CHF 177,00 | 149,99 € | 164,99 € (A) | 160,49 € (D)

Available

Discount group
Science (SC)

Product category
Monograph

Series
Algorithms and Computation in Mathematics

Other renditions
Softcover
ISBN 978-3-642-08332-7

Computer Science : Theory of Computation

Koblitz, Neal

Algebraic Aspects of Cryptography

- Cryptography is one of the hot topics right now used for manifold applications, such as telecommunication, secrecy for internet etc.
- Leads readers into advanced methods in number theory which are used for cryptography

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 sys- tems, 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.

Order online at springer.com/booksellers
Springer Nature Customer Service Center GmbH
Customer Service
Tiergartenstrasse 15-17
69121 Heidelberg
Germany
T: +49 (0)6221 345-4301
row-booksellers@springernature.com

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add $5.00 for shipping one book and $ 1.00 for each additional book. Outside the US and Canada add $ 10.00 for first book, $5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

ISBN 978-3-540-63446-1 / BIC: UY / SPRINGER NATURE: SCI16005