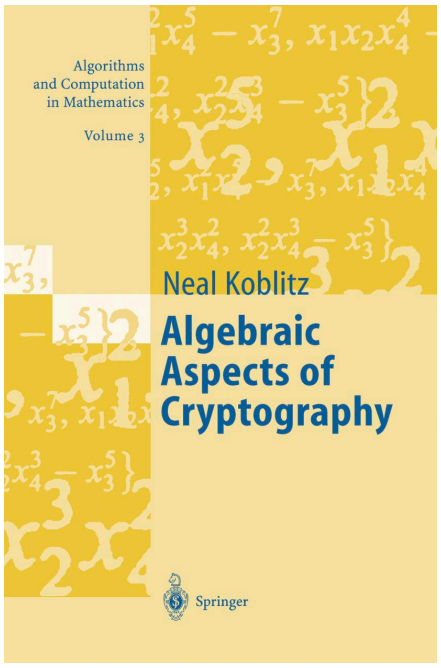

1998, IX, 206 p.

Printed book

Hardcover

149,99 € | £129.99 | $179.99
[1]160,49 € (D) | 164,99 € (A) | CHF 177,00

Softcover

109,99 € | £99.99 | $139.99
[1]117,69 € (D) | 120,99 € (A) | CHF 130,00

eBook

117,69 € | £103.50 | $139.00
[2]117,69 € (D) | 117,69 € (A) | CHF 141,50

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just
€ | $ 24.99
springer.com/mycopy

Neal Koblitz

Algebraic Aspects of Cryptography

Series: Algorithms and Computation in Mathematics

- 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 / or for the Americas call (toll free) 1-800-SPRINGER / or email us at: customerservice@springernature.com. / For outside the Americas call +49 (0) 6221-345-4301 / or email us at: customerservice@springernature.com.

The first € price and the £ and $ price are net prices, subject to local VAT. Prices indicated with [1] include VAT for books; the €(D) includes 7% for Germany, the €(A) includes 10% for Austria. Prices indicated with [2] include VAT for electronic products; 19% for Germany, 20% for Austria. All prices exclusive of carriage charges. Prices and other details are subject to change without notice. All errors and omissions excepted. [3] No discount for MyCopy.

Part of SPRINGER NATURE