Neal Koblitz

Algebraic Aspects of Cryptography

This is a textbook for a course (or self-instruction) in cryptography with emphasis on algebraic methods. The first half of the book is a self-contained informal introduction to areas of algebra, number theory, and computer science that are used in cryptography. Most of the material in the second half – "hidden monomial" systems, combinatorial-algebraic systems, and hyperelliptic systems – has not previously appeared in monograph form. The Appendix by Menezes, Wu, and Zuccherato gives an elementary treatment of hyperelliptic curves. This book is intended for graduate students, advanced undergraduates, and scientists working in various fields of data security.

From the reviews:

"...This is a textbook in cryptography with emphasis on algebraic methods. It is supported by many exercises (with answers) making it appropriate for a course in mathematics or computer science. ...Overall, this is an excellent expository text, and will be very useful to both the student and researcher."

M.V.D.Burmester, Mathematical Reviews 2000

"...I think this book is a very inspiring book on cryptography. It goes beyond the traditional topics (most of the cryptosystems presented here are first time in a textbook, some of Patarin's work is not published yet). This way the reader has the feeling how easy to suggest a cryptosystem, how easy to break a safe looking system and hence how hard to trust one. The interested readers are forced to think together with their researchers and feel the joy of discovering new ideas. At the same time the importance of "hardcore" mathematics is emphasized and hopefully some application driven students will be motivated to study theory."

P. Hajnal, Acta Scientiarum Mathematicarum 64. 1998

"...Overall, the book is highly recommended to everyone who has the requisite mathematical sophistication."

E. Leiss, Computing Reviews 1998

ISSN 1431-1550

ISBN 978-3-540-63446-1

9 783540 634461

springeronline.com

Contents