

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

Chapter 1. Cryptography	1
§1. Early History	1
§2. The Idea of Public Key Cryptography	2
§3. The RSA Cryptosystem	5
§4. Diffie–Hellman and the Digital Signature Algorithm	8
§5. Secret Sharing, Coin Flipping, and Time Spent on Homework	10
§6. Passwords, Signatures, and Ciphers	12
§7. Practical Cryptosystems and Useful Impractical Ones	13
Exercises	17
Chapter 2. Complexity of Computations	18
§1. The Big- O Notation	18
Exercises	21
§2. Length of Numbers	22
Exercises	23
§3. Time Estimates	24
Exercises	31
§4. P, NP, and NP-Completeness	34
Exercises	41
§5. Promise Problems	44
§6. Randomized Algorithms and Complexity Classes	45
Exercises	48
§7. Some Other Complexity Classes	48
Exercises	52
Chapter 3. Algebra	53
§1. Fields	53
Exercises	55
§2. Finite Fields	55
Exercises	61
§3. The Euclidean Algorithm for Polynomials	63
Exercises	64
§4. Polynomial Rings	65
Exercises	70

§5. Gröbner Bases	70
Exercises	78
Chapter 4. Hidden Monomial Cryptosystems	80
§1. The Imai–Matsumoto System	80
Exercises	86
§2. Patarin’s Little Dragon	87
Exercises	95
§3. Systems That Might Be More Secure	96
Exercises	102
Chapter 5. Combinatorial–Algebraic Cryptosystems	103
§1. History	103
§2. Irrelevance of Brassard’s Theorem	104
Exercises	105
§3. Concrete Combinatorial–Algebraic Systems	105
Exercises	109
§4. The Basic Computational Algebra Problem	111
Exercises	112
§5. Cryptographic Version of Ideal Membership	112
§6. Linear Algebra Attacks	113
§7. Designing a Secure System	114
Chapter 6. Elliptic and Hyperelliptic Cryptosystems	117
§1. Elliptic Curves	117
Exercises	129
§2. Elliptic Curve Cryptosystems	131
Exercises	136
§3. Elliptic Curve Analogues of Classical Number Theory Problems	137
Exercises	139
§4. Cultural Background: Conjectures on Elliptic Curves and Surprising Relations with Other Problems	139
§5. Hyperelliptic Curves	144
Exercises	148
§6. Hyperelliptic Cryptosystems	148
Exercises	154
Appendix. An Elementary Introduction to Hyperelliptic Curves by <i>Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato</i>	155
§1. Basic Definitions and Properties	156
§2. Polynomial and Rational Functions	159
§3. Zeros and Poles	161
§4. Divisors	167

§5. Representing Semi-Reduced Divisors	169
§6. Reduced Divisors	171
§7. Adding Reduced Divisors	172
Exercises	178
Answers to Exercises	179
Bibliography	193
Subject Index	201