## 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



springeronline.com



## Contents

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

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	§5.	Gröbner Bases	70 78			
\$1. The Imai–Matsumoto System	Che					
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           §3. Concrete Combinatorial-Algebraic Systems         105           §4. The Basic Computational Algebra Problem         111           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 Analogues of Classical Number Theory Problems         137           Exercises         139           §4. Cultural Background: Conjectures on Elliptic Curv						
§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           §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         139           g4. Cultural Background: Conjectures on Elliptic Curves         139           g5. Hy	§1.					
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           §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         139           g5. Hyperelliptic Curves         144           Exercises         148           §6. Hyperelliptic Cryptosystems         148 </td <td>00</td> <td></td> <td></td>	00					
\$3. Systems That Might Be More Secure	32.	에게 하고 있는 아니라 하는 것이 없는				
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 139  §5. Hyperelliptic Curves 144    Exercises 148  §6. Hyperelliptic Curves 148    Exercises 148  §6. Hyperelliptic Curves 148    Exercises 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 156  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161	00					
Chapter 5. Combinatorial-Algebraic Cryptosystems  §1. History  §2. Irrelevance of Brassard's Theorem Exercises  §3. Concrete Combinatorial-Algebraic Systems Exercises  §4. The Basic Computational Algebra Problem Exercises  §5. Cryptographic Version of Ideal Membership  §6. Linear Algebra Attacks  §7. Designing a Secure System  Chapter 6. Elliptic and Hyperelliptic Cryptosystems  §8. Elliptic Curves Exercises  §9. Elliptic Curves Cryptosystems  Exercises  §3. Elliptic Curve Analogues of Classical Number Theory Problems Exercises  §4. Cultural Background: Conjectures on Elliptic Curves and Surprising Relations with Other Problems  §5. Hyperelliptic Curves Exercises  §6. Hyperelliptic Cryptosystems Exercises  §6. Hyperelliptic Curves Exercises  §7. Hong Wu, and Robert J. Zuccherato  Exercises  §7. Polynomial and Rational Functions  §7. Zeros and Poles	83.					
§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         §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       144         Exercises       148         §5. Hyperelliptic Curves       144         Exercises       148         §6. Hyperelliptic Cryptosystems       154         Appendix. An Elementary Introduction to Hyperelliptic Curves         by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato       155         §1. Basic Definitions and Properties		Exercises	102			
§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         §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       144         Exercises       148         §5. Hyperelliptic Curves       144         Exercises       148         §6. Hyperelliptic Cryptosystems       154         Appendix. An Elementary Introduction to Hyperelliptic Curves         by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato       155         §1. Basic Definitions and Properties	Cha	apter 5. Combinatorial-Algebraic Cryptosystems	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         §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       139         §5. Hyperelliptic Curves       144         Exercises       148         §6. Hyperelliptic Curves       148         §6. Hyperelliptic Cryptosystems       154         Appendix. An Elementary Introduction to Hyperelliptic Curves         by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato       155         §1. Basic Definitions and Properties       156         §2.		어떻게 보면 하는데 하는데 아이들은 아이들은 아이들이 되었다면 하는데 아이들은 아이들이 아이들이 아이들이 아이들이 아이들이 아이들이 아이들이	103			
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  Exercises 119  §2. Elliptic Curves 117    Exercises 129  §3. 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 148  §6. Hyperelliptic Cryptosystems 148    Exercises 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161						
\$3. Concrete Combinatorial-Algebraic Systems Exercises \$4. The Basic Computational Algebra Problem Exercises \$5. Cryptographic Version of Ideal Membership \$6. Linear Algebra Attacks \$7. Designing a Secure System \$114  Chapter 6. Elliptic and Hyperelliptic Cryptosystems \$117  Exercises \$118  Exercises \$119  Exercises \$119  Exercises \$129  Exercises \$129  Exercises \$130  Exercises \$131  Exercises \$132  Exercises \$136  Exercises \$136  Exercises \$136  Exercises \$136  Exercises \$136  Exercises \$137  Exercises \$139  Exercises \$140  Exercises	3					
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 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161	83.	Concrete Combinatorial-Algebraic Systems				
\$4. The Basic Computational Algebra Problem  Exercises  \$5. Cryptographic Version of Ideal Membership  \$6. Linear Algebra Attacks  \$113  \$7. Designing a Secure System  114  Chapter 6. Elliptic and Hyperelliptic Cryptosystems  \$1. Elliptic Curves  Exercises  \$2. Elliptic Curve Cryptosystems  \$3. Elliptic Curve Analogues of Classical Number Theory Problems  Exercises  \$4. Cultural Background: Conjectures on Elliptic Curves  and Surprising Relations with Other Problems  \$5. Hyperelliptic Curves  44. Exercises  \$6. Hyperelliptic Curves  144  Exercises  156  158  Appendix. An Elementary Introduction to Hyperelliptic Curves  by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato  \$5. Polynomial and Rational Functions  \$5. Zeros and Poles  \$6. Polynomial and Rational Functions  \$6. Polynomial and Rational Functions  \$6. Polynomial and Properties  \$6. Polynomial and Rational Functions  \$6. Polynomial and Properties  \$6. Polynomial and Properties  \$6. Polynomial and Rational Functions  \$6. Polynomial and Properties  \$6. Polynomial Pr	30.					
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 129  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 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161	84.					
\$5. Cryptographic Version of Ideal Membership  \$6. Linear Algebra Attacks  \$7. Designing a Secure System  114  Chapter 6. Elliptic and Hyperelliptic Cryptosystems  117  \$1. Elliptic Curves  Exercises  \$2. Elliptic Curve Cryptosystems  Exercises  \$3. Elliptic Curve Analogues of Classical Number Theory Problems  Exercises  \$4. Cultural Background: Conjectures on Elliptic Curves  and Surprising Relations with Other Problems  \$5. Hyperelliptic Curves  44. Exercises  \$6. Hyperelliptic Curves  48. Exercises  19. Hyperelliptic Curves  59. Hyperelliptic Cryptosystems  Exercises  108  409  418  419  420  430  440  440  440  440  440  440	3					
\$6. Linear Algebra Attacks \$7. Designing a Secure System  114  Chapter 6. Elliptic and Hyperelliptic Cryptosystems  117  §1. Elliptic Curves	85.					
\$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 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 156  \$1. Basic Definitions and Properties 156  \$2. Polynomial and Rational Functions 159  \$3. Zeros and Poles 161	0					
Chapter 6. Elliptic and Hyperelliptic Cryptosystems  117  §1. Elliptic Curves	0					
\$1. Elliptic Curves	3	/ / / / / / / / / / / / / / / / / / /				
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 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161	Chapter 6. Elliptic and Hyperelliptic Cryptosystems					
\$2. Elliptic Curve Cryptosystems 136 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 Exercises 148 \$6. Hyperelliptic Cryptosystems 148 Exercises 154  Appendix. An Elementary Introduction to Hyperelliptic Curves 154  Appendix An Elementary Introduction to Hyperelliptic Curves 155 \$1. Basic Definitions and Properties 156 \$2. Polynomial and Rational Functions 159 \$3. Zeros and Poles 161	§1.	Elliptic Curves	117			
Exercises		Exercises	129			
\$3. Elliptic Curve Analogues of Classical Number Theory Problems Exercises	§2.	Elliptic Curve Cryptosystems	131			
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 Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161		Exercises	136			
\$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 Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155  \$1. Basic Definitions and Properties 156  \$2. Polynomial and Rational Functions 159  \$3. Zeros and Poles 161	§3.	Elliptic Curve Analogues of Classical Number Theory Problems	137			
and Surprising Relations with Other Problems  §5. Hyperelliptic Curves Exercises  §6. Hyperelliptic Cryptosystems Exercises  Appendix. An Elementary Introduction to Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato  §1. Basic Definitions and Properties §2. Polynomial and Rational Functions §3. Zeros and Poles  139  148  148  148  159  150  150  151  152  153  154			139			
\$5. Hyperelliptic Curves Exercises 148 \$6. Hyperelliptic Cryptosystems Exercises 154  Appendix. An Elementary Introduction to Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155 \$1. Basic Definitions and Properties \$2. Polynomial and Rational Functions \$3. Zeros and Poles 161	§4.	그 가는 것이 있는 것이 있는 것이 없는 것이었다면 없는 없는 것이었다면 없는 없는 것이었다면 없었다면 없는 것이었다면 없었다면 없었다면 없었다면 없었다면 없었다면 없었다면 없었다면 없				
Exercises 148  §6. Hyperelliptic Cryptosystems 148 Exercises 154  Appendix. An Elementary Introduction to Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161			139			
\$6. Hyperelliptic Cryptosystems Exercises  Appendix. An Elementary Introduction to Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato  \$1. Basic Definitions and Properties \$2. Polynomial and Rational Functions \$3. Zeros and Poles  148 154	§5.	사용하다 그 경우 하나 하는데 얼마 아내는데 아내는데 아내는데 아내는데 아내는데 아내는데 아내는데 아내는데	144			
Appendix. An Elementary Introduction to Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato  §1. Basic Definitions and Properties §2. Polynomial and Rational Functions §3. Zeros and Poles  154			148			
Appendix. An Elementary Introduction to Hyperelliptic Curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155  §1. Basic Definitions and Properties 156 §2. Polynomial and Rational Functions 159 §3. Zeros and Poles 161	§6.					
by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161		Exercises	154			
by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato 155  §1. Basic Definitions and Properties 156  §2. Polynomial and Rational Functions 159  §3. Zeros and Poles 161	Appendix. An Elementary Introduction to Hyperelliptic Curves					
§1. Basic Definitions and Properties156§2. Polynomial and Rational Functions159§3. Zeros and Poles161		그들은 사람이 되었다. 이 집에 가는 사람들은 사람들이 되었다. 그는 사람들은 사람들은 사람들은 사람들은 사람들은 사람들은 사람들은 사람들은	155			
§2. Polynomial and Rational Functions						
§3. Zeros and Poles	4.00					
	U					

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