

CONTENTS

Acknowledgments

xix

About the Authors

xx

CHAPTER 1 Introduction

1

1.1	Opinions, Products	2
1.2	Roadmap to the Book	2
1.3	Terminology	4
1.4	Notation	6
1.5	Cryptographically Protected Sessions	6
1.6	Active and Passive Attacks	7
1.7	Legal Issues	8
1.7.1	Patents	8
1.7.2	Government Regulations	9
1.8	Some Network Basics	9
1.8.1	Network Layers	10
1.8.2	TCP and UDP Ports	11
1.8.3	DNS (Domain Name System)	11
1.8.4	HTTP and URLs	12
1.8.5	Web Cookies	12
1.9	Names for Humans	13
1.10	Authentication and Authorization	14
1.10.1	ACL (Access Control List)	14
1.10.2	Central Administration/Capabilities	14
1.10.3	Groups	15
1.10.4	Cross-Organizational and Nested Groups	15
1.10.5	Roles	17
1.11	Malware: Viruses, Worms, Trojan Horses	18
1.11.1	Where Does Malware Come From?	19
1.11.2	Virus Checkers	20
1.12	Security Gateway	21
1.12.1	Firewall	21
1.12.2	Application-Level Gateway/Proxy	23
1.12.3	Secure Tunnels	24
1.12.4	Why Firewalls Don't Work	25

1.13	Denial-of-Service (DoS) Attacks	26
1.14	NAT (Network Address Translation).....	27
1.14.1	Summary	28
CHAPTER 2	Introduction to Cryptography	31
2.1	Introduction	31
2.1.1	The Fundamental Tenet of Cryptography	32
2.1.2	Keys.....	32
2.1.3	Computational Difficulty	32
2.1.4	To Publish or Not to Publish.....	34
2.1.5	Earliest Encryption.....	34
2.1.6	One-Time Pad (OTP)	35
2.2	Secret Key Cryptography	36
2.2.1	Transmitting Over an Insecure Channel.....	37
2.2.2	Secure Storage on Insecure Media	37
2.2.3	Authentication	37
2.2.4	Integrity Check.....	38
2.3	Public Key Cryptography.....	39
2.3.1	Transmitting Over an Insecure Channel.....	40
2.3.2	Secure Storage on Insecure Media	41
2.3.3	Authentication	41
2.3.4	Digital Signatures.....	42
2.4	Hash Algorithms	43
2.4.1	Password Hashing	43
2.4.2	Message Integrity	43
2.4.3	Message Fingerprint.....	44
2.4.4	Efficient Digital Signatures.....	44
2.5	Breaking an Encryption Scheme	45
2.5.1	Ciphertext Only	45
2.5.2	Known Plaintext.....	46
2.5.3	Chosen Plaintext.....	46
2.5.4	Chosen Ciphertext.....	47
2.5.5	Side-Channel Attacks.....	48
2.6	Random Numbers.....	48
2.6.1	Gathering Entropy	49
2.6.2	Generating Random Seeds	50
2.6.3	Calculating a Pseudorandom Stream from the Seed	50
2.6.4	Periodic Reseeding.....	51
2.6.5	Types of Random Numbers.....	51
2.6.6	Noteworthy Mistakes	52
2.7	Numbers	53
2.7.1	Finite Fields.....	54

88	2.7.2	Exponentiation.....	55
88	2.7.3	Avoiding a Side-Channel Attack.....	55
88	2.7.4	Types of Elements used in Cryptography	56
88	2.7.5	Euclidean Algorithm	56
90	2.7.6	Chinese Remainder Theorem	57
14	2.8	Homework	58
CHAPTER 3 Secret Key Cryptography			61
60	3.1	Introduction	61
60	3.2	Generic Block Cipher Issues	61
80	3.2.1	Blocksize, Keysize	61
60	3.2.2	Completely General Mapping	62
70	3.2.3	Looking Random	63
80	3.3	Constructing a Practical Block Cipher	64
80	3.3.1	Per-Round Keys.....	64
90	3.3.2	S-boxes and Bit Shuffles	64
100	3.3.3	Feistel Ciphers	65
100	3.4	Choosing Constants	67
101	3.5	Data Encryption Standard (DES)	67
101	3.5.1	DES Overview.....	68
101	3.5.2	The Mangler Function	69
101	3.5.3	Undesirable Symmetries.....	70
101	3.5.4	What's So Special About DES?	71
101	3.6	3DES (Multiple Encryption DES).....	71
101	3.6.1	How Many Encryptions?.....	72
101	3.6.1.1	Encrypting Twice with the Same Key	73
110	3.6.1.2	Encrypting Twice with Two Keys	73
110	3.6.1.3	Triple Encryption with Only Two Keys	74
111	3.6.2	Why EDE Rather Than EEE?.....	75
111	3.7	Advanced Encryption Standard (AES).....	75
111	3.7.1	Origins of AES	75
111	3.7.2	Broad Overview.....	76
111	3.7.3	AES Overview.....	78
111	3.7.4	Key Expansion.....	80
111	3.7.5	Inverse Rounds	80
111	3.7.6	Software Implementations of AES.....	81
111	3.8	RC4.....	81
111	3.9	Homework	83
CHAPTER 4 Modes of Operation			85
119	4.1	Introduction	85
120	4.2	Encrypting a Large Message	86

4.2.1	ECB (Electronic Code Book).....	86
4.2.2	CBC (Cipher Block Chaining).....	88
4.2.2.1	Randomized ECB.....	88
4.2.2.2	CBC.....	88
4.2.2.3	CBC Threat—Modifying Ciphertext Blocks.....	90
4.2.3	CTR (Counter Mode).....	91
4.2.3.1	Choosing IVs for CTR Mode.....	92
4.2.4	XEX (XOR Encrypt XOR).....	93
4.2.5	XTS (XEX with Ciphertext Stealing).....	94
4.3	Generating MACs.....	96
4.3.1	CBC-MAC.....	96
4.3.1.1	CBC Forgery Attack.....	96
4.3.2	CMAC.....	97
4.3.3	GMAC.....	98
4.3.3.1	GHASH.....	98
4.3.3.2	Transforming GHASH into GMAC.....	99
4.4	Ensuring Privacy and Integrity Together.....	100
4.4.1	CCM (Counter with CBC-MAC).....	100
4.4.2	GCM (Galois/Counter Mode).....	101
4.5	Performance Issues.....	102
4.6	Homework.....	102
CHAPTER 5	Cryptographic Hashes	105
5.1	Introduction.....	105
5.2	The Birthday Problem.....	108
5.3	A Brief History of Hash Functions.....	108
5.4	Nifty Things to Do with a Hash.....	110
5.4.1	Digital Signatures.....	110
5.4.2	Password Database.....	111
5.4.3	Secure Shorthand of Larger Piece of Data.....	111
5.4.4	Hash Chains.....	111
5.4.5	Blockchain.....	112
5.4.6	Puzzles.....	112
5.4.7	Bit Commitment.....	113
5.4.8	Hash Trees.....	113
5.4.9	Authentication.....	114
5.4.10	Computing a MAC with a Hash.....	114
5.4.11	HMAC.....	116
5.4.12	Encryption with a Secret and a Hash Algorithm.....	118
5.5	Creating a Hash Using a Block Cipher.....	119
5.6	Construction of Hash Functions.....	119
5.6.1	Construction of MD4, MD5, SHA-1 and SHA-2.....	120

5.6.2	Construction of SHA-3.....	122
5.7	Padding.....	124
5.7.1	MD4, MD5, SHA-1, and SHA2-256 Message Padding.....	124
5.7.2	SHA-3 Padding Rule.....	126
5.8	The Internal Encryption Algorithms.....	127
5.8.1	SHA-1 Internal Encryption Algorithm.....	127
5.8.2	SHA-2 Internal Encryption Algorithm.....	128
5.9	SHA-3 f Function (Also Known as KECCAK- f).....	129
5.10	Homework.....	132
CHAPTER 6 First-Generation Public Key Algorithms		135
6.1	Introduction.....	135
6.2	Modular Arithmetic.....	136
6.2.1	Modular Addition.....	136
6.2.2	Modular Multiplication.....	137
6.2.3	Modular Exponentiation.....	138
6.2.4	Fermat's Theorem and Euler's Theorem.....	139
6.3	RSA.....	140
6.3.1	RSA Algorithm.....	140
6.3.2	Why Does RSA Work?.....	141
6.3.3	Why Is RSA Secure?.....	141
6.3.4	How Efficient Are the RSA Operations?.....	142
6.3.4.1	Exponentiating with Big Numbers.....	142
6.3.4.2	Generating RSA Keys.....	144
6.3.4.3	Why a Non-Prime Has Multiple Square Roots of One.....	146
6.3.4.4	Having a Small Constant e	147
6.3.4.5	Optimizing RSA Private Key Operations.....	148
6.3.5	Arcane RSA Threats.....	149
6.3.5.1	Smooth Numbers.....	150
6.3.5.2	The Cube Root Problem.....	151
6.3.6	Public-Key Cryptography Standard (PKCS).....	151
6.3.6.1	Encryption.....	152
6.3.6.2	The Million-Message Attack.....	152
6.3.6.3	Signing.....	153
6.4	Diffie-Hellman.....	154
6.4.1	MITM (Meddler-in-the-Middle) Attack.....	155
6.4.2	Defenses Against MITM Attack.....	156
6.4.3	Safe Primes and the Small-Subgroup Attack.....	157
6.4.4	ElGamal Signatures.....	159
6.5	Digital Signature Algorithm (DSA).....	160
6.5.1	The DSA Algorithm.....	161
6.5.2	Why Is This Secure?.....	162

6.5.3	Per-Message Secret Number	162
6.6	How Secure Are RSA and Diffie-Hellman?	163
6.7	Elliptic Curve Cryptography (ECC).....	164
6.7.1	Elliptic Curve Diffie-Hellman (ECDH)	166
6.7.2	Elliptic Curve Digital Signature Algorithm (ECDSA)	167
6.8	Homework.....	168
CHAPTER 7	Quantum Computing	169
7.1	What Is a Quantum Computer?	169
7.1.1	A Preview of the Conclusions	169
7.1.2	First, What Is a Classical Computer?	170
7.1.3	Qubits and Superposition	171
7.1.3.1	Example of a Qubit.....	173
7.1.3.2	Multi-Qubit States and Entanglement	173
7.1.4	States and Gates as Vectors and Matrices.....	174
7.1.5	Becoming Superposed and Entangled.....	175
7.1.6	Linearity	176
7.1.6.1	No Cloning Theorem	176
7.1.7	Operating on Entangled Qubits	177
7.1.8	Unitarity	177
7.1.9	Doing Irreversible Operations by Measurement	178
7.1.10	Making Irreversible Classical Operations Reversible	178
7.1.11	Universal Gate Sets	179
7.2	Grover's Algorithm	180
7.2.1	Geometric Description	182
7.2.2	How to Negate the Amplitude of $ k\rangle$	183
7.2.3	How to Reflect All the Amplitudes Across the Mean.....	184
7.2.4	Parallelizing Grover's Algorithm.....	186
7.3	Shor's Algorithm.....	186
7.3.1	Why Exponentiation mod n Is a Periodic Function	187
7.3.2	How Finding the Period of $a^x \bmod n$ Lets You Factor n	187
7.3.3	Overview of Shor's Algorithm.....	188
7.3.4	Converting to the Frequency Graph—Introduction	190
7.3.5	The Mechanics of Converting to the Frequency Graph	191
7.3.6	Calculating the Period	194
7.3.7	Quantum Fourier Transform	194
7.4	Quantum Key Distribution (QKD).....	195
7.4.1	Why It's Sometimes Called Quantum Encryption.....	197
7.4.2	Is Quantum Key Distribution Important?.....	197
7.5	How Hard Are Quantum Computers to Build?.....	197
7.6	Quantum Error Correction	199
7.7	Homework.....	201

CHAPTER 8	Post-Quantum Cryptography	203
8.1	Signature and/or Encryption Schemes.....	204
8.1.1	NIST Criteria for Security Levels	205
8.1.2	Authentication	205
8.1.3	Defense Against Dishonest Ciphertext.....	206
8.2	Hash-based Signatures.....	207
8.2.1	Simplest Scheme – Signing a Single Bit	208
8.2.2	Signing an Arbitrary-sized Message	208
8.2.3	Signing Lots of Messages.....	209
8.2.4	Deterministic Tree Generation	211
8.2.5	Short Hashes.....	212
8.2.6	Hash Chains.....	213
8.2.7	Standardized Schemes	214
8.2.7.1	Stateless Schemes	214
8.3	Lattice-Based Cryptography.....	216
8.3.1	A Lattice Problem.....	217
8.3.2	Optimization: Matrices with Structure	218
8.3.3	NTRU-Encryption Family of Lattice Encryption Schemes	219
8.3.3.1	Bob Computes a (Public, Private) Key Pair	220
8.3.3.2	How Bob Decrypts to Find m	220
8.3.3.3	How Does this Relate to Lattices?.....	221
8.3.4	Lattice-Based Signatures	223
8.3.4.1	Basic Idea.....	223
8.3.4.2	Insecure Scheme	223
8.3.4.3	Fixing the Scheme	224
8.3.5	Learning with Errors (LWE)	225
8.3.5.1	LWE Optimizations	226
8.3.5.2	LWE-based NIST Submissions	229
8.4	Code-based Schemes	229
8.4.1	Non-cryptographic Error-correcting Codes.....	230
8.4.1.1	Invention Step.....	231
8.4.1.2	Codeword Creation Step.....	231
8.4.1.3	Misfortune Step.....	231
8.4.1.4	Diagnosis Step	232
8.4.2	The Parity-Check Matrix.....	234
8.4.3	Cryptographic Public Key Code-based Scheme.....	235
8.4.3.1	Neiderreiter Optimization	236
8.4.3.2	Generating a Public Key Pair.....	236
8.4.3.3	Using Circulant Matrices	239
8.5	Multivariate Cryptography	239
8.5.1	Solving Linear Equations	240

8.5.2	Quadratic Polynomials	240
8.5.3	Polynomial Systems	240
8.5.4	Multivariate Signature Systems	241
8.5.4.1	Multivariate Public Key Signatures.....	241
8.6	Homework.....	244
CHAPTER 9	Authentication of People	249
9.1	Password-based Authentication	251
9.1.1	Challenge-Response Based on Password.....	251
9.1.2	Verifying Passwords	252
9.2	Address-based Authentication.....	253
9.2.1	Network Address Impersonation.....	254
9.3	Biometrics	255
9.4	Cryptographic Authentication Protocols.....	255
9.5	Who Is Being Authenticated?	256
9.6	Passwords as Cryptographic Keys	256
9.7	On-Line Password Guessing	257
9.8	Off-Line Password Guessing	260
9.9	Using the Same Password in Multiple Places	261
9.10	Requiring Frequent Password Changes.....	261
9.11	Tricking Users into Divulging Passwords.....	262
9.12	Lamport's Hash	263
9.13	Password Managers.....	265
9.14	Web Cookies	266
9.15	Identity Providers (IDPs)	267
9.16	Authentication Tokens	268
9.16.1	Disconnected Tokens	268
9.16.2	Public Key Tokens	270
9.17	Strong Password Protocols.....	272
9.17.1	Subtle Details	274
9.17.2	Augmented Strong Password Protocols	275
9.17.3	SRP (Secure Remote Password)	276
9.18	Credentials Download Protocols	277
9.19	Homework.....	278
CHAPTER 10	Trusted Intermediaries	281
10.1	Introduction	281
10.2	Functional Comparison	282
10.3	Kerberos	283
10.3.1	KDC Introduces Alice to Bob	283
10.3.2	Alice Contacts Bob.....	284
10.3.3	Ticket Granting Ticket (TGT).....	285

10.3.4	Interrealm Authentication.....	286
10.3.5	Making Password-Guessing Attacks Difficult.....	287
10.3.6	Double TGT Protocol.....	288
10.3.7	Authorization Information.....	288
10.3.8	Delegation.....	289
10.4	PKI.....	289
10.4.1	Some Terminology.....	290
10.4.2	Names in Certificates.....	290
10.5	Website Gets a DNS Name and Certificate.....	291
10.6	PKI Trust Models.....	292
10.6.1	Monopoly Model.....	292
10.6.2	Monopoly plus Registration Authorities (RAs).....	293
10.6.3	Delegated CAs.....	294
10.6.4	Oligarchy.....	294
10.6.5	Anarchy Model.....	295
10.6.6	Name Constraints.....	296
10.6.7	Top-Down with Name Constraints.....	297
10.6.8	Multiple CAs for Any Namespace Node.....	297
10.6.9	Bottom-Up with Name Constraints.....	297
10.6.9.1	Functionality of Up-Links.....	298
10.6.9.2	Functionality of Cross-Links.....	299
10.6.10	Name Constraints in PKIX Certificates.....	300
10.7	Building Certificate Chains.....	301
10.8	Revocation.....	302
10.8.1	CRL (Certificate Revocation list).....	302
10.8.2	Online Certificate Status Protocol (OCSP).....	304
10.8.3	Good-Lists vs. Bad-Lists.....	304
10.9	Other Information in a PKIX Certificate.....	305
10.10	Issues with Expired Certificates.....	306
10.11	DNSSEC (DNS Security Extensions).....	307
10.12	Homework.....	309
CHAPTER 11	Communication Session Establishment	313
11.1	One-way Authentication of Alice.....	314
11.1.1	Timestamps vs. Challenges.....	316
11.1.2	One-Way Authentication of Alice using a Public Key.....	318
11.2	Mutual Authentication.....	320
11.2.1	Reflection Attack.....	320
11.2.2	Timestamps for Mutual Authentication.....	322
11.3	Integrity/Encryption for Data.....	323
11.3.1	Session Key Based on Shared Secret Credentials.....	324
11.3.2	Session Key Based on Public Key Credentials.....	325

11.3.3	Session Key Based on One-Party Public Keys	326
11.4	Nonce Types.....	326
11.5	Intentional MITM.....	328
11.6	Detecting MITM	329
11.7	What Layer?	330
11.8	Perfect Forward Secrecy	333
11.9	Preventing Forged Source Addresses.....	335
11.9.1	Allowing Bob to Be Stateless in TCP	335
11.9.2	Allowing Bob to Be Stateless in IPsec.....	336
11.10	Endpoint Identifier Hiding	337
11.11	Live Partner Reassurance	339
11.12	Arranging for Parallel Computation.....	340
11.13	Session Resumption/Multiple Sessions.....	341
11.14	Plausible Deniability	343
11.15	Negotiating Crypto Parameters	343
11.15.1	Suites vs. à la Carte	344
11.15.2	Downgrade Attack.....	345
11.16	Homework.....	345
CHAPTER 12 IPsec		349
12.1	IPsec Security Associations	349
12.1.1	Security Association Database.....	350
12.1.2	Security Policy Database.....	351
12.1.3	IKE-SAs and Child-SAs.....	351
12.2	IKE (Internet Key Exchange Protocol)	353
12.3	Creating a Child-SA.....	355
12.4	AH and ESP	356
12.4.1	ESP Integrity Protection.....	356
12.4.2	Why Protect the IP Header?.....	357
12.4.3	Tunnel, Transport Mode.....	358
12.4.4	IPv4 Header.....	360
12.4.5	IPv6 Header.....	360
12.5	AH (Authentication Header)	361
12.6	ESP (Encapsulating Security Payload)	362
12.7	Comparison of Encodings	364
12.8	Homework.....	364
CHAPTER 13 SSL/TLS and SSH		367
13.1	Using TCP	367
13.2	StartTLS	368
13.3	Functions in the TLS Handshake	369
13.4	TLS 1.2 (and Earlier) Basic Protocol.....	369

13.5	TLS 1.3	371
13.6	Session Resumption.....	372
13.7	PKI as Deployed by TLS.....	373
13.8	SSH (Secure Shell)	374
13.8.1	SSH Authentication	376
13.8.2	SSH Port Forwarding	376
13.9	Homework	377
CHAPTER 14 Electronic Mail Security		379
14.1	Distribution Lists	380
14.2	Store and Forward	382
14.3	Disguising Binary as Text	383
14.4	HTML-Formatted Email	384
14.5	Attachments	385
14.6	Non-cryptographic Security Features.....	385
14.6.1	Spam Defenses	385
14.7	Malicious Links in Email	387
14.8	Data Loss Prevention (DLP)	387
14.9	Knowing Bob's Email Address	388
14.10	Self-Destruct, Do-Not-Forward,	388
14.11	Preventing Spoofing of From Field.....	389
14.12	In-Flight Encryption	390
14.13	End-to-End Signed and Encrypted Email.....	390
14.14	Encryption by a Server	392
14.15	Message Integrity	393
14.16	Non-Repudiation	394
14.17	Plausible Deniability	394
14.18	Message Flow Confidentiality.....	395
14.19	Anonymity	397
14.20	Homework	398
CHAPTER 15 Electronic Money		401
15.1	ECASH.....	402
15.2	Offline eCash.....	403
15.2.1	Practical Attacks	405
15.3	Bitcoin	406
15.3.1	Transactions.....	407
15.3.2	Bitcoin Addresses.....	407
15.3.3	Blockchain.....	408
15.3.4	The Ledger.....	408
15.3.5	Mining	410
15.3.6	Blockchain Forks.....	411

15.3.7	Why Is Bitcoin So Energy-Intensive?	412
15.3.8	Integrity Checks: Proof of Work vs. Digital Signatures	412
15.3.9	Concerns	413
15.4	Wallets for Electronic Currency	414
15.5	Homework	414
CHAPTER 16 Cryptographic Tricks		417
16.1	Secret Sharing	417
16.2	Blind Signature	418
16.3	Blind Decryption	419
16.4	Zero-Knowledge Proofs	420
16.4.1	Graph Isomorphism ZKP	420
16.4.2	Proving Knowledge of a Square Root	421
16.4.3	Noninteractive ZKP	422
16.5	Group Signatures	423
16.5.1	Trivial Group Signature Schemes	424
16.5.1.1	Single Shared Key	424
16.5.1.2	Group Membership Certificate	424
16.5.1.3	Multiple Group Membership Certificates	425
16.5.1.4	Blindly Signed Multiple Group Membership Certificates	425
16.5.2	Ring Signatures	425
16.5.3	DAA (Direct Anonymous Attestation)	427
16.5.4	EPID (Enhanced Privacy ID)	428
16.6	Circuit Model	428
16.7	Secure Multiparty Computation (MPC)	429
16.8	Fully Homomorphic Encryption (FHE)	431
16.8.1	Bootstrapping	432
16.8.2	Easy-to-Understand Scheme	433
16.9	Homework	434
CHAPTER 17 Folklore		437
17.1	Misconceptions	437
17.2	Perfect Forward Secrecy	438
17.3	Change Encryption Keys Periodically	439
17.4	Don't Encrypt without Integrity Protection	440
17.5	Multiplexing Flows over One Secure Session	441
17.5.1	The Splicing Attack	441
17.5.2	Service Classes	442
17.5.3	Different Cryptographic Algorithms	442
17.6	Using Different Secret Keys	443
17.6.1	For Initiator and Responder in Handshake	443
17.6.2	For Encryption and Integrity	443

17.6.3	In Each Direction of a Secure Session	444
17.7	Using Different Public Keys	444
17.7.1	Use Different Keys for Different Purposes	444
17.7.2	Different Keys for Signing and Encryption.....	445
17.8	Establishing Session Keys.....	446
17.8.1	Have Both Sides Contribute to the Master Key	446
17.8.2	Don't Let One Side Determine the Key	446
17.9	Hash in a Constant When Hashing a Password.....	447
17.10	HMAC Rather than Simple Keyed Hash.....	447
17.11	Key Derivation	448
17.12	Use of Nonces in Protocols	449
17.13	Creating an Unpredictable Nonce	449
17.14	Compression	450
17.15	Minimal vs. Redundant Designs.....	451
17.16	Overestimate the Size of Key	451
17.17	Hardware Random Number Generators	452
17.18	Put Checksums at the End of Data	452
17.19	Forward Compatibility	453
17.19.1	Options	453
17.19.2	Version Numbers.....	454
17.19.2.1	Version Number Field Must Not Move	454
17.19.2.2	Negotiating Highest Version Supported	455
17.19.2.3	Minor Version Number Field	455
Glossary		G-1
Math		M-1
M.1	Introduction	M-1
M.2	Some definitions and notation.....	M-2
M.3	Arithmetic.....	M-3
M.4	Abstract Algebra.....	M-4
M.5	Modular Arithmetic	M-5
M.5.1	How Do Computers Do Arithmetic?.....	M-6
M.5.2	Computing Inverses in Modular Arithmetic.....	M-6
M.5.2.1	The Euclidean Algorithm.....	M-7
M.5.2.2	The Chinese Remainder Theorem	M-8
M.5.3	How Fast Can We Do Arithmetic?.....	M-8
M.6	Groups	M-9
M.7	Fields	M-10
M.7.1	Polynomials	M-11
M.7.2	Finite Fields.....	M-13
M.7.2.1	What Sizes Can Finite Fields Be?.....	M-14

	M.7.2.2	Representing a Field	M-14
M.8		Mathematics of Rijndael	M-16
	M.8.1	A Rijndael Round.....	M-17
M.9		Elliptic Curve Cryptography	M-18
M.10		Rings.....	M-19
M.11		Linear Transformations	M-20
M.12		Matrix Arithmetic.....	M-21
	M.12.1	Permutations.....	M-22
	M.12.2	Matrix Inverses.....	M-22
		M.12.2.1 Gaussian Elimination.....	M-22
M.13		Determinants	M-23
	M.13.1	Properties of Determinants.....	M-24
		M.13.1.1 Adjugate of a Matrix.....	M-24
	M.13.2	Proof: Determinant of Product is Product of Determinants	M-25
M.14		Homework.....	M-26

Bibliography **B-1**

Index **I-1**

1.1	Introduction	1
1.2	Some definitions and notation	1
1.3	Algebraic	1
1.4	Abstract Algebra	1
1.5	Module Arithmetic	1
1.6	How Do Computers Do Arithmetic?	1
1.7	Computing Inverses in Modular Arithmetic	1
1.8	The Euclidean Algorithm	1
1.9	The Extended Euclidean Algorithm	1
1.10	How Fast Can We Do Arithmetic?	1
1.11	Groups	1
1.12	Fields	1
1.13	Polynomials	1
1.14	Finite Fields	1
1.15	What Size Can Finite Fields Be?	1