Contents

Preface xiii
About the Author xv
Dependency Chart xvii
Acknowledgments xix

1 An Overview of the Subject 1

Basic Concepts 1
Functions 4
One-to-One and Onto Functions, Bijections 5
Inverse Functions 7
Substitution Ciphers 8
Attacks on Cryptosystems 12
The Vigenère Cipher 15
The Playfair Cipher 18
The One-Time Pad, Perfect Secrecy 25
Chapter 1 Exercises 28
Chapter 1 Computer Implementations and Exercises 35
- Vector/String Conversions 35
- Integer/Text Conversions 36
- Programming Basic Ciphers with Integer Arithmetic 38
- Computer-Generated Random Numbers 39

2 Divisibility and Modular Arithmetic 43

Divisibility 43
Primes 44
Greatest Common Divisors and Relatively Prime Integers 46
The Division Algorithm 47
The Euclidean Algorithm 48
Modular Arithmetic and Congruences 52
Modular Integer Systems 58
Modular Inverses 60
Extended Euclidean Algorithm 61
Solving Linear Congruences 64
- Summary of Procedure for Solving the Single Linear Congruence (Equation 2.2) 66

The Chinese Remainder Theorem 67
Chapter 2 Exercises 71
Chapter 2 Computer Implementations and Exercises 85

3 The Evolution of Codemaking until the Computer Era. 91
Ancient Codes 91
Formal Definition of a Cryptosystem 94
Affine Ciphers 96
Steganography 100
Nulls 102
Homophones 105
Composition of Functions 109
Tabular Form Notation for Permutations 110
The Enigma Machines 111
Cycles (Cyclic Permutations) 114
Dissection of the Enigma Machine into Permutations 119
Special Properties of All Enigma Machines 126
Chapter 3 Exercises 127
Chapter 3 Computer Implementations and Exercises 136
Computer Representations of Permutations 140

4 Matrices and the Hill Cryptosystem 145
The Anatomy of a Matrix 145
Matrix Addition, Subtraction, and Scalar Multiplication 146
Matrix Multiplication 147
Preview of the Fact That Matrix Multiplication Is Associative 149
Matrix Arithmetic 149
Definition of an Invertible (Square) Matrix 151
The Determinant of a Square Matrix 153
Inverses of 2 × 2 Matrices 155
The Transpose of a Matrix 156
Modular Integer Matrices 156
The Classical Adjoint (for Matrix Inversions) 159
The Hill Cryptosystem 162
Chapter 4 Exercises 166
Chapter 4 Computer Implementations and Exercises 174

5 The Evolution of Codebreaking until the Computer Era. 181
Frequency Analysis Attacks 181
The Demise of the Vigenère Cipher 187
The Babbage/Kasiski Attack 188
The Friedman Attack 192
The Index of Coincidence 193
Expected Values of the Index of Coincidence 193
How Enigmas Were Attacked 201
German Usage Protocols for Enigmas 202
The Polish Codebreakers 203
Rejewski's Attack 203
Invariance of Cycle Decomposition Form 205
Alan Turing and Bletchley Park 206
Chapter 5 Exercises 208
Chapter 5 Computer Implementations and Exercises 214

Programs to Aid in Frequency Analysis 214
Programs to Aid in the Babbage/Kasiski Attack 215
Programs Related to the Friedman Attack 218

6 Representation and Arithmetic of Integers in Different Bases 221
Representation of Integers in Different Bases 221
Hex(adecimal) and Binary Expansions 224
Addition Algorithm with Base *b* Expansions 229
Subtraction Algorithm with Base *b* Expansions 231
Multiplication Algorithm in Base *b* Expansions 234
Arithmetic with Large Integers 237
Fast Modular Exponentiation 239
Chapter 6 Exercises 241
Chapter 6 Computer Implementations and Exercises 248

7 Block Cryptosystems and the Data Encryption Standard (DES) . . . 251
The Evolution of Computers into Cryptosystems 251
DES Is Adopted to Fulfill an Important Need 252
The XOR Operation 254
Feistel Cryptosystems 255
A Scaled-Down Version of DES 258
DES 265
The Fall of DES 272
Triple DES 273
Modes of Operation for Block Cryptosystems 274
Electronic Codebook (ECB) Mode 274
Cipherblock Chaining (CBC) Mode 275
Cipher Feedback (CFB) Mode 276
Output Feedback (OFB) Mode 278
Chapter 7 Exercises 279
Chapter 7 Computer Implementations and Exercises 286

8 Some Number Theory and Algorithms 293
The Prime Number Theorem 293
Fermat's Little Theorem 295
The Euler Phi Function 298
Euler's Theorem 300
Modular Orders of Invertible Modular Integers 301
Primitive Roots 302
Existence of Primitive Roots 304
Determination of Primitive Roots 304
Order of Powers Formula 305
Prime Number Generation 308
Fermat's Primality Test 309
Carmichael Numbers 311
The Miller–Rabin Test 312
The Miller–Rabin Test with a Factoring Enhancement 315

The Pollard $p - 1$ Factoring Algorithm 316
Chapter 8 Exercises 319
Chapter 8 Computer Implementations and Exercises 325

9 Public Key Cryptography 331
An Informal Analogy for a Public Key Cryptosystem 331
The Quest for Secure Electronic Key Exchange 332
One-Way Functions 333
Review of the Discrete Logarithm Problem 334
The Diffie–Hellman Key Exchange 336
The Quest for a Complete Public Key Cryptosystem 337
The RSA Cryptosystem 338
Digital Signatures and Authentication 343
The ElGamal Cryptosystem 345
Digital Signatures with ElGamal 347
Knapsack Problems 349
The Merkle–Hellman Knapsack Cryptosystem 352
Government Controls on Cryptography 356
A Security Guarantee for RSA 357
Chapter 9 Exercises 360
Chapter 9 Computer Implementations and Exercises 369

10 Finite Fields in General, and $GF(2^8)$ in Particular. 377
Binary Operations 377
Rings 378
Fields 381
$\mathbb{Z}_p[X]$ = the Polynomials with Coefficients in $\mathbb{Z}_p$ 385
Addition and Multiplication of Polynomials in $\mathbb{Z}_p[X]$ 386
Vector Representation of Polynomials 387
$\mathbb{Z}_p[X]$ Is a Ring 388
Divisibility in $\mathbb{Z}_p[X]$ 389
The Division Algorithm for $\mathbb{Z}_p[X]$ 391
Congruences in $\mathbb{Z}_p[X]$ Modulo a Fixed Polynomial 395
Building Finite Fields from $\mathbb{Z}_p[X]$ 396
The Fields GF(2^4) and GF(2^8) 399
The Euclidean Algorithm for Polynomials 404
Chapter 10 Exercises 406
Chapter 10 Computer Implementations and Exercises 411

11 The Advanced Encryption Standard (AES) Protocol 417
An Open Call for a Replacement to DES 417
Nibbles 419
A Scaled-Down Version of AES 421
Decryption in the Scaled-Down Version of AES 429
AES 432
Byte Representation and Arithmetic 432
The AES Encryption Algorithm 435

The AES Decryption Algorithm 439
Security of the AES 440
Chapter 11 Exercises 441
Chapter 11 Computer Implementations and Exercises 445

12 Elliptic Curve Cryptography. 451

Elliptic Curves over the Real Numbers 452
The Addition Operation for Elliptic Curves 454
Groups 458
Elliptic Curves over $\mathbb{Z}_p$ 460
The Variety of Sizes of Modular Elliptic Curves 462
The Addition Operation for Elliptic Curves over $\mathbb{Z}_p$ 463
The Discrete Logarithm Problem on Modular Elliptic Curves 466
An Elliptic Curve Version of the Diffie–Hellman Key Exchange 467
Fast Integer Multiplication of Points on Modular Elliptic Curves 470
Representing Plaintexts on Modular Elliptic Curves 471
An Elliptic Curve Version of the ElGamal Cryptosystem 473
A Factoring Algorithm Based on Elliptic Curves 475
Chapter 12 Exercises 477
Chapter 12 Computer Implementations and Exercises 483

Appendices. 489

Appendix A: Sets and Basic Counting Principles 491

Concepts and Notations for Sets 491
Two Basic Counting Principles 495

Appendix B: Randomness and Probability. 501

Probability Terminology and Axioms 501
Conditional Probability 507
Conditioning and Bayes' Formula 509
Random Variables 511

Appendix C: Solutions to All Exercises for the Reader. 515

Chapter 1: An Overview of the Subject 515
Chapter 2: Divisibility and Modular Arithmetic 517
Chapter 3: The Evolution of Codemaking until the Computer Era 522
Chapter 4: Matrices and the Hill Cryptosystem 526
Chapter 5: The Evolution of Codebreaking until the Computer Era 530
Chapter 6: Representation and Arithmetic of Integers in Different Bases 536
Chapter 7: Block Cryptosystems and the Data Encryption Standard (DES) 540
Chapter 8: Some Number Theory and Algorithms 545
Chapter 9: Public Key Cryptography 550
Chapter 10: Finite Fields in General, and *GF*(2^8) in Particular 554
Chapter 11: The Advanced Encryption Standard (AES) Protocol 560
Chapter 12: Elliptic Curve Cryptography 563

Appendix D: Answers and Brief Solutions to Selected Odd-Numbered Exercises 569

Chapter 1 569
Chapter 2 572
Chapter 3 581
Chapter 4 587
Chapter 5 592
Chapter 6 595
Chapter 7 599
Chapter 8 601
Chapter 9 604
Chapter 10 608
Chapter 11 609
Chapter 12 611

Appendix E: Suggestions for Further Reading 615

Synopsis 615
History of Cryptography 615
Mathematical Foundations 615
Computer Implementations 616
Elliptic Curves 616
Additional Topics in Cryptography 616

References 619

Index of Corollaries, Lemmas, Propositions, and Theories 623

Index of Algorithms 625

Subject Index 627