Table of contents

- **Foreword** (p. ix)
- **Preface** (p. xi)
- **About the Author** (p. xvii)
- **Chapter 1 Aperitifs**
- **1.1 The Lexicon of Cryptography** (p. 1)
- **1.2 Cryptographic Systems** (p. 4)
- **1.3 Cryptanalysis** (p. 4)
- **1.4 Side Information** (p. 6)
- **1.5 Thomas Jefferson and the M-94** (p. 6)
- **1.6 Cryptography and History** (p. 7)
- **1.7 Cryptography and Computers** (p. 8)
- **1.8 The National Security Agency** (p. 9)
- **1.9 The Giants** (p. 10)
- **1.10 No Sex, Money, Crime or...Love** (p. 12)
- **1.11 An Example of the Inference Process in Cryptanalysis** (p. 13)
- **1.12 Warning!** (p. 15)
- **Chapter 2 Columnar Transposition**
- **2.1 Shannon's Classification of Secrecy Transformations** (p. 18)
- **2.2 The Rules of Columnar Transposition Encipherment** (p. 18)
- **2.3 Cribbing** (p. 21)
- **2.4 Examples of Cribbing** (p. 25)
- **2.5 Plaintext Language Models** (p. 30)
- **2.6 Counting k-Grams** (p. 33)
- **2.7 Deriving the Parameters of a Markov Model from Sliding Window Counts** (p. 34)
- **2.8 Markov Scoring** (p. 34)
- **2.9 The ADFGVX Transposition System** (p. 47)
- **2.10 Coda** (p. 49)
- **2.11 Columnar Transposition Problems** (p. 50)
- **Chapter 3 Monoalphabetic Substitution**
- **3.1 Monoalphabetic Substitution** (p. 63)
- **3.2 Caesar's Cipher** (p. 65)
- **3.3 Cribbing Using Isomorphs** (p. 66)
- **3.4 The x[superscript 2]-Test of a Hypothesis** (p. 67)
- **3.5 Pruning from the Table of Isomorphs** (p. 68)
- **3.6 Partial Maximum Likelihood Estimation of a Monoalphabetic Substitution** (p. 73)
- **3.7 The Hidden Markov Model (HMM)** (p. 78)
- **3.8 Hill Encipherment of ASCII N-Grams** (p. 90)
- **3.9 Gaussian Elimination** (p. 102)
- **3.10 Monoalphabetic Substitution Problems** (p. 111)
- **Chapter 4 Polyalphabetic Substitution**
- **4.1 Running Keys** (p. 116)
- **4.2 Blaise de Vigenere** (p. 117)

- **4.3 Gilbert S. Vernam** (p. 117)
- **4.4 The One-Time Pad** (p. 119)
- **4.5 Finding the Key of Vernam-Vigenere Ciphertext with Known Period by Correlation** (p. 120)
- **4.6 Coincidence** (p. 124)
- **4.7 Venona** (p. 127)
- **4.8 Polyalphabetic Substitution Problems** (p. 132)
- **Chapter 5 Statistical Tests**
- **5.1 Weaknesses in a Cryptosystem** (p. 136)
- **5.2 The Kolmogorov-Smirnov Test** (p. 136)
- **5.3 NIST's Proposed Statistical Tests** (p. 138)
- **5.4 Diagnosis** (p. 139)
- **5.5 Statistical Tests Problems** (p. 143)
- **Chapter 6 The Emergence of Cipher Machines**
- **6.1 The Rotor** (p. 150)
- **6.2 Rotor Systems** (p. 152)
- **6.3 Rotor Patents** (p. 153)
- **6.4 A Characteristic Property of Conjugacy** (p. 155)
- **6.5 Analysis of a 1-Rotor System: Ciphertext Only** (p. 156)
- **6.6 The Displacement Sequence of a Permutation** (p. 158)
- **6.7 Arthur Scherbius** (p. 160)
- **6.8 Enigma Key Distribution Protocol** (p. 163)
- **6.9 Cryptanalysis of the Enigma** (p. 166)
- **6.10 Cribbing Enigma Ciphertext** (p. 167)
- **6.11 The Lorenz Schlusselzusatz** (p. 170)
- **6.12 The SZ40 Pin Wheels** (p. 171)
- **6.13 SZ40 Cryptanalysis Problems** (p. 175)
- **6.14 Cribbing SZ40 Ciphertext** (p. 176)
- **Chapter 7 The Japanese Cipher Machines**
- **7.1 Japanese Signaling Conventions** (p. 191)
- **7.2 Half-Rotors** (p. 191)
- **7.3 Components of the RED Machine** (p. 193)
- **7.4 Cribbing RED Ciphertext** (p. 200)
- **7.5 Generalized Vowels and Consonants** (p. 209)
- **7.6 "Climb Mount Itaka" - War!** (p. 210)
- **7.7 Components of the Purple Machine** (p. 211)
- **7.8 The Purple Keys** (p. 217)
- **7.9 Cribbing Purple Finding the V-Stepper** (p. 219)
- **7.10 Cribbing purple Finding the C-Steppers** (p. 238)
- **Chapter 8 Stream Ciphers**
- **8.1 Stream Ciphers** (p. 244)
- **8.2 Feedback Shift Registers** (p. 244)
- **8.3 The Algebra of Polynomials over Z[subscript 2]** (p. 247)
- **8.4 The Characteristic Polynomial of a Linear Feedback Shift Register** (p. 251)
- **8.5 Properties of Maximal Length LFSR Sequences** (p. 254)

- **8.6 Linear Equivalence** (p. 258)
- **8.7 Combining Multiple Linear Feedback Shift Registers** (p. 259)
- **8.8 Matrix Representation of the LFSR** (p. 260)
- **8.9 Cribbing of Stream Enciphered ASCII Plaintext** (p. 261)
- **8.10 Nonlinear Feedback Shift Registers** (p. 271)
- **8.11 Nonlinear Key Stream Generation** (p. 273)
- **8.12 Irregular Clocking** (p. 275)
- **8.13 RC4** (p. 278)
- **8.14 Stream Encipherment Problems** (p. 281)
- **Chapter 9 Block-Ciphers Lucifer, Des, and Aes**
- **9.1 Lucifer** (p. 283)
- **9.2 DES** (p. 288)
- **9.3 The DES S-Boxes, P-Box, and Initial Permutation (IP)** (p. 289)
- **9.4 DES Key Schedule** (p. 292)
- **9.5 Sample DES Encipherment** (p. 294)
- **9.6 Chaining** (p. 295)
- **9.7 Is DES a Random Mapping?** (p. 297)
- **9.8 DES in the Output-Feedback Mode (OFB)** (p. 299)
- **9.9 Cryptanalysis of DES** (p. 300)
- **9.10 Differential Cryptanalysis** (p. 302)
- **9.11 The EFS DES-Cracker** (p. 308)
- **9.12 What Now?** (p. 311)
- **9.13 The Future Advanced Data Encryption Standard** (p. 312)
- **9.14 And the Winner Is!** (p. 312)
- **9.15 The Rijndael Operations** (p. 314)
- **9.16 The Rijndael Cipher** (p. 323)
- **9.17 Rijndael's Strength Propagation of Patterns** (p. 323)
- **9.18 When is a Product Block-Cipher Secure?** (p. 326)
- **9.19 Generating the Symmetric Group** (p. 327)
- **9.20 A Class of Block Ciphers** (p. 329)
- **9.21 The IDEA Block Cipher** (p. 332)
- **Chapter 10 The Paradigm of Public key Cryptography**
- **10.1 In the Beginning...** (p. 334)
- **10.2 Key Distribution** (p. 335)
- **10.3 E-Commerce** (p. 336)
- **10.4 Public-Key Cryptosystems: Easy and Hard Computational Problems** (p. 337)
- **10.5 Do PKCs Solve the Problem of Key Distribution?** (p. 341)
- **10.6 P.S.** (p. 342)
- **Chapter 11 The Knapsack Cryptosystem**
- **11.1 Subset Sum and Knapsack Problems** (p. 344)
- **11.2 Modular Arithmetic and the Euclidean Algorithm** (p. 346)
- **11.3 A Modular Arithmetic Knapsack Problem** (p. 350)
- **11.4 Trap-Door Knapsacks** (p. 350)
- **11.5 Knapsack Encipherment and Decipherment of ASCII-Plaintext** (p. 355)

- **11.6 Cryptanalysis of the Merkle-Hellman Knapsack System (Modular Mapping)** (p. 358)
- **11.7 Diophantine Approximation** (p. 364)
- **11.8 Short Vectors in a Lattice** (p. 368)
- **11.9 Knapsack-Like Cryptosystems** (p. 371)
- **11.10 Knapsack Cryptosystem Problems** (p. 371)
- **Chapter 12 The RSA Cryptosystem**
- **12.1 A Short Number-Theoretic Digression** (p. 376)
- **12.2 RSA** (p. 378)
- **12.3 The RSA Encipherment and Decipherment of ASCII-Plaintext** (p. 379)
- **12.4 Attack on RSA** (p. 382)
- **12.5 Williams Variation of RSA** (p. 383)
- **12.6 Multiprecision Modular Arithmetic** (p. 387)
- **Chapter 13 Prime Numbers and Factorization**
- **13.1 Number Theory and Cryptography** (p. 390)
- **13.2 Prime Numbers and the Sieve of Eratosthenes** (p. 390)
- **13.3 Pollard's p - 1 Method** (p. 391)
- **13.4 Pollard's [rho]-Algorithm** (p. 394)
- **13.5 Quadratic Residues** (p. 396)
- **13.6 Random Factorization** (p. 401)
- **13.7 The Quadratic Sieve (QS)** (p. 403)
- **13.8 Testing if an Integer is a Prime** (p. 405)
- **13.9 The RSA Challenge** (p. 407)
- **13.10 Perfect Numbers and the Mersenne Primes** (p. 408)
- **13.11 Multiprecision Arithmetic** (p. 409)
- **13.12 Prime Number Testing and Factorization Problems** (p. 410)
- **Chapter 14 The Discrete Logarithm Problem**
- **14.1 The Discrete Logarithm Problem Modulo p** (p. 414)
- **14.2 Solution of the DLP Modulo p Given a Factorization of p - 1** (p. 415)
- **14.3 Adelman's Subexponential Algorithm for the Discrete Logarithm Problem** (p. 419)
- **14.4 The Baby-Step, Giant-Step Algorithm** (p. 420)
- **14.5 The Index-Calculus Method** (p. 420)
- **14.6 Pollard's [rho]-Algorithm** (p. 424)
- **14.7 Extension Fields** (p. 426)
- **14.8 The Current State of Discrete Logarithm Research** (p. 428)
- **Chapter 15 Elliptic Curve Cryptography**
- **15.1 Elliptic Curves** (p. 429)
- **15.2 The Elliptic Group over the Reals** (p. 431)
- **15.3 Lenstra's Factorization Algorithm** (p. 432)
- **15.4 The Elliptic Group over Z[subscript p] (p > 3)** (p. 434)
- **15.5 Elliptic Groups over the Field Z[subscript m,2]** (p. 436)
- **15.6 Computations in the Elliptic Group [epsilon][subscript Zm,2](a, b)** (p. 438)
- **15.7 Supersingular Elliptic Curves** (p. 441)
- **15.8 Diffie-Hellman Key Exchange Using an Elliptic Curve** (p. 442)

- **15.9 The Menezes-Vanstone Elliptic Curve Cryptosystem** (p. 443)
- **15.10 The Elliptic Curve Digital Signature Algorithm** (p. 444)
- **15.11 The Certicom Challenge** (p. 445)
- **15.12 NSA and Elliptic Curve Cryptography** (p. 445)
- **Chapter 16 Key Exchange in a Network**
- **16.1 Key Distribution in a Network** (p. 447)
- **16.2 U.S. Patent '770** (p. 448)
- **16.3 Spoofing** (p. 448)
- **16.4 El Gamal's Extension of Diffie-Hellman** (p. 450)
- **16.5 Shamir's Autonomous Key Exchange** (p. 451)
- **16.6 X9.17 Key Exchange Architecture** (p. 453)
- **16.7 The Needham-Schroeder Key Distribution Protocol** (p. 456)
- **Chapter 17 Digital Signatures and Authentication**
- **17.1 The Need for Signatures** (p. 464)
- **17.2 Threats to Network Transactions** (p. 465)
- **17.3 Secrecy, Digital Signatures, and Authentication** (p. 465)
- **17.4 The Desiderata of a Digital Signature** (p. 466)
- **17.5 Public-Key Cryptography and Signature Systems** (p. 467)
- **17.6 Rabin's Quadratic Residue Signature Protocol** (p. 468)
- **17.7 Hash Functions** (p. 470)
- **17.8 MD5** (p. 471)
- **17.9 The Secure Hash Algorithm** (p. 473)
- **17.10 NIST's Digital Signature Algorithm** (p. 474)
- **17.11 El Gamal's Signature Protocol** (p. 475)
- **17.12 The Fiat-Shamir Identification and Signature Schema** (p. 476)
- **17.13 The Oblivious Transfer** (p. 478)
- **Chapter 18 Applications of cryptography**
- **18.1 UNIX Password Encipherment** (p. 480)
- **18.2 Magnetic Stripe Technology** (p. 482)
- **18.3 Protecting ATM Transactions** (p. 484)
- **18.4 Keyed-Access Cards** (p. 491)
- **18.5 Smart Cards** (p. 491)
- **18.6 Who Can You Trust?: Kohnfelder's Certificates** (p. 495)
- **18.7 X.509 Certificates** (p. 495)
- **18.8 The Secure Socket Layer (SSL)** (p. 497)
- **18.9 Making a Secure Credit Card Payment on the Web** (p. 502)
- **Chapter 19 Cryptographic Patents**
- **19.1 What is a Patent?** (p. 506)
- **19.2 Patentability of Ideas** (p. 507)
- **19.3 The Format of a Patent** (p. 507)
- **19.4 Patentable versus Nonpatentable Subjects** (p. 508)
- **19.5 Infringement** (p. 509)
- **19.6 The Role of Patents in Cryptography** (p. 509)
- **19.7 U.S. Patent 3,543,904** (p. 509)
- **19.8 U.S. Patent 4,200,770** (p. 511)
- **19.9 U.S. Patent 4,218,582** (p. 512)

- **19.10 U.S. Patent 4,405,829** (p. 512)
- **19.11 PKS/RSADSI Litigation** (p. 514)
- **19.12 Leon Stambler** (p. 514)
- **Index** (p. 516)