

# ■ ■ ■ CONTENTS ■ ■ ■

*Preface* xi

*Acknowledgments* xiii

## **1** Introduction to Ciphers and Substitution 1

- 1.1 Alice and Bob and Carl and Julius: Terminology and Caesar Cipher 1
- 1.2 The Key to the Matter: Generalizing the Caesar Cipher 4
- 1.3 Multiplicative Ciphers 6
- 1.4 Affine Ciphers 15
- 1.5 Attack at Dawn: Cryptanalysis of Simple Substitution Ciphers 18
- 1.6 Just to Get Up That Hill: Polygraphic Substitution Ciphers 20
- 1.7 Known-Plaintext Attacks 25
- 1.8 Looking Forward 26

## **2** Polyalphabetic Substitution Ciphers 29

- 2.1 Homophonic Ciphers 29
- 2.2 Coincidence or Conspiracy? 31
- 2.3 Alberti Ciphers 36
- 2.4 It's Hip to Be Square: *Tabula Recta* or Vigenère Square Ciphers 39
- 2.5 How Many Is Many? Determining the Number of Alphabets 43
- 2.6 Superman Is Staying for Dinner: Superimposition and Reduction 52
- 2.7 Products of Polyalphabetic Ciphers 55
- 2.8 Pinwheel Machines and Rotor Machines 58
- 2.9 Looking Forward 73

### **3** Transposition Ciphers 75

- 3.1 This Is Sparta! The Scytale 75
- 3.2 Rails and Routes: Geometric Transposition Ciphers 78
- 3.3 Permutations and Permutation Ciphers 81
- 3.4 Permutation Products 86
- 3.5 Keyed Columnar Transposition Ciphers 91

#### **Sidebar 3.1 Functional Nihilism 94**

- 3.6 Determining the Width of the Rectangle 97
- 3.7 Anagramming 101

#### **Sidebar 3.2 But When You Talk about Disruption 104**

- 3.8 Looking Forward 106

### **4** Ciphers and Computers 109

- 4.1 Bringing Home the Bacon: Polyliteral Ciphers and Binary Numerals 109
- 4.2 Fractionating Ciphers 115
- 4.3 How to Design a Digital Cipher: SP-Networks and Feistel Networks 119

#### **Sidebar 4.1 Digitizing Plaintext 125**

- 4.4 The Data Encryption Standard 130
- 4.5 The Advanced Encryption Standard 135
- 4.6 Looking Forward 143

### **5** Stream Ciphers 145

- 5.1 Running-Key Ciphers 145

#### **Sidebar 5.1 We Have All Been Here Before 150**

- 5.2 One-Time Pads 153
- 5.3 Baby You Can Drive My Car: Autokey Ciphers 157
- 5.4 Linear Feedback Shift Registers 167
- 5.5 Adding Nonlinearity to LFSRs 174
- 5.6 Looking Forward 178

### **6** Ciphers Involving Exponentiation 182

- 6.1 Encrypting Using Exponentiation 182
- 6.2 Fermat's Little Theorem 183
- 6.3 Decrypting Using Exponentiation 186
- 6.4 The Discrete Logarithm Problem 188

- 6.5 Composite Moduli 190
- 6.6 The Euler Phi Function 192
- 6.7 Decryption with Composite Moduli 195

**Sidebar 6.1 Fee-fi-fo-fum** 197

- 6.8 Looking Forward 199

## **7 Public-Key Ciphers 201**

- 7.1 Right out in Public: The Idea of Public-Key Ciphers 201
- 7.2 Diffie-Hellman Key Agreement 207
- 7.3 Asymmetric-Key Cryptography 213
- 7.4 RSA 216
- 7.5 Priming the Pump: Primality Testing 222
- 7.6 Why is RSA a (Good) Public-Key System? 226
- 7.7 Cryptanalysis of RSA 229
- 7.8 Looking Forward 233

## **Appendix A The Secret History of Public-Key Cryptography 235**

## **8 Other Public-Key Systems 241**

- 8.1 The Three-Pass Protocol 241
- 8.2 ElGamal 247
- 8.3 Elliptic Curve Cryptography 251
- 8.4 Digital Signatures 265
- 8.5 Looking Forward 271

## **9 The Future of Cryptography 276**

- 9.1 Quantum Computing 276
- 9.2 Postquantum Cryptography 281
- 9.3 Quantum Cryptography 292
- 9.4 Looking Forward 301

*List of Symbols* 303

*Notes* 305

*Suggestions for Further Reading* 345

*Bibliography* 349

*Index* 367