Contents

Preface to the First Edition **ix**

Preface to the Second Edition **xiii**

1 Monoalphabetic Ciphers Using Additive Alphabets **1**
1.1 The Caesar Cipher 1
1.2 Modular arithmetic 3
1.3 Additive alphabets 6
1.4 Solution of additive alphabets 9
1.5 Frequency considerations 12
1.6 Multiplications 17
1.7 Solution of multiplicative alphabets 22
1.8 Affine ciphers 26

2 General Monoalphabetic Substitution **31**
2.1 Mixed alphabets 31
2.2 Solution of mixed alphabet ciphers 34
2.3 Solution of five-letter groupings 40
2.4 Monoalphabets with symbols 47

3 Polyalphabetic Substitution **51**
3.1 Polyalphabetic ciphers 51
3.2 Recognition of polyalphabetic ciphers 54
3.3 Determination of number of alphabets 62
3.4 Solutions of additive subalphabets 66
3.5 Mixed plain sequences 70
3.6 Matching alphabets 73
3.7 Reduction to a monoalphabet 83
3.8 Mixed cipher sequences 84
3.9 General comments 99

4 Polygraphic Systems **103**
4.1 Linear Transformations 103
4.2 Multiplication of matrices—inverses 110
4.3 Involutory transformations 115
4.4 Recognition of digraphic ciphers 118
4.5 Solution of a linear transformation 119
4.6 How to make the Hill System more secure 127

5 Transposition **129**
5.1 Columnar transposition 129
5.2 Completely filled rectangles 135
5.3 Incompletely filled rectangles 138
5.4 Probable word method 140
5.5 General case 145
5.6 Identical length messages 153

6 RSA Encryption **159**
6.1 Public-key encryption 159
6.2 The RSA method 160
6.3 Creating the RSA keys 162
6.4 Why RSA works—Fermat's Little Theorem 163
6.5 Computational considerations 166
6.6 *Maple* and *Mathematica* for RSA 171
6.7 Breaking RSA and signatures 175

7 Perfect Security—One-time Pads **179**
7.1 One-time pads 179
7.2 Pseudo-random number generators 181

Appendix A: Tables **185**

Appendix B: ASCII Codes **191**

Appendix C: Binary Numbers **193**

Solutions to Exercises **197**

Further Readings **205**

Index **207**

About the Authors **211**