

Contents

Preface ix

- 1 Introduction 1
 - Some aspects of secure communication 1
 - Julius Caesar's cipher 2
 - Some basic definitions 3
 - Three stages to decryption: identification, breaking and setting 4
 - Codes and ciphers 5
 - Assessing the strength of a cipher system 7
 - Error detecting and correcting codes 8
 - Other methods of concealing messages 9
 - Modular arithmetic 10
 - Modular addition and subtraction of letters 11
 - Gender 11
 - End matter 12
- 2 From Julius Caesar to simple substitution 13
 - Julius Caesar ciphers and their solution 13
 - Simple substitution ciphers 15
 - How to solve a simple substitution cipher 17
 - Letter frequencies in languages other than English 24
 - How many letters are needed to solve a simple substitution cipher? 26
- 3 Polyalphabetic systems 28
 - Strengthening Julius Caesar: Vigenère ciphers 28
 - How to solve a Vigenère cipher 30
 - Indicators 33
 - Depths 34
 - Recognising 'depths' 34
 - How much text do we need to solve a Vigenère cipher? 37
 - Jefferson's cylinder 37

- 4 Jigsaw ciphers 40
 - Transpositions 40
 - Simple transposition 40
 - Double transposition 44
 - Other forms of transposition 48
 - Assessment of the security of transposition ciphers 51
 - Double encipherment in general 52
- 5 Two-letter ciphers 54
 - Monograph to digraph 54
 - MDTM ciphers 56
 - Digraph to digraph 58
 - Playfair encipherment 59
 - Playfair decipherment 60
 - Cryptanalytic aspects of Playfair 61
 - Double Playfair 61
- 6 Codes 64
 - Characteristics of codes 64
 - One-part and two-part codes 65
 - Code plus additive 67
- 7 Ciphers for spies 72
 - Stencil ciphers 73
 - Book ciphers 75
 - Letter frequencies in book ciphers 79
 - Solving a book cipher 79
 - Indicators 86
 - Disastrous errors in using a book cipher 86
 - 'GARBO's ciphers 88
 - One-time pad 92
- 8 Producing random numbers and letters 94
 - Random sequences 94
 - Producing random sequences 95
 - Coin spinning 95
 - Throwing dice 96
 - Lottery type draws 97
 - Cosmic rays 97
 - Amplifier noise 97
 - Pseudo-random sequences 98
 - Linear recurrences 99
 - Using a binary stream of key for encipherment 100
 - Binary linear sequences as key generators 101

- Cryptanalysis of a linear recurrence 104
- Improving the security of binary keys 104
- Pseudo-random number generators 106
- The mid-square method 106
- Linear congruential generators 107
- 9 The Enigma cipher machine 110
 - Historical background 110
 - The original Enigma 112
 - Encipherment using wired wheels 116
 - Encipherment by the Enigma 118
 - The Enigma plugboard 121
 - The Achilles heel of the Enigma 121
 - The indicator 'chains' in the Enigma 125
 - Aligning the chains 128
 - Identifying R1 and its setting 128
 - Doubly enciphered Enigma messages 132
 - The Abwehr Enigma 132
- 10 The Hagelin cipher machine 133
 - Historical background 133
 - Structure of the Hagelin machine 134
 - Encipherment on the Hagelin 135
 - Choosing the cage for the Hagelin 138
 - The theoretical 'work factor' for the Hagelin 142
 - Solving the Hagelin from a stretch of key 143
 - Additional features of the Hagelin machine 147
 - The slide 147
 - Identifying the slide in a cipher message 148
 - Overlapping 148
 - Solving the Hagelin from cipher texts only 150
- 11 Beyond the Enigma 153
 - The SZ42: a pre-electronic machine 153
 - Description of the SZ42 machine 155
 - Encipherment on the SZ42 155
 - Breaking and setting the SZ42 158
 - Modifications to the SZ42 159
- 12 Public key cryptography 161
 - Historical background 161
 - Security issues 163
 - Protection of programs and data 163
 - Encipherment of programs, data and messages 164

	The key distribution problem	166
	The Diffie–Hellman key exchange system	166
	Strength of the Diffie–Hellman system	168
13	Encipherment and the internet	170
	Generalisation of simple substitution	170
	Factorisation of large integers	171
	The standard method of factorisation	172
	Fermat’s ‘Little Theorem’	174
	The Fermat–Euler Theorem (as needed in the RSA system)	175
	Encipherment and decipherment keys in the RSA system	175
	The encipherment and decipherment processes in the RSA system	178
	How does the key-owner reply to correspondents?	182
	The Data Encryption Standard (DES)	183
	Security of the DES	184
	Chaining	186
	Implementation of the DES	186
	Using both RSA and DES	186
	A salutary note	187
	Beyond the DES	187
	Authentication and signature verification	188
	Elliptic curve cryptography	189
	Appendix	190
	Solutions to problems	218
	<i>References</i>	230
	<i>Name index</i>	235
	<i>Subject index</i>	237