

# Contents

<b>Preface</b>	<b>xi</b>
<b>1 Monoalphabetic Substitution Ciphers</b>	<b>1</b>
1.1 Well-Ordering Axiom, Principle of Mathematical Induction	2
The Well-Ordering Axiom	2
The Principle of Mathematical Induction	3
Exercises 1.1	7
1.2 Prime Numbers, Division Algorithm, Greatest Common Divisor	7
Exercises 1.2	15
1.3 Relatively Prime Integers, Fundamental Theorem of Arithmetic	16
The Fundamental Theorem of Arithmetic	17
Exercises 1.3	18
1.4 Modular Arithmetic	19
Exercises 1.4	26
1.5 Simple Ciphers	27
The Cast of Characters	27
Additive Ciphers	28
Multiplicative Ciphers	30
Affine Ciphers	32
Keyword Ciphers	33
Exercises 1.5	34
	<b>vii</b>

1.6	Cryptanalysis of Monoalphabetic Substitution Ciphers	35
	Exercises 1.6	41
1.7	Personalities	42
<b>2</b>	<b>Polyalphabetic Substitution Ciphers</b>	<b>45</b>
2.1	The Multiplication Principle	46
	Exercises 2.1	50
2.2	Permutations and Combinations	51
	Exercises 2.2	59
2.3	Probability	61
	Some Definitions	62
	Determining the Probability of an Event	63
	Properties of Probability	67
	Exercises 2.3	70
2.4	Independent Events and Expected Number	72
	Independent Events	72
	Expected Number	74
	Exercises 2.4	75
2.5	Disguising the Frequencies	76
	Changing Letters to Numbers	77
	The Vigenère Square	79
	Enciphering a Message Using the Vigenère Square	79
	Deciphering a Message Using the Vigenère Square	81
	Decrypting a Message Using the Vigenère Square	82
	The Friedman Test	86
	Determining the Length of the Keyword	89
	Exercises 2.5	97
2.6	Personalities	99
<b>3</b>	<b>Polygraphic Substitution Ciphers</b>	<b>103</b>
3.1	Elementary Polygraphic Substitution Ciphers	104
	Exercises 3.1	108
3.2	Elementary Matrix Theory	108
	Identities and Inverses	113
	Linear Systems of Equations	116
	Geometrical Transformations	118
	Exercises 3.2	121
3.3	Hill's System	124
	Enciphering and Deciphering a Message Using Hill's System	124
	Cryptanalysis of a Message Enciphered Using Hill's System	128
	Exercises 3.3	137
3.4	Personalities	138

<b>4</b>	<b>Public Key Cryptography</b>	<b>141</b>
4.1	More Number Theory	142
	Exercises 4.1	150
4.2	The RSA Algorithm	150
	Generation of Keys	151
	Exchanging Messages	151
	Frequently Asked Questions	154
	Exercises 4.2	159
4.3	Two Examples	160
	Exercises 4.3	170
4.4	Other Illustrations of Public Key Cryptography	171
	Signature Authentication	171
	Hybrid Systems	172
	Use RSA to Transmit the Key	172
	The Diffie–Hellman Key Exchange System	173
	The Massey–Omura System	174
	Exercises 4.4	177
4.5	Personalities	178
<b>Appendix A</b>	<b>ASCII Code</b>	<b>181</b>
<b>Appendix B</b>	<b>Taxonomy of Cryptology</b>	<b>183</b>
<b>Appendix C</b>	<b>Answers to Even-Numbered Problems</b>	<b>185</b>