

---

# Contents

<b>1</b>	<b>Introduction</b> .....	1
1.1	What Is Randomness and Does There Exist True Randomness? .....	1
1.2	Randomness as a Source of Efficiency – an Exemplary Application .....	5
1.3	Concept of the Book .....	11
1.4	To the Student .....	14
1.5	To the Teacher .....	16
<b>2</b>	<b>Fundamentals</b> .....	19
2.1	Objectives .....	19
2.2	Elementary Probability Theory .....	20
2.3	Models of Randomized Algorithms .....	37
2.4	Classification of Randomized Algorithms .....	51
2.5	Classification of Randomized Algorithms for Optimization Problems .....	72
2.6	Paradigms of the Design of Randomized Algorithms .....	87
2.7	Summary .....	96
<b>3</b>	<b>Foiling the Adversary</b> .....	101
3.1	Objectives .....	101
3.2	Hashing .....	102
3.3	Universal Hashing .....	109
3.4	Online Algorithms .....	116
3.5	Randomized Online Algorithms .....	120
3.6	Summary .....	128
<b>4</b>	<b>Fingerprinting</b> .....	131
4.1	Objectives .....	131
4.2	Communication Protocols .....	133
4.3	The Substring Problem .....	139

4.4	Verification of Matrix Multiplication .....	141
4.5	Equivalence of Two Polynomials .....	144
4.6	Summary .....	149
<b>5</b>	<b>Success Amplification and Random Sampling .....</b>	<b>153</b>
5.1	Objectives .....	153
5.2	Efficient Amplification by Repeating Critical Computation Parts .....	154
5.3	Repeated Random Sampling and Satisfiability .....	166
5.4	Random Sampling and Generating Quadratic Nonresidues .....	174
5.5	Summary .....	181
<b>6</b>	<b>Abundance of Witnesses .....</b>	<b>183</b>
6.1	Objectives .....	183
6.2	Searching for Witnesses for Primality Testing .....	184
6.3	Solovay-Strassen Algorithm for Primality Testing .....	192
6.4	Generation of Random Primes .....	202
6.5	Summary .....	206
<b>7</b>	<b>Optimization and Random Rounding .....</b>	<b>209</b>
7.1	Objectives .....	209
7.2	Relaxation to Linear Programming .....	210
7.3	Random Rounding and MAX-SAT .....	216
7.4	Combining Random Sampling and Random Rounding .....	222
7.5	Summary .....	225
<b>A</b>	<b>Fundamentals of Mathematics .....</b>	<b>227</b>
A.1	Objectives .....	227
A.2	Algebra and Number Theory .....	228
A.3	Combinatorics .....	256
A.4	Summary .....	264
	<b>References .....</b>	<b>267</b>
	<b>Index .....</b>	<b>271</b>