
Inhaltsverzeichnis

Vorwort	VII
1 Einladung zur Kryptokomplexität	1
2 Grundlagen der Informatik und Mathematik	11
2.1 Algorithmen: Der Euklidische Algorithmus	11
2.2 Formale Sprachen und Berechenbarkeitstheorie	19
2.3 Logik	33
2.3.1 Aussagenlogik	33
2.3.2 Prädikatenlogik	39
2.4 Algebra, Zahlentheorie und Graphentheorie	43
2.4.1 Algebra und Zahlentheorie	43
2.4.2 Permutationsgruppen	48
2.4.3 Graphentheorie	49
2.5 Wahrscheinlichkeitstheorie	52
2.6 Übungen und Probleme	54
2.7 Zusammenfassung und bibliographische Notizen	58
3 Grundlagen der Komplexitätstheorie	61
3.1 Aufgaben und Ziele der Komplexitätstheorie	61
3.2 Komplexitätsmaße und -klassen	64
3.3 Beschleunigungs-, Kompressions- und Hierarchiesätze	72
3.4 Zwischen Logarithmischem und Polynomialem Raum	82
3.5 Reduzierbarkeiten und Vollständigkeit	88
3.5.1 Many-One-Reduzierbarkeiten, Härte und Vollständigkeit ...	88
3.5.2 NL-Vollständigkeit	93
3.5.3 NP-Vollständigkeit	100
3.6 Innerhalb von NP	120
3.6.1 P versus NP und das Graphisomorphie-Problem	120
3.6.2 Die Berman–Hartmanis-Isomorphievermutung und Einwegfunktionen	122

3.7	Übungen und Probleme	129
3.8	Zusammenfassung und bibliographische Notizen	136
4	Grundlagen der Kryptologie	145
4.1	Aufgaben und Ziele der Kryptologie	145
4.2	Einige klassische Kryptosysteme und ihre Kryptoanalyse	148
4.2.1	Substitutions- und Permutationschiffren	149
4.2.2	Affin-lineare Blockchiffren	155
4.2.3	Block- und Stromchiffren	165
4.3	Perfekte Geheimhaltung	172
4.3.1	Satz von Shannon und Vernams One-Time Pad	172
4.3.2	Entropie und Schlüsselmehrdeutigkeit	177
4.4	Übungen und Probleme	183
4.5	Zusammenfassung und bibliographische Notizen	190
5	Hierarchien über NP	195
5.1	Die boolesche Hierarchie über NP	196
5.2	Die Polynomialzeit-Hierarchie	215
5.3	Paralleler Zugriff auf NP	227
5.3.1	Eine kurze Abschweifung in die Theorie der Wahlsysteme ..	233
5.3.2	Gewinnerproblem für Young-Wahlen	235
5.4	Frage-Hierarchien über NP	239
5.5	Die boolesche Hierarchie kollabiert die Polynomialzeit-Hierarchie ..	245
5.6	Alternierende Turingmaschinen	249
5.7	Die Low- und die High-Hierarchie in NP	261
5.8	Übungen und Probleme	271
5.9	Zusammenfassung und bibliographische Notizen	278
6	Randomisierte Algorithmen und Komplexitätsklassen	293
6.1	Das Erfüllbarkeitsproblem der Aussagenlogik	294
6.1.1	Deterministische Zeitkomplexität	296
6.1.2	Probabilistische Zeitkomplexität	297
6.2	Probabilistische Polynomialzeit-Klassen	302
6.2.1	PP, RP und ZPP: Monte-Carlo- und Las-Vegas-Algorithmen	302
6.2.2	BPP: Probabilistische Polynomialzeit mit beschränktem Fehler	310
6.3	Quantoren und Arthur-Merlin-Spiele	314
6.3.1	Quantoren und BPP	314
6.3.2	Die Arthur-Merlin-Hierarchie	321
6.4	Zählklassen	326
6.5	Graphisomorphie und Lowness	330
6.5.1	Graphisomorphie ist in der Low-Hierarchie	330
6.5.2	Graphisomorphie ist in SPP	334
6.6	Übungen und Probleme	338
6.7	Zusammenfassung und bibliographische Notizen	343

7	RSA-Kryptosystem, Primzahltests und das Faktorisierungsproblem	349
7.1	RSA	350
7.1.1	Das RSA Public-Key-Kryptosystem	350
7.1.2	Digitale Signaturen mit RSA	355
7.2	Primzahltests	355
7.2.1	Fermat-Test	358
7.2.2	Miller–Rabin-Test	362
7.2.3	Solovay–Strassen-Test	368
7.2.4	Das Primzahl-Problem ist in P	374
7.3	Das Faktorisierungsproblem	375
7.3.1	Probedivision	376
7.3.2	Pollards Algorithmus	377
7.3.3	Das quadratische Sieb	378
7.3.4	Andere Faktorisierungsmethoden	383
7.4	Sicherheit von RSA: Angriffe und Gegenmaßnahmen	386
7.5	Übungen und Probleme	395
7.6	Zusammenfassung und bibliographische Notizen	399
8	Weitere Public-Key-Kryptosysteme und Protokolle	403
8.1	Diffie–Hellman und das Problem des diskreten Logarithmus	404
8.1.1	Das Schlüsseltausch-Protokoll von Diffie und Hellman	405
8.1.2	Diskrete Logarithmen und das Diffie–Hellman-Problem	408
8.2	Die Protokolle von ElGamal	412
8.2.1	ElGamals Public-Key-Kryptosystem	412
8.2.2	Digitale Signaturen mit ElGamal	414
8.2.3	Sicherheit der Protokolle von ElGamal	416
8.3	Rabins Public-Key-Kryptosystem	424
8.3.1	Rabins Kryptosystem	425
8.3.2	Sicherheit des Systems von Rabin	427
8.4	Arthur-Merlin-Spiele und Zero-Knowledge	430
8.5	Das Public-Key-Kryptosystem von Merkle und Hellman	439
8.6	Die Protokolle von Rabin, Rivest und Sherman	442
8.7	Übungen und Probleme	450
8.8	Zusammenfassung und bibliographische Notizen	456
	Tabellenverzeichnis	463
	Abbildungsverzeichnis	465
	Literaturverzeichnis	467
	Sach- und Autorenverzeichnis	497