

Inhaltsverzeichnis

1. Ganze Zahlen	1
1.1 Grundlagen	1
1.2 Teilbarkeit	2
1.3 Darstellung ganzer Zahlen	3
1.4 O - und Ω -Notation	5
1.5 Aufwand von Addition, Multiplikation und Division mit Rest	5
1.6 Polynomzeit	7
1.7 Größter gemeinsamer Teiler	7
1.8 Euklidischer Algorithmus	10
1.9 Erweiterter euklidischer Algorithmus	13
1.10 Analyse des erweiterten euklidischen Algorithmus	15
1.11 Zerlegung in Primzahlen	18
1.12 Übungen	20
2. Kongruenzen und Restklassenringe	23
2.1 Kongruenzen	23
2.2 Halbgruppen	25
2.3 Gruppen	27
2.4 Restklassenring	27
2.5 Körper	28
2.6 Division im Restklassenring	29
2.7 Rechenzeit für die Operationen im Restklassenring	30
2.8 Die prime Restklassengruppe	31
2.9 Ordnung von Gruppenelementen	32
2.10 Untergruppen	34
2.11 Der kleine Satz von Fermat	35
2.12 Schnelle Exponentiation	36
2.13 Schnelle Auswertung von Potenzprodukten	38
2.14 Berechnung von Elementordnungen	40
2.15 Der Chinesische Restsatz	41
2.16 Zerlegung des Restklassenrings	44
2.17 Bestimmung der Eulerschen φ -Funktion	45
2.18 Polynome	46
2.19 Polynome über Körpern	48

2.20	Struktur der Einheitengruppe endlicher Körper	50
2.21	Struktur der primen Restklassengruppe nach einer Primzahl	51
2.22	Übungen	52
3.	Verschlüsselung	55
3.1	Verschlüsselungsverfahren	55
3.2	Symmetrische und asymmetrische Kryptosysteme	56
3.3	Kryptoanalyse	57
3.4	Alphabete und Wörter	58
3.5	Permutationen	61
3.6	Blockchiffren	62
3.7	Mehrfachverschlüsselung	63
3.8	Verwendung von Blockchiffren	63
3.8.1	ECB-Mode	64
3.8.2	CBC-Mode	65
3.8.3	CFB-Mode	68
3.8.4	OFB-Mode	70
3.9	Stromchiffren	72
3.10	Die affine Chiffre	73
3.11	Matrizen und lineare Abbildungen	74
3.11.1	Matrizen über Ringen	75
3.11.2	Produkt von Matrizen mit Vektoren	75
3.11.3	Summe und Produkt von Matrizen	75
3.11.4	Der Matrizenring	76
3.11.5	Determinante	76
3.11.6	Inverse von Matrizen	77
3.11.7	Affin lineare Funktionen	78
3.12	Affin lineare Blockchiffren	79
3.13	Vigenère-, Hill- und Permutationschiffre	79
3.14	Kryptoanalyse affin linearer Blockchiffren	80
3.15	Übungen	81
4.	Wahrscheinlichkeit und perfekte Sicherheit	83
4.1	Wahrscheinlichkeit	83
4.2	Bedingte Wahrscheinlichkeit	84
4.3	Geburtstagsparadox	85
4.4	Perfekte Sicherheit	87
4.5	Das Vernam-One-Time-Pad	89
4.6	Zufallszahlen	90
4.7	Pseudozufallszahlen	90
4.8	Übungen	90

- 5. Der DES-Algorithmus** 93
 - 5.1 Feistel-Chiffren 93
 - 5.2 Der DES-Algorithmus 94
 - 5.2.1 Klartext- und Schlüsselraum 94
 - 5.2.2 Die initiale Permutation 95
 - 5.2.3 Die interne Blockchiffre 96
 - 5.2.4 Die S-Boxen 97
 - 5.2.5 Die Rundenschlüssel 97
 - 5.2.6 Entschlüsselung 99
 - 5.3 Ein Beispiel für DES 100
 - 5.4 Sicherheit des DES 101
 - 5.5 Übungen 102

- 6. Primzahlerzeugung** 103
 - 6.1 Probedivision 103
 - 6.2 Der Fermat-Test 104
 - 6.3 Carmichael-Zahlen 105
 - 6.4 Der Miller-Rabin-Test 106
 - 6.5 Zufällige Wahl von Primzahlen 110
 - 6.6 Übungen 110

- 7. Public-Key Verschlüsselung** 111
 - 7.1 Die Idee 111
 - 7.2 Das RSA-Verfahren 112
 - 7.2.1 Schlüsselerzeugung 113
 - 7.2.2 Verschlüsselung 113
 - 7.2.3 Entschlüsselung 115
 - 7.2.4 Sicherheit des geheimen Schlüssels 116
 - 7.2.5 RSA und Faktorisierung 118
 - 7.2.6 Wahl von p und q 119
 - 7.2.7 Auswahl von e und d 119
 - 7.2.8 Effizienz 120
 - 7.2.9 Multiplikativität 122
 - 7.2.10 Verallgemeinerung 122
 - 7.3 Das Rabin-Verschlüsselungsverfahren 123
 - 7.3.1 Schlüsselerzeugung 123
 - 7.3.2 Verschlüsselung 124
 - 7.3.3 Entschlüsselung 124
 - 7.3.4 Effizienz 125
 - 7.3.5 Sicherheit 125
 - 7.3.6 Eine Chosen Ciphertext-Attacke 126
 - 7.4 Diffie-Hellman-Schlüsselaustausch 127
 - 7.4.1 Diskrete Logarithmen 127
 - 7.4.2 Schlüsselaustausch 128

7.4.3	Sicherheit	129
7.4.4	Andere Gruppen	130
7.5	Das ElGamal-Verschlüsselungsverfahren	130
7.5.1	Schlüsselerzeugung	130
7.5.2	Verschlüsselung	131
7.5.3	Entschlüsselung	131
7.5.4	Effizienz	131
7.5.5	ElGamal und Diffie-Hellman	132
7.5.6	Parameterwahl	132
7.5.7	ElGamal als randomisiertes Verschlüsselungsverfahren	133
7.5.8	Verallgemeinerung	133
7.6	Übungen	134
8.	Faktorisierung	137
8.1	Probedivision	137
8.2	Die $p - 1$ -Methode	138
8.3	Das Quadratische Sieb	138
8.3.1	Das Prinzip	139
8.3.2	Bestimmung von x und y	139
8.3.3	Auswahl geeigneter Kongruenzen	140
8.3.4	Das Sieb	141
8.4	Analyse des Quadratischen Siebs	143
8.5	Effizienz anderer Faktorisierungsverfahren	146
8.6	Übungen	146
9.	Diskrete Logarithmen	149
9.1	Das DL-Problem	149
9.2	Enumeration	150
9.3	Shanks Babystep-Giantstep-Algorithmus	150
9.4	Der Pollard- ρ -Algorithmus	152
9.5	Der Pohlig-Hellman-Algorithmus	155
9.5.1	Reduktion auf Primzahlpotenzordnung	156
9.5.2	Reduktion auf Primzahlordnung	157
9.5.3	Gesamtalgorithmus und Analyse	159
9.6	Index-Calculus	159
9.6.1	Idee	160
9.6.2	Diskrete Logarithmen der Faktorbasiselemente	161
9.6.3	Individuelle Logarithmen	162
9.6.4	Analyse	163
9.7	Andere Algorithmen	163
9.8	Verallgemeinerung des Index-Calculus-Verfahrens	163
9.9	Übungen	164

10. Kryptographische Hashfunktionen	165
10.1 Hashfunktionen und Kompressionsfunktionen	165
10.2 Geburtstagsattacke	167
10.3 Kompressionsfunktionen aus Verschlüsselungsfunktionen	168
10.4 Hashfunktionen aus Kompressionsfunktionen	169
10.5 Effiziente Hashfunktionen	171
10.6 Eine arithmetische Kompressionsfunktion	172
10.7 Message Authentication Codes	173
10.8 Übungen	174
11. Digitale Signaturen	175
11.1 Idee	175
11.2 RSA-Signaturen	176
11.2.1 Schlüsselerzeugung	176
11.2.2 Erzeugung der Signatur	176
11.2.3 Verifikation	177
11.2.4 Angriffe	177
11.2.5 Signatur von Texten mit Redundanz	178
11.2.6 Signatur mit Hashwert	179
11.2.7 Wahl von p und q	180
11.3 Signaturen aus Public-Key-Verfahren	180
11.4 ElGamal-Signatur	180
11.4.1 Schlüsselerzeugung	181
11.4.2 Erzeugung der Signatur	181
11.4.3 Verifikation	181
11.4.4 Die Wahl von p	182
11.4.5 Die Wahl von k	183
11.4.6 Existentielle Fälschung	183
11.4.7 Effizienz	184
11.4.8 Verallgemeinerung	185
11.5 Der Digital Signature Algorithm (DSA)	185
11.5.1 Schlüsselerzeugung	185
11.5.2 Erzeugung der Signatur	186
11.5.3 Verifikation	186
11.5.4 Effizienz	187
11.5.5 Sicherheit	187
11.6 Übungen	188
12. Andere Gruppen	189
12.1 Endliche Körper	189
12.1.1 Konstruktion	189
12.1.2 DL-Problem	190
12.2 Elliptische Kurven	191
12.2.1 Definition	191

12.2.2	Gruppenstruktur	192
12.2.3	Kryptographisch sichere Kurven	193
12.2.4	Vorteile von EC-Kryptographie	194
12.3	Quadratische Formen	194
12.4	Übungen	195
13.	Identifikation	197
13.1	Paßwörter	197
13.2	Einmal-Paßwörter	199
13.3	Challenge-Response-Identifikation	199
13.3.1	Verwendung von symmetrischer Kryptographie	199
13.3.2	Verwendung von Public-Key-Kryptographie	200
13.3.3	Zero-Knowledge-Beweise	200
13.4	Übungen	202
14.	Public-Key-Infrastrukturen	205
14.1	Persönliche Sicherheitsumgebung	205
14.1.1	Bedeutung	205
14.1.2	Implementierung	206
14.1.3	Darstellungsproblem	206
14.2	Zertifizierungsstellen	207
14.2.1	Registrierung	207
14.2.2	Schlüsselerzeugung	207
14.2.3	Zertifizierung	208
14.2.4	Archivierung	208
14.2.5	Personalisierung des PSE	209
14.2.6	Verzeichnisdienst	209
14.2.7	Schlüssel-Update	210
14.2.8	Rückruf von Zertifikaten	210
14.2.9	Zugriff auf ungültige Schlüssel	210
14.3	Zertifikatsketten	211
	Lösungen der Übungsaufgaben	213
	Literaturverzeichnis	225
	Sachverzeichnis	227