



Johannes Buchmann

Einführung in die Kryptographie

Dritte, erweiterte Auflage



Springer



Inhaltsverzeichnis

1. Einleitung	1
2. Ganze Zahlen	3
2.1 Grundlagen	3
2.2 Teilbarkeit	4
2.3 Darstellung ganzer Zahlen	5
2.4 O - und Ω -Notation	7
2.5 Aufwand von Addition, Multiplikation und Division mit Rest	8
2.6 Polynomzeit	9
2.7 Größter gemeinsamer Teiler	9
2.8 Euklidischer Algorithmus	12
2.9 Erweiterter euklidischer Algorithmus	15
2.10 Analyse des erweiterten euklidischen Algorithmus	16
2.11 Zerlegung in Primzahlen	20
2.12 Übungen	22
3. Kongruenzen und Restklassenringe	25
3.1 Kongruenzen	25
3.2 Halbgruppen	27
3.3 Gruppen	29
3.4 Restklassenringe	29
3.5 Körper	30
3.6 Division im Restklassenring	31
3.7 Rechenzeit für die Operationen im Restklassenring	32
3.8 Prime Restklassengruppen	33
3.9 Ordnung von Gruppenelementen	34
3.10 Untergruppen	36
3.11 Der kleine Satz von Fermat	37
3.12 Schnelle Exponentiation	38
3.13 Schnelle Auswertung von Potenzprodukten	40
3.14 Berechnung von Elementordnungen	41
3.15 Der Chinesische Restsatz	43
3.16 Zerlegung des Restklassenrings	45
3.17 Bestimmung der Eulerschen φ -Funktion	46

3.18	Polynome	47
3.19	Polynome über Körpern	49
3.20	Konstruktion endlicher Körper	51
3.21	Struktur der Einheitengruppe endlicher Körper	54
3.22	Struktur der primen Restklassengruppe nach einer Primzahl .	55
3.23	Übungen	56
4.	Verschlüsselung	59
4.1	Verschlüsselungsverfahren	59
4.2	Private-Key-Verfahren und Public-Key-Verfahren	60
4.3	Sicherheit	61
4.3.1	Typen von Attacken	61
4.3.2	Randomisierte Verschlüsselung	63
4.3.3	Mathematische Modellierung	64
4.4	Alphabete und Wörter	64
4.5	Permutationen	66
4.6	Blockchiffren	68
4.7	Mehrfachverschlüsselung	69
4.8	Verschlüsselungsmodi	69
4.8.1	ECB-Mode	69
4.8.2	CBC-Mode	71
4.8.3	CFB-Mode	74
4.8.4	OFB-Mode	76
4.9	Stromchiffren	77
4.10	Die affine Chiffre	79
4.11	Matrizen und lineare Abbildungen	80
4.11.1	Matrizen über Ringen	80
4.11.2	Produkt von Matrizen mit Vektoren	81
4.11.3	Summe und Produkt von Matrizen	81
4.11.4	Der Matrizenring	81
4.11.5	Determinante	82
4.11.6	Inverse von Matrizen	82
4.11.7	Affin lineare Funktionen	83
4.12	Affin lineare Blockchiffren	84
4.13	Vigenère-, Hill- und Permutationschiffre	85
4.14	Kryptoanalyse affin linearer Blockchiffren	85
4.15	Sichere Blockchiffren	87
4.15.1	Konfusion und Diffusion	87
4.15.2	Exhaustive Key Search	87
4.15.3	Time-Memory Trade-Off	88
4.15.4	Differentielle Kryptoanalyse	89
4.16	Übungen	90





5. Wahrscheinlichkeit und perfekte Geheimhaltung	93
5.1 Wahrscheinlichkeit	93
5.2 Bedingte Wahrscheinlichkeit	94
5.3 Geburtstagsparadox	95
5.4 Perfekte Geheimhaltung	97
5.5 Das Vernam-One-Time-Pad	99
5.6 Zufallszahlen	100
5.7 Pseudozufallszahlen	101
5.8 Übungen	101
6. Der DES-Algorithmus	103
6.1 Feistel-Chiffren	103
6.2 Der DES-Algorithmus	104
6.2.1 Klartext- und Schlüsselraum	104
6.2.2 Die initiale Permutation	105
6.2.3 Die interne Blockchiffre	106
6.2.4 Die S-Boxen	107
6.2.5 Die Rundenschlüssel	107
6.2.6 Entschlüsselung	109
6.3 Ein Beispiel für DES	110
6.4 Sicherheit des DES	111
6.5 Übungen	112
7. Der AES-Verschlüsselungsalgorithmus	113
7.1 Bezeichnungen	113
7.2 Cipher	114
7.2.1 Identifikation der Bytes mit Elementen von $GF(2^8)$	115
7.2.2 SubBytes	115
7.2.3 ShiftRows	116
7.2.4 MixColumns	117
7.2.5 AddRoundKey	117
7.3 KeyExpansion	118
7.4 Ein Beispiel	119
7.5 InvCipher	120
7.6 Übungen	120
8. Primzahlerzeugung	123
8.1 Probedivision	123
8.2 Der Fermat-Test	125
8.3 Carmichael-Zahlen	125
8.4 Der Miller-Rabin-Test	127
8.5 Zufällige Wahl von Primzahlen	130
8.6 Übungen	130

9. Public-Key Verschlüsselung	133
9.1 Idee	133
9.2 Sicherheit	134
9.2.1 Sicherheit des privaten Schlüssels	135
9.2.2 Semantische Sicherheit	135
9.2.3 Adaptive-Chosen-Ciphertext-Sicherheit	136
9.2.4 Sicherheitsbeweise	137
9.3 Das RSA-Verfahren	137
9.3.1 Schlüsselerzeugung	137
9.3.2 Verschlüsselung	138
9.3.3 Entschlüsselung	139
9.3.4 Sicherheit des geheimen Schlüssels	140
9.3.5 RSA und Faktorisierung	143
9.3.6 Auswahl von p und q	143
9.3.7 Auswahl von e	143
9.3.8 Auswahl von d	145
9.3.9 Effizienz	145
9.3.10 Multiplikativität	146
9.3.11 Sichere Verwendung	147
9.3.12 Verallgemeinerung	148
9.4 Das Rabin-Verschlüsselungsverfahren	148
9.4.1 Schlüsselerzeugung	149
9.4.2 Verschlüsselung	149
9.4.3 Entschlüsselung	149
9.4.4 Effizienz	151
9.4.5 Sicherheit gegen Ciphertext-Only-Angriffe	151
9.4.6 Eine Chosen Ciphertext-Attacke	152
9.4.7 Sichere Verwendung	152
9.5 Diffie-Hellman-Schlüsselaustausch	153
9.5.1 Diskrete Logarithmen	153
9.5.2 Schlüsselaustausch	154
9.5.3 Sicherheit	155
9.5.4 Andere Gruppen	155
9.6 Das ElGamal-Verschlüsselungsverfahren	156
9.6.1 Schlüsselerzeugung	156
9.6.2 Verschlüsselung	156
9.6.3 Entschlüsselung	157
9.6.4 Effizienz	157
9.6.5 ElGamal und Diffie-Hellman	158
9.6.6 Parameterwahl	158
9.6.7 ElGamal ist randomisiert	159
9.6.8 Verallgemeinerung	159
9.7 Übungen	160



10. Faktorisierung	163
10.1 Probedivision	163
10.2 Die $p - 1$ -Methode	164
10.3 Das Quadratische Sieb	164
10.3.1 Das Prinzip	165
10.3.2 Bestimmung von x und y	165
10.3.3 Auswahl geeigneter Kongruenzen	166
10.3.4 Das Sieb	167
10.4 Analyse des Quadratischen Siebs	169
10.5 Effizienz anderer Faktorisierungsverfahren	171
10.6 Übungen	173
11. Diskrete Logarithmen	175
11.1 Das DL-Problem	175
11.2 Enumeration	176
11.3 Shanks Babystep-Giantstep-Algorithmus	176
11.4 Der Pollard- ρ -Algorithmus	178
11.5 Der Pohlig-Hellman-Algorithmus	181
11.5.1 Reduktion auf Primzahlpotenzordnung	182
11.5.2 Reduktion auf Primzahlordnung	183
11.5.3 Gesamtalgorithmus und Analyse	185
11.6 Index-Calculus	185
11.6.1 Idee	186
11.6.2 Diskrete Logarithmen der Faktorbasiselemente	186
11.6.3 Individuelle Logarithmen	188
11.6.4 Analyse	188
11.7 Andere Algorithmen	189
11.8 Verallgemeinerung des Index-Calculus-Verfahrens	189
11.9 Übungen	190
12. Kryptographische Hashfunktionen	191
12.1 Hashfunktionen und Kompressionsfunktionen	191
12.2 Geburtstagsattacke	193
12.3 Kompressionsfunktionen aus Verschlüsselungsfunktionen	194
12.4 Hashfunktionen aus Kompressionsfunktionen	195
12.5 SHA-1	197
12.6 Andere Hashfunktionen	199
12.7 Eine arithmetische Kompressionsfunktion	199
12.8 Message Authentication Codes	200
12.9 Übungen	201

13. Digitale Signaturen	203
13.1 Idee	203
13.2 Sicherheit	204
13.2.1 Sicherheit des privaten Schlüssels	204
13.2.2 No-Message-Attacks	204
13.2.3 Adaptive-Chosen-Message-Attacks	205
13.3 RSA-Signaturen	206
13.3.1 Schlüsselerzeugung	206
13.3.2 Erzeugung der Signatur	206
13.3.3 Verifikation	206
13.3.4 Angriffe	207
13.3.5 Signatur von Texten mit Redundanz	208
13.3.6 Signatur mit Hashwert	209
13.3.7 Wahl von p und q	210
13.3.8 Sichere Verwendung	210
13.4 Signaturen aus Public-Key-Verfahren	210
13.5 ElGamal-Signatur	210
13.5.1 Schlüsselerzeugung	211
13.5.2 Erzeugung der Signatur	211
13.5.3 Verifikation	211
13.5.4 Die Wahl von p	212
13.5.5 Die Wahl von k	213
13.5.6 Existentielle Fälschung	213
13.5.7 Effizienz	214
13.5.8 Sichere Verwendung	215
13.5.9 Verallgemeinerung	215
13.6 Der Digital Signature Algorithm (DSA)	215
13.6.1 Schlüsselerzeugung	215
13.6.2 Erzeugung der Signatur	216
13.6.3 Verifikation	216
13.6.4 Effizienz	217
13.6.5 Sicherheit	217
13.7 Übungen	218
14. Andere Gruppen	221
14.1 Endliche Körper	221
14.2 Elliptische Kurven	221
14.2.1 Definition	222
14.2.2 Gruppenstruktur	223
14.2.3 Kryptographisch sichere Kurven	223
14.2.4 Vorteile von EC-Kryptographie	224
14.3 Quadratische Formen	225
14.4 Übungen	225



15. Identifikation	227
15.1 Anwendungen	227
15.2 Paßwörter	228
15.3 Einmal-Paßwörter	229
15.4 Challenge-Response-Identifikation	229
15.4.1 Verwendung von symmetrischer Kryptographie	229
15.4.2 Verwendung von Public-Key-Kryptographie	230
15.4.3 Zero-Knowledge-Beweise	230
15.5 Übungen	233
16. Secret Sharing	235
16.1 Prinzip	235
16.2 Das Shamir-Secret-Sharing-Protokoll	235
16.2.1 Initialisierung	236
16.2.2 Verteilung der Geheimnisteile	236
16.2.3 Rekonstruktion des Geheimnisses	237
16.2.4 Sicherheit	238
16.3 Übungen	238
17. Public-Key-Infrastrukturen	239
17.1 Persönliche Sicherheitsumgebung	239
17.1.1 Bedeutung	239
17.1.2 Implementierung	240
17.1.3 Darstellungsproblem	240
17.2 Zertifizierungsstellen	241
17.2.1 Registrierung	241
17.2.2 Schlüsselerzeugung	241
17.2.3 Zertifizierung	242
17.2.4 Archivierung	242
17.2.5 Personalisierung des PSE	243
17.2.6 Verzeichnisdienst	243
17.2.7 Schlüssel-Update	244
17.2.8 Rückruf von Zertifikaten	244
17.2.9 Zugriff auf ungültige Schlüssel	244
17.3 Zertifikatsketten	245
Lösungen der Übungsaufgaben	247
Literaturverzeichnis	259
Sachverzeichnis	263