

Inhalt

Teil 1: Arithmetik und Zahlentheorie in C++

1	Einleitung	3
2	Das Zahlformat – die Darstellung großer Zahlen in C	11
3	Schnittstellensemantik.	15
4	Die Grundrechenarten	17
4.1	Addition und Subtraktion	18
4.2	Multiplikation	27
4.2.1	Die Schulmethode	28
4.2.2	Quadrieren geht schneller.	33
4.2.3	Noch schneller mit Karatsuba?	38
4.3	Division mit Rest.	43
5	Modulare Arithmetik – Rechnen mit Restklassen	57
6	Wo alles zusammenkommt: Modulare Potenzierung	69
6.1	Erste Ansätze.	69
6.2	<i>M</i> -äre Potenzierung.	74
6.3	Additionsketten und Fenster.	88
6.4	Montgomery-Reduktion und Potenzierung.	92
6.5	Kryptographische Anwendung der Potenzierung.	105
7	Bitweise und logische Funktionen	111
7.1	Shift-Operationen	111
7.2	ALLES ODER NICHTS: Bitweise Verknüpfungen	117
7.3	Direkter Zugriff auf einzelne Binärstellen	121
7.4	Vergleichsoperationen	124
8	Eingabe, Ausgabe, Zuweisung, Konvertierung	129
9	Dynamische Register	139
10	Zahlentheoretische Grundfunktionen.	147
10.1	Größter gemeinsamer Teiler.	148
10.2	Multiplikative Inverse in Restklassenringen	155
10.3	Wurzel und Logarithmus	162
10.4	Quadratwurzeln in Restklassenringen	168
10.4.1	Das Jacobi-Symbol.	169
10.4.2	Quadratwurzeln modulo p^k	176
10.4.3	Quadratwurzeln modulo n	181
10.4.4	Kryptographie mit quadratischen Resten.	189
10.5	Ein Primzahltest	192
11	Große Zufallszahlen.	209

12	Testen: Münchhausen lässt grüßen	221
12.1	Statische Analyse.	224
12.2	Tests zur Laufzeit	226

Teil 2: Arithmetik und Kryptographie in C++

13	Klasse, mit C++ ist alles viel einfacher...	235
13.1	Not a public affair: Die Zahldarstellung in LINT.	240
13.2	Konstruktoren	241
13.3	Überladene Operatoren	244
14	Das LINT-Public-Interface: Members and Friends	253
14.1	Arithmetik	253
14.2	Zahlentheorie.	261
14.3	Stream-I/O von LINT-Objekten.	264
14.3.1	Formatierte Ausgabe von LINT-Objekten	266
14.3.2	Manipulatoren	273
14.3.3	File-I/O von LINT-Objekten	276
15	Fehlerbehandlung.	281
15.1	(don't) panic	281
15.2	Benutzerdefinierte Fehlerbehandlung	283
15.3	Ausnahmezustand: LINT-Exceptions	285
16	Ein Anwendungsbeispiel: Das RSA-Verfahren	291
16.1	Asymmetrische Kryptosysteme	291
16.2	Der RSA-Algorithmus	294
16.3	Digitale RSA-Signaturen	307
16.4	RSA-Klassen in C++	315
17	Do it yourself: Test LINT	323
18	Ansätze zum weiteren Ausbau.	327
19	<i>Rijndael</i> – Nachfolger für den DES	329
19.1	Arithmetik mit Polynomen	331
19.2	Der Rijndael-Algorithmus.	335
19.3	Berechnung der Rundenschlüssel	337
19.4	Die S-Box	339
19.5	Die ShiftRow-Transformation.	341
19.6	Die MixColumn-Transformation	342
19.7	Der AddRoundKey-Schritt	342
19.8	Die Verschlüsselung im Gesamtablauf.	343
19.9	Die Entschlüsselung	346
20	Nachwort.	351

Teil 3: Anhänge

Anhang A: Verzeichnis der C-Funktionen	354
Anhang B: Verzeichnis der C++-Funktionen	363
Anhang C: Die Makros	379
Anhang D: Rechenzeiten	385
Anhang E: Notationen	389
Anhang F: Arithmetik- und Zahlentheoriepakete	391
Literaturverzeichnis	393