

Michael Welschenbach

Kryptographie in C und C++

Zahlentheoretische Grundlagen,
Computer-Arithmetik mit großen Zahlen,
kryptographische Tools



Springer

Inhalt

Teil 1: Arithmetik und Zahlentheorie in C

| | | |
|--------|---|-----|
| 1 | Einleitung | 3 |
| 2 | Das Zahlformat – die Darstellung großer Zahlen in C | 9 |
| 3 | Schnittstellensemantik | 13 |
| 4 | Die Grundrechenarten | 15 |
| 4.1 | Addition und Subtraktion | 16 |
| 4.2 | Multiplikation | 25 |
| 4.3 | Quadrieren geht schneller | 34 |
| 4.4 | Division mit Rest | 38 |
| 5 | Modulare Arithmetik – Das Rechnen mit Restklassen | 53 |
| 6 | Wo alles zusammenkommt: Modulare Potenzierung | 65 |
| 7 | Bitweise und logische Funktionen | 99 |
| 7.1 | Shift-Operationen | 99 |
| 7.2 | ALLES ODER NICHTS: Bitweise Verknüpfungen | 105 |
| 7.3 | Direkter Zugriff auf einzelne Binärstellen | 109 |
| 7.4 | Vergleichsoperationen | 112 |
| 8 | Eingabe, Ausgabe, Zuweisung, Konvertierung | 117 |
| 9 | Dynamische Register | 125 |
| 10 | Zahlentheoretische Grundfunktionen | 133 |
| 10.1 | Größter gemeinsamer Teiler | 134 |
| 10.2 | Multiplikative Inverse in Restklassenringen | 140 |
| 10.3 | Wurzel und Logarithmus | 147 |
| 10.4 | Quadratwurzeln in Restklassenringen | 151 |
| 10.4.1 | Das Jacobi-Symbol | 152 |
| 10.4.2 | Quadratwurzeln modulo p^k | 158 |
| 10.4.3 | Quadratwurzeln modulo n | 164 |
| 10.5 | Ein Primzahltest | 174 |
| 11 | Große Zufallszahlen | 191 |
| 12 | Testen: Münchhausen läßt grüßen | 203 |
| 12.1 | Statische Analyse | 206 |
| 12.2 | Tests zur Laufzeit | 208 |

Teil 2: Arithmetik in C++ mit der Klasse LINT

| | | |
|--------|--|-----|
| 13 | Klasse, mit C++ ist alles viel einfacher... | 219 |
| 13.1 | Not a public affair: Die Zahldarstellung in LINT | 224 |
| 13.2 | Konstruktoren | 225 |
| 13.3 | Überladene Operatoren | 228 |
| 14 | Das LINT-Public-Interface: Members und Friends | 237 |
| 14.1 | Arithmetik | 237 |
| 14.2 | Zahlentheorie | 245 |
| 14.3 | Stream-I/O von LINT-Objekten | 248 |
| 14.3.1 | Formatierte Ausgabe von LINT-Objekten | 250 |
| 14.3.2 | Manipulatoren | 257 |
| 14.3.3 | File-I/O von LINT-Objekten | 260 |
| 15 | Fehlerbehandlung | 265 |
| 15.1 | (don't) panic... | 265 |
| 15.2 | Benutzerdefinierte Fehlerbehandlung | 267 |
| 15.3 | Ausnahmestand: LINT-Exceptions | 269 |
| 16 | Ein Anwendungsbeispiel: Digitale RSA-Signaturen | 275 |
| 17 | Do it yourself: Test LINT | 293 |
| 18 | Ansätze zum weiteren Ausbau | 297 |
| 19 | Nachwort | 299 |
| | Literaturverzeichnis | 301 |
| | Anhang A: Verzeichnis der C-Funktionen | 305 |
| | Anhang B: Die Makros | 313 |
| | Anhang C: Rechenzeiten | 319 |
| | Anhang D: Notationen | 321 |
| | Index | 323 |