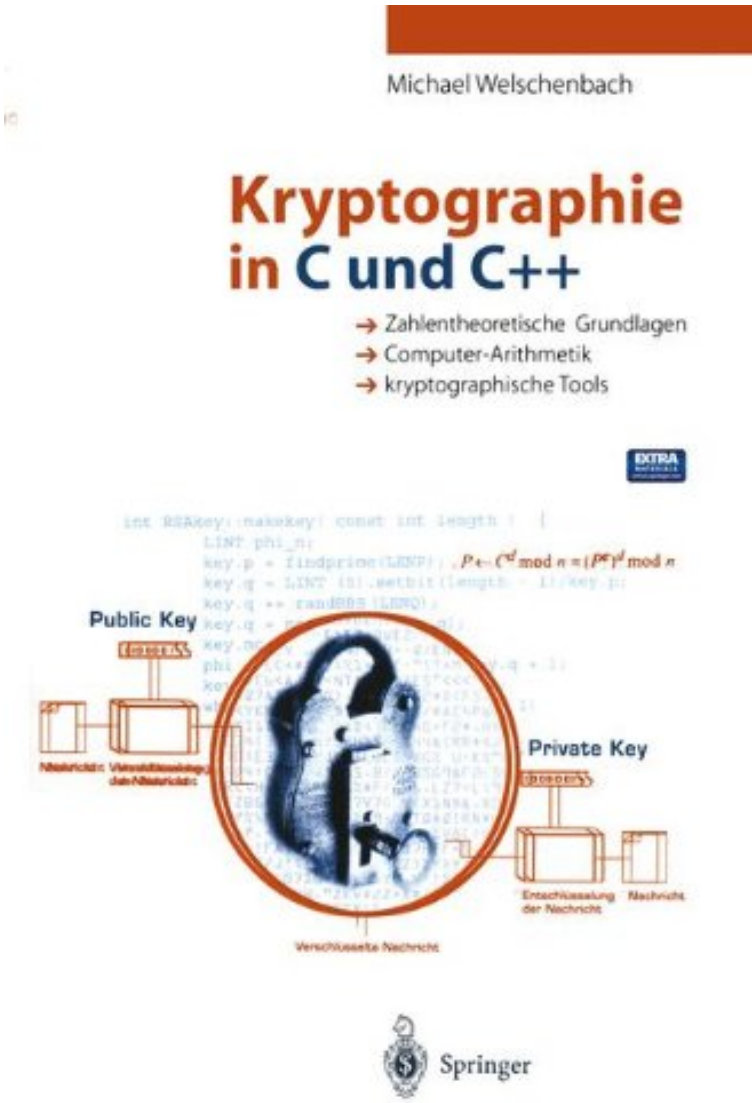
Kryptographie in C und C++: Zahlentheoretische Grundlagen, Computer-Arithmetik mit groen Zahlen, kryptographische Tools

Von Michael Welschenbach
*ePub | *DOC | audiobook | ebooks | Download PDF*



Produktinformation -Verkaufsrang: #3363158 in BcherVerffentlicht am: 1998-05-15Abmessungen: .0 x .0b x .0l, .0 Pfund Einband: Taschenbuch329 Seiten | File size: 16.Mb

Von Michael Welschenbach : Kryptographie in C und C++: Zahlentheoretische Grundlagen, Computer-Arithmetik mit groen Zahlen, kryptographische Tools before purchasing it in order to gage whether or not it would be worth my time, and all praised Kryptographie in C und C++: Zahlentheoretische Grundlagen, Computer-Arithmetik mit groen Zahlen, kryptographische Tools:

KundenrezensionenHilfreichste Kundenrezensionen17 von 17 Kunden fanden die folgende Rezension hilfreich. Kryptographie - praxisnah, hintergrndig und effizientVon Ein KundeDas Buch "Kryptographie in C und C++" von Michael Welschenbach stellt ein uerst praxisnahes Werk zum Thema Kryptographie dar. Es besticht durch seine hervorragende Mischung aus zahlentheoretischen Grundlagen und ihrer programmtechnischen Umsetzung. Abgerundet wird das Ganze durch die im Sourcecode beiliegenden Funktionsbibliotheken in C und C++, die zum einen Basisbausteine fr die Implementierung kryptographischer Verfahren und zum anderen eine hierauf aufbauende RSA-Implementierung enthalten.Das Buch bietet einem interessierten "Neuling" einen umfassenden Einblick in die Programmierung kryptographischer Verfahren. Dem "Fortgeschrittenen" erffnen die einzelnen Kapitel tiefgreifende Einblicke in theoretische Hintergrnde und deren Auswirkungen auf die effiziente Gestaltung relevanter Algorithmen. Aus dem Blickwinkel der Lehre ist das Buch sowohl fr Autodidakten als auch als Grundlage fr die Vermittlung von Inhalten zum Thema Kryptographie bestens geeignet. Einige Grnde hierfr seien im folgenden genannt: Der Autor baut sein Buch methodisch und didaktisch geschickt auf, so da die theoretischen Grundlagen nicht "vom Himmel fallen", sondern durch ihre Notwendigkeit fr die Implementierung kryptographischer Verfahren klug motiviert werden. Der Autor liefert neben C-Code auch eine Implementierung in C++ und hebt bei dieser Gelegenheit auch die Vorzge des objektorientierten Ansatzes hervor. Die Zeitmessungen und Performance-Aussagen runden das Bild ab. Insgesamt liefert der Autor mit seinem Sourcecode Material, das sich fr den flexiblen und vielfltigen Einsatz in Forschung und Lehre problemlos eignet. Die explizite Aufforderung des Autors zur Weiterentwicklung seiner Programme, seine Hinweise auf Stellen, an denen sich potentiell die besten Verbesserungschancen bieten sowie insgesamt sein den Leser mit einbeziehender Schreibstil motivieren stets zum Mit- und Weiterdenken. Wohltuend auflockernd wirken dabei zu Beginn eines jeden Kapitels passende Zitate aus den unterschiedlichsten Quellen: von Goethe ber Erich Kstner bis hin zu Lego-Katalogen und den legendren Janosch-Figuren.Bei Betrachtung aller genannten (und nicht genannten) Qualitten des Buches bleibt nur zu hoffen, da der Autor die Zeit und Geduld aufzubringen vermag, die aus seiner stndigen Beschftigung mit dem Thema Kryptographie entspringenden Erfahrungen und Ideen in einer weiteren Auflage seines Buches an die interessierte Leserschaft weiterzugeben. Eine Implementierung der vorgestellten Algorithmen in Java knnte dabei die flexiblen Einsatzmglichkeiten der Software noch weiter steigern.5 von 5 Kunden fanden die folgende Rezension hilfreich. Kryptographie - wie es *wirklich* gehtVon Ein KundeDieses Buch ist in jeder Hinsicht auesserst empfehlenswert. Anders als alle anderen auf dem Markt befindlichen Buecher ueber Kryptographie begnuegt es sich nicht damit, die mathematischen Grundlagen der gaengigsten Verschluesselungsverfahren zu entwickeln und dann die doch recht komplexen Algorithmen in Pseudo-Code darzustellen. Vielmehr stellt es ganz im Sinne des "Literarischen Programmierens" die Algorithmen Zeile fuer Zeile in lauffaehigem C/C++ dar und erklaert, warum man es genau so tun sollte und nicht anders. Daher ist es auch aus programmiertechnischer Sicht interessant. Der vorgestellte Code ist von hoechster Qualitaet und dabei (trotzdem!) didaktisch hervorragend aufbereitet. Eine grosse Leistung! Auch wer noch nie eine groessere Klassenbibliothek entwickelt oder studiert hat, kann hier gutes OOD und durchdachtes Software-Engineering an einem konkreten Beispiel realisiert sehen. Wer bis ins Detail wissen will oder muss, was softwaremaessig *wirklich* hinter Schlagwoerten wie RSA, Diffie-Hellmann und Public-Key-Kryptographie steht, dem sei dieses Buch ans Herz gelegt.3 von 21 Kunden fanden die folgende Rezension hilfreich. Fr kommerzielle Nutzer uninteressantVon Ein KundeDas Buch an sich ist sehr gut. Nur leider erlaubt der Autor fr die Software, die ja der eigentliche Gegenstand des Buches ist und deren Entstehung besprochen wird, nur eine nicht-kommerzielle Nutzung. Wer also vorhat, die Software kommerziell einzusetzen, sollte mglicherweise vor dem Kauf mit dem Autor Rcksprache halten, was das Buch *wirklich* kostet.

KurzbeschreibungIn dem nun vorliegenden Buch wird ein Programmpaket entwickelt, das dem Bedarf an leistungsfhigen Erweiterungen der Programmiersprachen C und C++ fr Berechnungen mit groen Zahlen vollauf gengt. Es prsentiert Funktionen und Methoden, die hinsichtlich theoretischer Fundierung, Stabilitt und Performanz professionellen Ansprchen gengt. Deren Anwendung wird an einer objektorientierten Implementierung des RSA-Kryptosystems demonstriert.Die beiliegende CD-ROM bietet den Lesern, denen es primr um den praktischen Einsatz der Programmfunktionen geht, eine stabile Plattform fr eigene Anwendungen.AutorenkommentarKurzbeschreibungKryptographie in C und C++ bietet einen umfassenden Einstieg in die Realisierung moderner Public Key-Kryptosysteme. Es werden Funktionen fr die Arithmetik mit groen Zahlen, modulare Arithmetik, ggT, jacobi-Symbol, Wurzeln in endlichen Ringen, Lsung linearer Kongruenzensysteme und Chinesischer Restsatz, Erzeugung kryptographisch starker Zufallszahlen, Primzahltests u. a. entwickelt und auf einer beiliegenden CDROM bereitgestellt. Schnelle Assembler-Routinen fuer die Multiplikation und Division sind ebenfalls enthalten. Hierauf aufbauend wird eine C++-Klasse konstruiert, die die Darstellung groer Zahlen und die Algorithmen fr ihre Verarbeitung integriert. Die Anwendung der Methoden wird an einer Implementierung des RSA-Verfahrens nach objektorientierten Prinzipien demonstriert. Das Buch erlutert in klarer Form die mathematischen Grundlagen

aller Programmfunktionen und vermittelt so zwischen Theorie und Praxis.BuchrckseiteDas Buch bietet einen umfassenden berblick ber die Grundlagen moderner kryptographischer Verfahren. Der Autor stellt ausfhrlich deren programmtechnische Umsetzung dar, indem er ein Programmpaket als leistungsfhige Erweiterung der Programmiersprachen C und C++ fr Berechnungen mit groen Zahlen entwickelt. Das Buch prsentiert Funktionen und Methoden, die hinsichtlich theoretischer Fundierung, Stabilitt und Performanz professionellen Ansprchen gengen. Deren Anwendung wird an einer objektorientierten Implementierung des RSA-Kryptosystems demonstriert. Die beiliegende CD-ROM bietet den Leserinnen und Lesern, denen es primr um den praktischen Einsatz der Programmfunktionen geht, einen gut sortierten Baukasten fr eigene Anwendungen. Michael Welschenbach, Jahrgang 1956, hat Mathematik an der Universitt Kln studiert. Er leitet den Projektbereich Sichere Systeme bei debis Systemhaus Information Security Services GmbH in Bonn. Er beschftigt sich seit dem Studium mit theoretischen und praktischen Aspekten der Kryptographie; sein besonderes Interesse gilt dabei den Fragen der Implementierung.