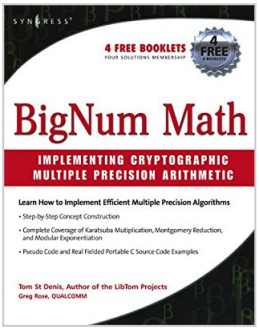

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic

By Tom St Denis

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic
By Tom St Denis

Implementing cryptography requires integers of significant magnitude to resist cryptanalytic attacks. Modern programming languages only provide support for integers which are relatively small and single precision. The purpose of this text is to instruct the reader regarding how to implement efficient multiple precision algorithms.

Bignum math is the backbone of modern computer security algorithms. It is the ability to work with hundred-digit numbers efficiently using techniques that are both elegant and occasionally bizarre. This book introduces the reader to the concept of bignum algorithms and proceeds to build an entire library of functionality from the ground up. Through the use of theory, pseudo-code and actual fielded C source code the book explains each and every algorithm that goes into a modern bignum library. Excellent for the student as a learning tool and practitioner as a reference alike BigNum Math is for anyone with a background in computer science who has taken introductory level mathematic courses. The text is for students learning mathematics and cryptography as well as the practioner who needs a reference for any of the algorithms documented within.

* Complete coverage of Karatsuba Multiplication, the Barrett Algorithm, Toom-Cook 3-Way Multiplication, and More

* Tom St Denis is the developer of the industry standard cryptographic suite of tools called LibTom.

* This book provides step-by-step exercises to enforce concepts

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic

By Tom St Denis

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis

Implementing cryptography requires integers of significant magnitude to resist cryptanalytic attacks. Modern programming languages only provide support for integers which are relatively small and single precision. The purpose of this text is to instruct the reader regarding how to implement efficient multiple precision algorithms.

Bignum math is the backbone of modern computer security algorithms. It is the ability to work with hundred-digit numbers efficiently using techniques that are both elegant and occasionally bizarre. This book introduces the reader to the concept of bignum algorithms and proceeds to build an entire library of functionality from the ground up. Through the use of theory, pseudo-code and actual fielded C source code the book explains each and every algorithm that goes into a modern bignum library. Excellent for the student as a learning tool and practitioner as a reference alike BigNum Math is for anyone with a background in computer science who has taken introductory level mathematic courses. The text is for students learning mathematics and cryptography as well as the practioner who needs a reference for any of the algorithms documented within.

* Complete coverage of Karatsuba Multiplication, the Barrett Algorithm, Toom-Cook 3-Way Multiplication, and More

* Tom St Denis is the developer of the industry standard cryptographic suite of tools called LibTom.

* This book provides step-by-step exercises to enforce concepts

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis Bibliography

- Rank: #2677920 in eBooks
- Published on: 2006-08-18
- Released on: 2006-08-18
- Format: Kindle eBook

Editorial Review

About the Author
Tom St Denis is the author of the industry standard LibTom series of projects. Tom is a senior software developer and cryptographer for the Advanced Micro Devices Corporation. He has been engaged in various international development contracts and speaking engagements since 2004. He is at work on his next book, Cryptography for Developers.

Users Review

From reader reviews:

Stan Whitley:

With other case, little men and women like to read book BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic. You can choose the best book if you like reading a book. Given that we know about how is important any book BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic. You can add knowledge and of course you can around the world by way of a book. Absolutely right, because from book you can realize everything! From your country until foreign or abroad you will be known. About simple point until wonderful thing you are able to know that. In this era, we can easily open a book or perhaps searching by internet system. It is called e-book. You should use it when you feel fed up to go to the library. Let's read.

Monte Lawson:

Book is to be different for each and every grade. Book for children until finally adult are different content. As we know that book is very important for all of us. The book BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic seemed to be making you to know about other information and of course you can take more information. It is rather advantages for you. The e-book BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic is not only giving you far more new information but also to be your friend when you feel bored. You can spend your own personal spend time to read your reserve. Try to make relationship with the book BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic. You never truly feel lose out for everything should you read some books.

Jeffery Bruce:

This BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic is great book for you because the content which is full of information for you who all always deal with world and possess to make decision every minute. This specific book reveal it info accurately using great manage word or we can point out no rambling sentences included. So if you are read it hurriedly you can have whole data in it. Doesn't mean it only provides straight forward sentences but tough core information with splendid delivering sentences. Having BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic in your hand like having the world in your arm, data in it is not ridiculous 1. We can say that no guide that offer you world

in ten or fifteen moment right but this book already do that. So , this is good reading book. Hey Mr. and Mrs. active do you still doubt in which?

Anna Rangel:

What is your hobby? Have you heard which question when you got students? We believe that that question was given by teacher to the students. Many kinds of hobby, All people has different hobby. So you know that little person including reading or as reading become their hobby. You should know that reading is very important and book as to be the issue. Book is important thing to add you knowledge, except your personal teacher or lecturer. You discover good news or update with regards to something by book. A substantial number of sorts of books that can you go onto be your object. One of them is BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic.

Read BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis for online ebook

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis books to read online.

Online BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis ebook PDF download

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis Doc

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis Mobipocket

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic By Tom St Denis EPub