1.

Record Nr.	UNISALENTO991003251509707536
Autore	St. Denis, Tom.
Titolo	BigNum math [electronic resource] : implementing cryptographic multiple precision arithmetic / Tom St. Denis, Greg Rose
Pubbl/distr/stampa	Rockland, MA : Syngress Pub., c2006.
ISBN	9781597491129 1597491128
Descrizione fisica	xviii, 296 p. ; 23 cm.
Altri autori (Persone)	Rose, Greg.author
Disciplina	519.7
Soggetti	Programming (Mathematics) Computer security Electronic books.
Lingua di pubblicazione	Inglese
Formato	Risorsa elettronica
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references (p. 289-290) and index.
Nota di contenuto	Introduction; Multiple Precision Arithmetic; Exercises; Portability and Stability; Getting Started; Maintenance Algorithms; Basic Operations; Sign Manipulation; Basic Arithmetic; Multiplication and Squaring; The Multipliers; Multiplication; Modular Reduction; Basics of Modular Reduction; Exponentiation; Exponentiation Basics; Higher Level Algorithms; Number Theoretic Algorithms.
Sommario/riassunto	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.