

1. Record Nr.	UNINA9910450905103321
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 Publishing, c2006
ISBN	1-281-03573-4 9786611035730 0-08-048838-2 1-59749-124-1
Edizione	[1st edition]
Descrizione fisica	1 online resource (316 p.)
Altri autori (Persone)	RoseGreg
Disciplina	519.7
Soggetti	Programming (Mathematics) Computer security Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references (p. 289-290) and index.
Nota di contenuto	Cover; Contents; List of Figures; Preface; Chapter 1 Introduction; Chapter 2 Getting Started; Chapter 3 Basic Operations; Chapter 4 Basic Arithmetic; Chapter 5 Multiplication and Squaring; Chapter 6 Modular Reduction; Chapter 7 Exponentiation; Chapter 8 Higher Level Algorithms; Chapter 9 Number Theoretic Algorithms; Bibliography; Index
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 algor