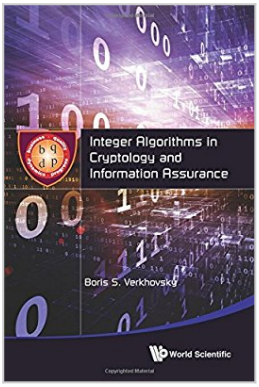


# Integer Algorithms in Cryptology and Information Assurance

*By Boris S Verkhovsky*



**Integer Algorithms in Cryptology and Information Assurance** By Boris S Verkhovsky

**Integer Algorithms in Cryptology and Information Assurance** is a collection of the author's own innovative approaches in algorithms and protocols for secret and reliable communication. It concentrates on the "what" and "how" behind implementing the proposed cryptographic algorithms rather than on formal proofs of "why" these algorithms work.

The book consists of five parts (in 28 chapters) and describes the author's research results in:

- Innovative methods in cryptography (secret communication between initiated parties);
- Cryptanalysis (how to break the encryption algorithms based on computational complexity of integer factorization and discrete logarithm problems);
- How to provide a reliable transmission of information via unreliable communication channels and;
- How to exploit a synergetic effect that stems from combining the cryptographic and information assurance protocols.This text contains innovative cryptographic algorithms; computationally efficient algorithms for information assurance; new methods to solve the classical problem of integer factorization, which plays a key role in cryptanalysis; and numerous illustrative examples and tables that facilitate the understanding of the proposed algorithms.
  The fundamental ideas contained within are *not* based on temporary advances in technology, which might become obsolete in several years. The problems addressed in the book have their own intrinsic computational complexities, and the ideas and methods described in the book will remain important for years to come.Readership: Integer Algorithms in Cryptology and Information Assurance would be a book of interest for researchers and developers working on telecommunication security and/or reliability, in industries such as business and banking, national security agencies, militaries, interplanetary space exploration, and telemedicine. Faculty members in Computer Science, Electrical Engineering, Information Technology, Bio-Engineering and Applied Mathematics Departments, who are planning to teach advanced courses in cryptography; graduate and PhD students; advanced undergraduate students of

the same fields; and various national cryptographic societies would also find this book useful.

# Integer Algorithms in Cryptology and Information Assurance

*By Boris S Verkhovsky*

**Integer Algorithms in Cryptology and Information Assurance** By Boris S Verkhovsky

**Integer Algorithms in Cryptology and Information Assurance** is a collection of the author's own innovative approaches in algorithms and protocols for secret and reliable communication. It concentrates on the "what" and "how" behind implementing the proposed cryptographic algorithms rather than on formal proofs of "why" these algorithms work.

The book consists of five parts (in 28 chapters) and describes the author's research results in:

- Innovative methods in cryptography (secret communication between initiated parties);
- Cryptanalysis (how to break the encryption algorithms based on computational complexity of integer factorization and discrete logarithm problems);
- How to provide a reliable transmission of information via unreliable communication channels and;
- How to exploit a synergetic effect that stems from combining the cryptographic and information assurance protocols.This text contains innovative cryptographic algorithms; computationally efficient algorithms for information assurance; new methods to solve the classical problem of integer factorization, which plays a key role in cryptanalysis; and numerous illustrative examples and tables that facilitate the understanding of the proposed algorithms.
  The fundamental ideas contained within are *not* based on temporary advances in technology, which might become obsolete in several years. The problems addressed in the book have their own intrinsic computational complexities, and the ideas and methods described in the book will remain important for years to come.Readership: Integer Algorithms in Cryptology and Information Assurance would be a book of interest for researchers and developers working on telecommunication security and/or reliability, in industries such as business and banking, national security agencies, militaries, interplanetary space exploration, and telemedicine. Faculty members in Computer Science, Electrical Engineering, Information Technology, Bio-Engineering and Applied Mathematics Departments, who are planning to teach advanced courses in cryptography; graduate and PhD students; advanced undergraduate students of the same fields; and various national cryptographic societies would also find this book useful.

**Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky Bibliography**

- Sales Rank: #2632358 in Books
- Published on: 2014-10-29
- Released on: 2014-09-05
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.04" w x 6.00" l, .0 pounds
- Binding: Hardcover
- 460 pages

## Editorial Review

From the Inside Flap
Integer Algorithms in Cryptology and Information Assurance is a collection of the author's own innovative approaches in algorithms and protocols for secret and reliable communication. It concentrates on the "what" and "how" behind implementing the proposed cryptographic algorithms rather than on formal proofs of "why" these algorithms work.

The book consists of five parts (in 28 chapters) and describes the author's research results in:

Innovative methods in cryptography (secret communication between initiated parties);

Cryptanalysis (how to break the encryption algorithms based on computational complexity of integer factorization and discrete logarithm problems);

How to provide a reliable transmission of information via unreliable communication channels and;

How to exploit a synergetic effect that stems from combining the cryptographic and information assurance protocols.

This text contains innovative cryptographic algorithms; computationally efficient algorithms for information assurance; new methods to solve the classical problem of integer factorization, which plays a key role in cryptanalysis; and numerous illustrative examples and tables that facilitate the understanding of the proposed algorithms.

The fundamental ideas contained within are not based on temporary advances in technology, which might become obsolete in several years. The problems addressed in the book have their own intrinsic computational complexities, and the ideas and methods described in the book will remain important for years to come.

About the Author
**Dr Boris S Verkhovsky** (8 Oct 1933 - 24 Aug 2014) was a Professor of Computer Science at the New Jersey Institute of Technology (NJIT). He received his PhD in Computer Science jointly from the Academy of Sciences of the USSR and the Latvia State University, Riga.

Professor Verkhovsky's research experience and interests spanned across communication security, design and analysis of cryptosystems and information assurance protocols, the design and control of large-scale systems, optimization and algorithms, and the design and control of telecommunication networks.

His prior affiliations are: the Scientific Research Institute of Computers (Moscow), the Academy of Sciences of the USSR, Princeton University School of Engineering, IBM Thomas J Watson Research Center (Yorktown Heights), Bell Laboratories, University of Colorado and, since 1986, the NJIT.

Professor Verkhovsky was a recipient of awards including the USSR Ministry of Radio-Electronics Award; the Academy of Sciences of the USSR Award; the Alvin Johnson Award; and the Millennium Award and the Medal of Excellence. Professor Verkhovsky was also a recipient of the Blasé Pascal Award and Medal, and was listed in Marquis' *Who's Who in America* up till his passing.

Verkhovsky was the Wallace J Eckert Scientist at the IBM Thomas J Watson Research Center, a Member of Technical Staff at Bell Labs, and held the Charles Dana Endowed Chair Professorship. In 2002 he was elected as a member, and in 2003, as a Fellow of the European Academy of Science (EAS). He served as the EAS's Vice President from 2003 till 2006.

## Users Review

**From reader reviews:**

**Lisa Bates:**

Hey guys, do you wishes to finds a new book to learn? May be the book with the name Integer Algorithms in Cryptology and Information Assurance suitable to you? The particular book was written by popular writer in this era. The particular book untitled Integer Algorithms in Cryptology and Information Assuranceis the main one of several books this everyone read now. This specific book was inspired a lot of people in the world. When you read this guide you will enter the new age that you ever know prior to. The author explained their idea in the simple way, thus all of people can easily to know the core of this reserve. This book will give you a great deal of information about this world now. In order to see the represented of the world on this book.

**Homer Simon:**

Playing with family in a very park, coming to see the ocean world or hanging out with close friends is thing that usually you have done when you have spare time, then why you don't try thing that really opposite from that. One particular activity that make you not experience tired but still relaxing, trilling like on roller coaster you already been ride on and with addition associated with. Even you love Integer Algorithms in Cryptology and Information Assurance, you may enjoy both. It is great combination right, you still would like to miss it? What kind of hang-out type is it? Oh can occur its mind hangout guys. What? Still don't have it, oh come on its identified as reading friends.

**Lisa Martin:**

Is it a person who having spare time and then spend it whole day by watching television programs or just lying down on the bed? Do you need something new? This Integer Algorithms in Cryptology and Information Assurance can be the respond to, oh how comes? A fresh book you know. You are so out of date, spending your time by reading in this brand new era is common not a nerd activity. So what these textbooks have than the others?

**Della Ferguson:**

Do you like reading a reserve? Confuse to looking for your selected book? Or your book ended up being rare? Why so many concern for the book? But almost any people feel that they enjoy with regard to reading. Some people likes looking at, not only science book but additionally novel and Integer Algorithms in Cryptology and Information Assurance or even others sources were given expertise for you. After you know how the great a book, you feel would like to read more and more. Science publication was created for teacher

or perhaps students especially. Those textbooks are helping them to include their knowledge. In different case, beside science guide, any other book likes Integer Algorithms in Cryptology and Information Assurance to make your spare time more colorful. Many types of book like here.

# Read Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky for online ebook

Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky 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 Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky books to read online.

## Online Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky ebook PDF download

### Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky Doc

**Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky Mobipocket**

**Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky EPub**

**RF8LK0QU4NM: Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky**