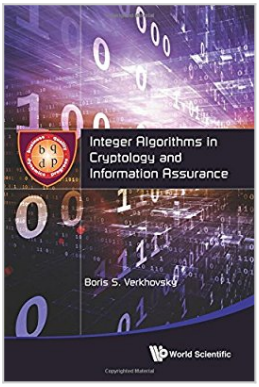

Integer Algorithms in Cryptology and Information Assurance

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:

Tommy Heckman:

As people who live in the actual modest era should be up-date about what going on or info even knowledge to make these people keep up with the era and that is always change and move ahead. Some of you maybe may update themselves by looking at books. It is a good choice for yourself but the problems coming to anyone is you don't know what kind you should start with. This Integer Algorithms in Cryptology and Information Assurance is our recommendation so you keep up with the world. Why, because book serves what you want and want in this era.

Barbara Corbin:

This book untitled Integer Algorithms in Cryptology and Information Assurance to be one of several books which best seller in this year, that is because when you read this book you can get a lot of benefit upon it. You will easily to buy this kind of book in the book retail outlet or you can order it by using online. The publisher in this book sells the e-book too. It makes you more readily to read this book, as you can read this book in your Smartphone. So there is no reason to you personally to past this reserve from your list.

Michael Earl:

The book with title Integer Algorithms in Cryptology and Information Assurance posesses a lot of information that you can study it. You can get a lot of profit after read this book. This book exist new understanding the information that exist in this reserve represented the condition of the world at this point. That is important to yo7u to find out how the improvement of the world. That book will bring you throughout new era of the glowbal growth. You can read the e-book in your smart phone, so you can read that anywhere you want.

Joyce Pippin:

Beside this specific Integer Algorithms in Cryptology and Information Assurance in your phone, it may give you a way to get more close to the new knowledge or data. The information and the knowledge you will got here is fresh from oven so don't always be worry if you feel like an old people live in narrow community. It is good thing to have Integer Algorithms in Cryptology and Information Assurance because this book offers for you readable information. Do you occasionally have book but you do not get what it's facts concerning. Oh come on, that would not happen if you have this in the hand. The Enjoyable option here cannot be questionable, including treasuring beautiful island. Techniques you still want to miss this? Find this book and also read it from currently!

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

JD34PVIAZX5: Integer Algorithms in Cryptology and Information Assurance By Boris S Verkhovsky