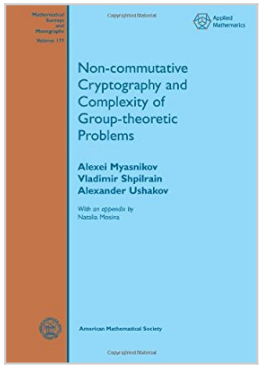

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs)

By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov

This book is about relations between three different areas of mathematics and theoretical computer science: combinatorial group theory, cryptography, and complexity theory. It explores how non-commutative (infinite) groups, which are typically studied in combinatorial group theory, can be used in public-key cryptography. It also shows that there is remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. In particular, a lot of emphasis in the book is put on studying search problems, as compared to decision problems traditionally studied in combinatorial group theory. Then, complexity theory, notably generic-case complexity of algorithms, is employed for cryptanalysis of various cryptographic protocols based on infinite groups, and the ideas and machinery from the theory of generic-case complexity are used to study asymptotically dominant properties of some infinite groups that have been applied in public-key cryptography so far. This book also describes new interesting developments in the algorithmic theory of solvable groups and another spectacular new development related to complexity of group-theoretic problems, which is based on the ideas of compressed words and straight-line programs coming from computer science.

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs)

By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov

This book is about relations between three different areas of mathematics and theoretical computer science: combinatorial group theory, cryptography, and complexity theory. It explores how non-commutative (infinite) groups, which are typically studied in combinatorial group theory, can be used in public-key cryptography. It also shows that there is remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. In particular, a lot of emphasis in the book is put on studying search problems, as compared to decision problems traditionally studied in combinatorial group theory. Then, complexity theory, notably generic-case complexity of algorithms, is employed for cryptanalysis of various cryptographic protocols based on infinite groups, and the ideas and machinery from the theory of generic-case complexity are used to study asymptotically dominant properties of some infinite groups that have been applied in public-key cryptography so far. This book also describes new interesting developments in the algorithmic theory of solvable groups and another spectacular new development related to complexity of group-theoretic problems, which is based on the ideas of compressed words and straight-line programs coming from computer science.

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov Bibliography

- Sales Rank: #3879541 in Books
- Published on: 2011-11-09
- Original language: English
- Number of items: 1
- Dimensions: 10.25" h x 7.25" w x 1.00" l, .0 pounds
- Binding: Hardcover
- 385 pages

Editorial Review

Review
The world of cryptography is evolving; new improvements constantly open new opportunities in public-key cryptography. Cryptography inspires new group-theoretic problems and leads to important new ideas. The book includes exciting new improvements in the algorithmic theory of solvable groups. Another exceptional new development is the authors' analysis of the complexity of group-theoretic problems. --MAA Reviews

Users Review

From reader reviews:

Jenny Davis:

Reading can called brain hangout, why? Because if you are reading a book specifically book entitled Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) your thoughts will drift away trough every dimension, wandering in most aspect that maybe unfamiliar for but surely might be your mind friends. Imaging each word written in a guide then become one contact form conclusion and explanation that maybe you never get just before. The Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) giving you yet another experience more than blown away your brain but also giving you useful details for your better life with this era. So now let us present to you the relaxing pattern at this point is your body and mind are going to be pleased when you are finished reading through it, like winning a. Do you want to try this extraordinary investing spare time activity?

James Babb:

You can spend your free time to learn this book this publication. This Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) is simple to create you can read it in the recreation area, in the beach, train and also soon. If you did not get much space to bring typically the printed book, you can buy the particular e-book. It is make you much easier to read it. You can save the actual book in your smart phone. And so there are a lot of benefits that you will get when one buys this book.

Dwight Richardson:

That e-book can make you to feel relax. This book Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) was multi-colored and of course has pictures around. As we know that book Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) has many kinds or style. Start from kids until teenagers. For example Naruto or Private investigator Conan you can read and believe that you are the character on there. Therefore not at all of book are generally make you bored, any it offers you feel happy,

fun and relax. Try to choose the best book in your case and try to like reading that will.

Doris Trumbull:

What is your hobby? Have you heard that will question when you got students? We believe that that problem was given by teacher on their students. Many kinds of hobby, Every person has different hobby. So you know that little person such as reading or as studying become their hobby. You have to know that reading is very important as well as book as to be the matter. Book is important thing to add you knowledge, except your personal teacher or lecturer. You will find good news or update concerning something by book. Amount types of books that can you choose to use be your object. One of them is niagra Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs).

Read Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov for online ebook

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov 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 Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov books to read online.

Online Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov ebook PDF download

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov Doc

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov Mobipocket

Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov EPub

HRKYMOJUXC1: Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) By Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov