



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

Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov

Download now

[Click here](#) if your download doesn't start automatically

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

Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov

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

 [Download Non-Commutative Cryptography and Complexity of Gro ...pdf](#)

 [Read Online Non-Commutative Cryptography and Complexity of G ...pdf](#)

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

From reader reviews:

Salina Rodriguez:

As people who live in the actual modest era should be update about what going on or info even knowledge to make them keep up with the era and that is always change and move ahead. Some of you maybe will update themselves by looking at books. It is a good choice in your case but the problems coming to anyone is you don't know which you should start with. This Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) is our recommendation to make you keep up with the world. Why, because this book serves what you want and want in this era.

Jean Gaitan:

The knowledge that you get from Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) is a more deep you rooting the information that hide inside the words the more you get considering reading it. It doesn't mean that this book is hard to be aware of but Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) giving you buzz feeling of reading. The article author conveys their point in specific way that can be understood by simply anyone who read the idea because the author of this e-book is well-known enough. This book also makes your own vocabulary increase well. It is therefore easy to understand then can go to you, both in printed or e-book style are available. We recommend you for having that Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) instantly.

Marian Dyer:

The guide with title Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) has a lot of information that you can find out it. You can get a lot of gain after read this book. This kind of book exist new understanding the information that exist in this reserve represented the condition of the world today. That is important to yo7u to find out how the improvement of the world. That book will bring you throughout new era of the the positive effect. You can read the e-book with your smart phone, so you can read the item anywhere you want.

Donna Robinson:

In this period globalization it is important to someone to find information. The information will make professionals understand the condition of the world. The condition of the world makes the information simpler to share. You can find a lot of referrals to get information example: internet, newspaper, book, and soon. You can see that now, a lot of publisher in which print many kinds of book. Often the book that recommended to you personally is Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) this e-book consist a lot of the information from the

condition of this world now. This kind of book was represented how does the world has grown up. The words styles that writer use for explain it is easy to understand. The actual writer made some study when he makes this book. This is why this book appropriate all of you.

Download and Read Online Non-Commutative Cryptography and Complexity of Group-Theoretic Problems (Mathematical Surveys and Monographs) Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov #KAGT3YOI5QP

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