Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series)

Maria Isabel González Vasco, Rainer Steinwandt

Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series)

Maria Isabel González Vasco, Rainer Steinwandt

Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series)
Maria Isabel González Vasco, Rainer Steinwandt

Group theoretic problems have propelled scientific achievements across a wide range of fields, including mathematics, physics, chemistry, and the life sciences. Many cryptographic constructions exploit the computational hardness of group theoretical problems, and the area is viewed as a potential source of quantum-resilient cryptographic primitives for the future.

Group Theoretic Cryptography supplies an ideal introduction to cryptography for those who are interested in group theory and want to learn about the possible interplays between the two fields. Assuming an undergraduate-level understanding of linear algebra and discrete mathematics, it details the specifics of using non-Abelian groups in the field of cryptography.

Moreover, the book evidences how group theoretic techniques help us gain new insight into well known, seemingly unrelated, cryptographic constructions, such as DES.

The book starts with brief overviews of the fundamentals of group theory, complexity theory, and cryptography. Part two is devoted to public-key encryption, including provable security guarantees, public-key encryption in the standard model, and public-key encryption using infinite groups.

The third part of the book covers secret-key encryption. It examines block ciphers, like the Advanced Encryption Standard, and cryptographic hash functions and message authentication codes. The last part delves into a number of cryptographic applications which are nowadays as relevant as encryption—identification protocols, key establishment, and signature schemes are covered.

The book supplies formal security analyses and highlights potential vulnerabilities for cryptographic constructions involving group theory. Summaries and references for further reading, as well as exercises, are included at the end of each chapter. Selected solutions for exercises are provided in the back of the book.

Download and Read Free Online Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) Maria Isabel González Vasco, Rainer Steinwandt

---

From reader reviews:

Wanda Crane:

In this 21st century, people become competitive in each and every way. By being competitive now, people have do something to make these people survives, being in the middle of often the crowded place and notice through surrounding. One thing that occasionally many people have underestimated it for a while is reading. Yep, by reading a reserve your ability to survive enhance then having chance to endure than other is high. For you who want to start reading a book, we give you this Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) book as basic and daily reading publication. Why, because this book is more than just a book.

Elizabeth Webster:

This Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) are generally reliable for you who want to be a successful person, why. The explanation of this Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) can be among the great books you must have is actually giving you more than just simple reading food but feed a person with information that possibly will shock your preceding knowledge. This book is usually handy, you can bring it almost everywhere and whenever your conditions at e-book and printed versions. Beside that this Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) giving you an enormous of experience for example rich vocabulary, giving you test of critical thinking that we understand it useful in your day pastime. So , let's have it and revel in reading.

Martha Lockridge:

Hey guys, do you really wants to finds a new book to see? May be the book with the title Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) suitable to you? Typically the book was written by well known writer in this era. The book untitled Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series)is the one of several books in which everyone read now. This kind of book was inspired many people in the world. When you read this reserve you will enter the new dimensions that you ever know just before. The author explained their concept in the simple way, thus all of people can easily to be aware of the core of this book. This book will give you a lots of information about this world now. In order to see the represented of the world within this book.

Jerry Bell:

Spent a free a chance to be fun activity to accomplish! A lot of people spent their spare time with their family, or their particular friends. Usually they accomplishing activity like watching television, about to beach, or picnic inside park. They actually doing same every week. Do you feel it? Would you like to something different to fill your personal free time/ holiday? Can be reading a book might be option to fill your no cost time/ holiday. The first thing that you'll ask may be what kinds of publication that you should

read. If you want to attempt look for book, may be the publication untitled Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) can be excellent book to read. May be it is usually best activity to you.

Read Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt for online ebook

Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt 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 Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt books to read online.

Online Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt ebook PDF download

Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt Doc

Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt Mobipocket

Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) by Maria Isabel González Vasco, Rainer Steinwandt EPub