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:

Arthur Pascual:

The ability that you get from Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) is a more deep you excavating the information that hide within the words the more you get enthusiastic about reading it. It doesn't mean that this book is hard to be aware of but Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) giving you enjoyment feeling of reading. The author conveys their point in particular way that can be understood by anyone who read the idea because the author of this guide is well-known enough. This book also makes your personal vocabulary increase well. That makes it easy to understand then can go together with you, both in printed or e-book style are available. We suggest you for having this specific Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) instantly.

Edward Thompson:

Reading can called thoughts hangout, why? Because when you are reading a book specially book entitled Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) your thoughts will drift away trough every dimension, wandering in every single aspect that maybe unknown for but surely will end up your mind friends. Imaging every word written in a publication then become one application form conclusion and explanation in which maybe you never get previous to. The Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) giving you yet another experience more than blown away your brain but also giving you useful details for your better life on this era. So now let us present to you the relaxing pattern is your body and mind are going to be pleased when you are finished examining it, like winning a sport. Do you want to try this extraordinary investing spare time activity?

Anita Cannon:

Do you have something that you like such as book? The book lovers usually prefer to decide on book like comic, limited story and the biggest one is novel. Now, why not attempting Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) that give your fun preference will be satisfied through reading this book. Reading routine all over the world can be said as the opportunity for people to know world a great deal better then how they react when it comes to the world. It can't be claimed constantly that reading addiction only for the geeky person but for all of you who wants to always be success person. So , for all you who want to start examining as your good habit, you could pick Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) become your current starter.

Krystal Sutherland:

Do you one of the book lovers? If yes, do you ever feeling doubt while you are in the book store? Make an

effort to pick one book that you just dont know the inside because don't judge book by its protect may doesn't work the following is difficult job because you are frightened that the inside maybe not because fantastic as in the outside look likes. Maybe you answer might be Group Theoretic Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) why because the amazing cover that make you consider with regards to the content will not disappoint you actually. The inside or content is actually fantastic as the outside or cover. Your reading 6th sense will directly direct you to pick up this book.

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