


[DOWNLOAD](#)


Group Theoretic Cryptography (Hardback)

By María Isabel González Vasco, Spyros Magliveras, Rainer Steinwandt

Taylor & Francis Inc, United States, 2015. Hardback. Condition: New. Language: English. Brand new Book. 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...



[READ ONLINE](#)
[7.18 MB]

Reviews

A new e book with a brand new standpoint. I am quite late in start reading this one, but better then never. I discovered this ebook from my i and dad advised this publication to understand.

-- Jada Franecki II

Here is the very best book i have got read through until now. I could possibly comprehended everything using this composed e publication. You will not sense monotony at whenever you want of your time (that's what catalogues are for concerning should you ask me).

-- Izaiah Schowalter

Other Books



Introduction to Quantitative Finance: A Math Tool Kit (Hardback)

MIT Press Ltd, United States, 2010. Hardback. Condition: New. Language: English. Brand new Book. An introduction to many mathematical topics applicable to quantitative finance that teaches how to "think in mathematics" rather than simply do mathematics by rote. This text offers an accessible...



Scientific and Applied Pharmacognosy: Intended for the Use of Students in Pharmacy, as a Hand Book for Pharmacists, and as a Reference Book for Food and Drug Analysts and Pharmacologists (Hardback)

Arkose Press, United States, 2015. Hardback. Condition: New. Language: English . Brand New Book ***** Print on Demand *****. This work has been selected by scholars as being culturally important, and is part of the knowledge base of civilization as we know it....



The Tabernacle or the Gospel According to Moses (Hardback)

Wentworth Press, United States, 2019. Hardback. Condition: New. Language: English. Brand new Book. This work has been selected by scholars as being culturally important, and is part of the knowledge base of civilization as we know it. This work was reproduced from...



LGB The Together Book (Sesame Street) (Hardback)

Random House USA Inc, United States, 2017. Hardback. Condition: New. Language: English. Brand new Book. A classic Sesame Street Little Golden Book about cooperation and friendship returns--just in time for the 75th-anniversary celebration of Little Golden Books! One of the first two...



Enchanted Ivy (Hardback)

SIMON & SCHUSTER, United States, 2010. Hardback. Condition: New. Reprint ed. Language: English. Brand new Book. What Lily Carter wants most in the world is to attend Princeton University just like her grandfather. When she finally visits the campus, Grandpa surprises her:...



Indifference Pricing: Theory and Applications (Hardback)

Princeton University Press, United States, 2009. Hardback. Condition: New. Language: English. Brand new Book. This is the first book about the emerging field of utility indifference pricing for valuing derivatives in incomplete markets. Rene Carmona brings together a who's who of leading...