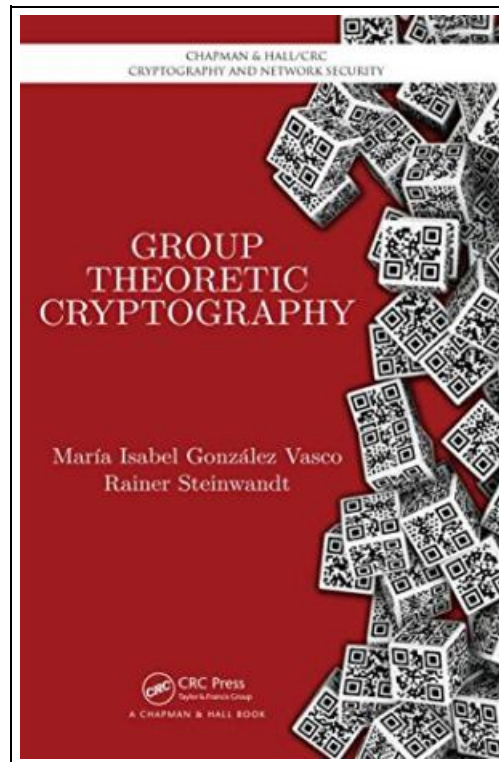


Group Theoretic Cryptography (Hardback)



Filesize: 9.63 MB

Reviews

Extensive guide for ebook enthusiasts. It is definitely basic but surprises in the fifty percent from the pdf. Your life span is going to be change the instant you comprehensive looking over this ebook.

(Audie Hettinger)

GROUP THEORETIC CRYPTOGRAPHY (HARDBACK)

[DOWNLOAD](#)

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 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.

[Read Group Theoretic Cryptography \(Hardback\) Online](#)[Download PDF Group Theoretic Cryptography \(Hardback\)](#)

You May Also Like



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...

[Download](#) [eBook](#)

»



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...

[Download](#) [eBook](#)

»



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...

[Download](#) [eBook](#)

»



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...

[Download](#) [eBook](#)

»



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...

[Download](#) [eBook](#)

»

**Hacks for Minecrafters: Combat Edition: The Unofficial Guide to Tips and Tricks That Other Guides Won't Teach You (Hardback)**

Skyhorse Publishing, United States, 2014. Hardback. Condition: New. Language: English. Brand new Book. From the author of Hacks for Minecrafters and Hacks for Minecrafters: Master Builder comes the most encompassing guide ever to combat in

[Download](#) [eBook](#)

»

**Crafty Fun With Paper! (Hardback)**

Anness Publishing, United Kingdom, 2014. Hardback. Condition: New. Language: English. Brand new Book. This title features 50 fabulous papercraft projects to make yourself. You can create your own stationery, decorations, toys, games, masks, disguises and

[Download](#) [eBook](#)

»

**Applied Conic Finance (Hardback)**

CAMBRIDGE UNIVERSITY PRESS, United Kingdom, 2016. Hardback. Condition: New. Language: English. Brand new Book. This is a comprehensive introduction to the brand new theory of conic finance, also referred to as the two-price theory, which

[Download](#) [eBook](#)

»

**Minecraft Guide to The Nether and the End: An official Minecraft book from Mojang (Hardback)**

Egmont UK Ltd, United Kingdom, 2017. Hardback. Condition: New. Language: English. Brand new Book. Now that you've mastered the Overworld, the time has come to brave the perilous Nether and End dimensions. But survival will

[Download](#) [eBook](#)

»

**Ladybird Tales: The Little Red Hen (Hardback)**

Penguin Books Ltd, United Kingdom, 2013. Hardback. Condition: New. UK ed. Language: English. Brand new Book. This beautiful hardback Ladybird edition of The Little Red Hen is a perfect first illustrated introduction to this classic

[Download](#) [eBook](#)

»