Librería

Bonilla y Asociados

desde 1950

Título: Group-Based Cryptography

Autor: Myasnikov Alexei/ Shpilrain Vladimir/ Ushakov Alexander

Precio: $606.85

Editorial:

Año: 2008

Tema:

Edición: 1ª

Sinopsis

ISBN: 9783764388263

This book is about relations between three different areas of mathematics and theoretical computer science: combinatorial group theory, cryptography, and complexity theory. It is explored how non-commutative (infinite) groups, which are typically studied in combinatorial group theory, can be used in public key cryptography. It is also shown that there is a 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.

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.

Its elementary exposition makes the book accessible to graduate as well as undergraduate students in mathematics or computer science.