Librería

Bonilla y Asociados

desde 1950

Título: Non-Commutative Cryptography And Complexity Of Group-Theoretic Problems (Vol. 1

Autor: Myasnikov, Alexei; Shpilrain, Vladimir; Ushakov, Alexander

Precio: $1460.00

Editorial:

Año: 2011

Tema:

Edición: 1ª

Sinopsis

ISBN: 9780821853603

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

In particular, a lot of emphasis in the book is put on studying search problems, as compared to decision problems traditionally studied in combinatorial 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.

This book also describes new interesting developments in the algorithmic theory of solvable groups and another spectacular new development related to complexity of group-theoretic problems, which is based on the ideas of compressed words and straight-line programs coming from computer science.