Algebraic Cryptanalysis

Algebraic Cryptanalysis_下载链接1_

著者:Gregory V. Bard

出版者:Springer

出版时间:2009-8-28

装帧:Hardcover

isbn:9780387887562

Algebraic Cryptanalysis bridges the gap between a course in cryptography, and being able to read the cryptanalytic literature. This book is divided into three parts: Part One covers the process of turning a cipher into a system of equations; Part Two covers finite field linear algebra; Part Three covers the solution of Polynomial Systems of Equations, with a survey of the methods used in practice, including SAT-solvers and the methods of Nicolas Courtois. Topics include: Analytic Combinatorics, and its application to cryptanalysis The equicomplexity of linear algebra operations Graph coloring Factoring integers via the quadratic sieve, with its applications to the cryptanalysis of RSA Algebraic Cryptanalysis is designed for advanced-level students in computer science and mathematics as a secondary text or reference book for self-guided study. This book is suitable for researchers in Applied Abstract Algebra or Algebraic Geometry who wish to find more applied topics or practitioners working for security and communications companies.

作者介绍:

目录:

Algebraic Cryptanalysis_下载链接1_

标签

计算机科学

Springer

Cryptanalysis

Algebraic

2009

评论

Algebraic Cryptanalysis_下载链接1_

书评

Algebraic Cryptanalysis_下载链接1_