第一图书网, tushu007.com

<<密码学中的代数>>

图书基本信息

书名：<<密码学中的代数>>

13位ISBN编号：9787302242901

10位ISBN编号：7302242909

出版时间：2010-12

出版时间：清华大学出版社

作者：科比次

页数：206

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

前言

This book is intended as a text for a course on cryptography with emphasis onalgebraic methods. It is written so as to be accessible to graduate or advancedundergraduate students, as well as to scientists in other fields. The first threechapters form a self-contained introduction to basic concepts and techniques. Heremy approach is intuitive and informal. For example, the treatment of computationalcomplexity in Chapter 2, while lacking formalistic rigor, emphasizes the aspectsof the subject that are most important in cryptography. Chapters 4-6 and the Appendix contain material that for the most part has notpreviously appeared in textbook form. A novel feature is the inclusion of threetypes of cryptography - "hidden monomial" systems, combinatorial-algebraic sys-tems, and hyperelliptic systems - that are at an early stage of development. It istoo soon to know which, if any, of these cryptosystems will ultimately be ofpractical use. But in the rapidly growing field of cryptography it is worthwhileto continually explore new one-way constructions coming from different areas ofmathematics. Perhaps some of the readers will contribute to the research that stillneeds to be done. This book is designed not as a comprehensive reference work, but rather asa selective textbook. The many exercises （with answers at the back of the book ）make it suitable for use in a math or computer science course or in a program ofindependent study. I wish to thank the participants in the Mathematical Sciences Research Insti-tutes Summer Graduate Student Program in Algebraic Aspects of Cryptography（Berkeley, 16-27 June 1997） for giving me the opportunity to test-teach parts of themanuscript of this book and for finding errors and unclarities that needed fixing.I am especially grateful to Alfred Menezes for carefully reading the manuscriptand making many valuable corrections and suggestions. Finally, I would like tothank Jacques Patarin for letting me report on his work （some of it not yet pub-lished） in Chapter 4; and Alfred Menezes, Yi-Hong Wu, and Robert Zuccheratofor agreeing to let me include their elementary treatment of hyperelliptic curvesas an Appendix.

第一图书网, tushu007.com

<<密码学中的代数>>

内容概要

This book is intended as a text for a course on cryptography with emphasis onalgebraic methods. It is written so as to be accessible to graduate or advancedundergraduate students, as well as to scientists in other fields. The first threechapters form a self-contained introduction to basic concepts and techniques. Heremy approach is intuitive and informal. For example, the treatment of computationalcomplexity in Chapter 2, while lacking formalistic rigor, emphasizes the aspectsof the subject that are most important in cryptography.

第一图书网, tushu007.com

<<密码学中的代数>>

书籍目录

Chapter 1 CryptographyChapter 2 Complexity of ComputationsChapter 3 AlgebraChapter 4 Hidden Monomial CryptosystemsChapter 5 Combinatorial-Algebraic CryptosystemsChapter 6 Elliptic and Hyperelliptic CryptosystemsAppendix.An Elementary Introduction to Hyperelliptic CcurvesAnswers to ExercisesBibliographySubject Index

第一图书网, tushu007.com

章节摘录

This means that everyone can send a message to a given user using the same enciphering key, which they simply look up in a public directory. There is no need for the sender to have made any secret arrangement with the recipient; indeed, the recipient need never have had any prior contact with the sender at all. It was the invention of public key cryptography that led to a dramatic expansion of the role of algebra and number theory in cryptography. The reason is that this type of mathematics seems to provide the best source of one-way functions. Later we shall discuss the most important examples. A curious historical question is why public key cryptography had to wait until 1976 to be invented. Nothing involved in the idea of public key cryptography or the early public key cryptosystems required the use of 20th century mathematics. The first public key cryptosystem to be used in the real world - the RSA system （see below） - uses number theory that was well understood by Euler. Why had it not occurred to Euler to invent RSA and offer it to the military advisers of Catherine the Great in gratitude for her generous support for the Russian Imperial Academy of Sciences, of which he was a member ?

第一图书网, tushu007.com

<<密码学中的代数>>

编辑推荐

This is a textbook for a course （or self-instruction） in cryptography with emphasison algebraic methods. The first half of the book is a self-contained informalintroduction to areas of algebra， number theory， and computer science that are usedin cryptography. Most of the material in the second half -"hidden monomial"systems， combinatorial-algebraic systems， and hyperelliptic systems - has notpreviously appeared in monograph form. The Appendix by Menezes， Wu， andZuccherato gives an elementary treatment of hyperelliptic curves. This book isintended for graduate students， advanced undergraduates， and scientists workingin various fields of data security." ...I think this book is a very inspiring book on cryptography. It goes beyond thetraditional topics （most of the cryptosystems presented here are first time in atextbook， some of Patarins work is not published yet）. This way the reader has thefeeling how easy to suggest a cryptosystem， how easy to break a safe looking systemand hence how hard to trust one. The interested readers are forced to think togetherwith their researchers and feel the joy of discovering new ideas. At the same timethe importance of "hardcore" mathematics is emphasized and hopefully some application driven students will be motivated to study theory. "

第一图书网, tushu007.com

<<密码学中的代数>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com