

<<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>

## &lt;&lt;密码学中的代数&gt;&gt;

## 前言

This book is intended as a text for a course on cryptography with emphasis on algebraic methods. It is written so as to be accessible to graduate or advanced undergraduate students, as well as to scientists in other fields. The first three chapters form a self-contained introduction to basic concepts and techniques. Heremy approach is intuitive and informal. For example, the treatment of computational complexity in Chapter 2, while lacking formalistic rigor, emphasizes the aspects of the subject that are most important in cryptography. Chapters 4-6 and the Appendix contain material that for the most part has not previously appeared in textbook form. A novel feature is the inclusion of three types of cryptography - "hidden monomial" systems, combinatorial-algebraic systems, and hyperelliptic systems - that are at an early stage of development. It is too soon to know which, if any, of these cryptosystems will ultimately be of practical use. But in the rapidly growing field of cryptography it is worthwhile to continually explore new one-way constructions coming from different areas of mathematics. Perhaps some of the readers will contribute to the research that still needs to be done. This book is designed not as a comprehensive reference work, but rather as a 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 of independent study. I wish to thank the participants in the Mathematical Sciences Research Institutes Summer Graduate Student Program in Algebraic Aspects of Cryptography (Berkeley, 16-27 June 1997) for giving me the opportunity to test-teach parts of the manuscript of this book and for finding errors and unclarities that needed fixing. I am especially grateful to Alfred Menezes for carefully reading the manuscript and making many valuable corrections and suggestions. Finally, I would like to thank Jacques Patarin for letting me report on his work (some of it not yet published) in Chapter 4; and Alfred Menezes, Yi-Hong Wu, and Robert Zuccherato for agreeing to let me include their elementary treatment of hyperelliptic curves as an Appendix.

## <<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 on algebraic methods. It is written so as to be accessible to graduate or advanced undergraduate students, as well as to scientists in other fields. The first three chapters form a self-contained introduction to basic concepts and techniques. Heremy approach is intuitive and informal. For example, the treatment of computational complexity in Chapter 2, while lacking formalistic rigor, emphasizes the aspects of the subject that are most important in cryptography.

<<密码学中的代数>>

书籍目录

Chapter 1 Cryptography Chapter 2 Complexity of Computations Chapter 3 Algebra Chapter 4 Hidden Monomial Cryptosystems Chapter 5 Combinatorial-Algebraic Cryptosystems Chapter 6 Elliptic and Hyperelliptic Cryptosystems Appendix. An Elementary Introduction to Hyperelliptic Curves Answers to Exercises Bibliography Subject Index

## 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 ?

## &lt;&lt;密码学中的代数&gt;&gt;

## 编辑推荐

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

<<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>