

<<数论与密码学教程>>

图书基本信息

书名：<<数论与密码学教程>>

13位ISBN编号：9787506291620

10位ISBN编号：7506291622

出版时间：2008-1

出版时间：世界图书出版公司

作者：科布科茨

页数：235

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>

<<数论与密码学教程>>

内容概要

本书是一部讲述数论的密码学应用的研究生教材。

该书是《数论与密码学教程》的第2版，它是在第一版的基础上修订而成的。

书中增加了零知识的证明和不经意传输，平方筛因子分解方法，椭圆曲线在素性检验中的应用，概率加密术，hash 函数等一些新内容。

全书共分6个章节，具体内容包括基础数论浅述，有限域和二次剩余，密码学，公共密钥，素性和因式分解和椭圆曲线密码学。

该书可供各大专院校作为教材使用，也可供从事相关工作的人员作为参考用书使用。

<<数论与密码学教程>>

书籍目录

Foreword
Preface to the Second Edition
Chapter . Some Topics in Elementary Number Theory 1. Time estimates for doing arithmetic 2. Divisibility and the Euclidean algorithm 3. Congruences 4. Some applications to factoring
Chapter . Finite Fields and Quadratic Residues 1. Finite fields 2. Quadratic residues and reciprocity
Chapter . Cryptography 1. Some simple cryptosystems 2. Enciphering matrices
Chapter . Public Key 1. The idea of public key cryptography 2. RSA 3. Discrete log 4. Knapsack 5. Zero-knowledge protocols and oblivious transfer
Chapter . Primality and Factoring 1. Pseudoprimes 2. The rho method 3. Fermat factorization and factor hases 4. The continued fraction method 5. The quadratic sieve method
Chapter . Elliptic Curves 1. Basic facts 2. Elliptic curve cryptosystems 3. Elliptic curve primality test 4. Elliptic curve factorization
Answers to Exercises
Index

<<数论与密码学教程>>

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>