<<密码学基础（第二卷）>>

图书基本信息

书名：<<密码学基础（第二卷）>>

13位ISBN编号：9787121008405

10位ISBN编号：7121008408

出版时间：2005-2-1

出版时间：电子工业出版社

作者：戈德赖克

页数：798

字数：627000

<<密码学基础（第二卷）>>

内容概要

密码学涉及解决通信保密问题的计算系统的概念、定义及构造。
密码系统的设计必须基于坚实的基础。
本书继上一卷对这一基础问题再次给出了系统而严格的论述：用已有工具来定义密码系统的目标并解决新的密码学问题。
全书详细阐述了三种基本应用：加密、签名和一般的密码学协议。
该书的重点是澄清基本概念及证明密码学问题解决方法的可行性，而不侧重于对特殊方法的描述。
本书可作为密码学、应用数学、信息安全等专业的研究生教材，也可作为相关专业人员的参考用书。

作者简介

Oded Goldreich 以色列魏茨曼科学研究所的计算机科学教授，现任Meyer W.Weisgal讲座教授。作为一名活跃的学者，他已经发表了大量密码学方面的论文，是密码学领域公认的世界级专家。他还是“ Journal of Cryptology ”，“ SIAM Journal on Computing ”杂志的编辑，1999年在Spri

<<密码学基础（第二卷）>>

书籍目录

<<密码学基础（第二卷）>>

版权说明