《密码学基础（第二卷）》

图书基本信息

《密码学基础（第二卷）》

内容概要

密码学涉及解决安全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。本书对这一基础问题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。本书的重点是澄清基本概念并论述解决几个主要密码问题的可行性，而不侧重于对特殊方法的描述。

《密码学基础》第一卷主要讨论的是单向函数、伪随机性和零知识证明。本书在第一卷的基础上接着讨论加密、签名和一般的密码协议。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。

注意：本书第一卷内容共4章，为了体现顺序性，第二卷的章号与第一卷的章号衔接，因此本书（第二卷）正文从第5章开始。本书（第二卷）附录与第一卷的附录序号衔接，因此本书附录为附录C。本书第一卷已由人民邮电出版社出版，书名：《密码学基础》，书号：10355。

《密码学基础（第二卷）》

作者简介

Oded Goldreich是以色列魏茨曼学院的计算机科学教授，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 Cryptoloty和SIAM Journal on Computing杂志的编辑，出版了《现代密码学、概

《密码学基础（第二卷）》

书籍目录

《密码学基础（第二卷）》

版权说明