<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787563525973

10位ISBN编号：7563525971

出版时间：2011-4

出版时间：北京邮电大学出版社

作者：任伟

页数：288

<<现代密码学>>

内容概要

本书内容包括密码学概述、古典密码体制、信息理论安全、序列密码、分组密码、hash函数与消息鉴别、公钥加密（基础）、公钥加密（扩展）、数字签名、实体认证和身份识别、密钥管理。
《现代密码学》特点是注重介绍知识的内在逻辑性，展现密码学方案设计的内在规律和基本原理，注重使用比较和类比的方式探究一般规律和方法论，使学习者“知其所以然”。

本书面向的主要对象包括高等学校信息安全、密码学、电子对抗、应用数学等专业本科高年级学生和研究生。
对具有密码学基础的研究人员也有一定启发作用。

<<现代密码学>>

书籍目录

<<现代密码学>>

编辑推荐

《普通高校信息安全系列教材：现代密码学》也是一本旨在让学习者能够“真正学懂密码学”的密码学教材。
“密码学”是信息安全专业、密码学专业、电子对抗专业中一门最重要的专业课，在学科知识体系中占据重要的地位。
但多年的教学实践以及学生的体会表明，它也是_门非常难学（和难讲授）的综合课程，其数学基础涉及算法数论、计算复杂性、抽象代数、信息论、概率论等，讲授的内容覆盖面广，各知识点均具有一定难度和深度。

版权说明