

<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787508329598

10位ISBN编号：7508329597

出版时间：2005-1

出版时间：中国电力出版社

作者：蔡乐才 编

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;应用密码学&gt;&gt;

## 内容概要

本书是按照高等本科院校的培养目标和基本要求，并结合作者多年来教学经验和工程实践的基础，为实施教学改革，使密码学技术面向应用实践，而编写的一本应用密码学技术基础教材。

本书在详细介绍密码学的基本概念及分类的基础上，介绍了目前应用较多的密码学技术。

全书的内容涵盖两个方面：一方面介绍了密码学理论，其中对常见密码算法，如DES、RSA、IDEA和AES等进行了详细的介绍和分析，以便于密码算法的分析、设计和应用；另一方面，为了突出密码学的实际应用，结合目前信息处理和信息传输中比较典型的密码算法应用，如数字签名、身份识别和电子货币等，进行了实例分析，建立了密码算法应用系统的基本架构，并就应用中可能存在的密码算法性能问题进行了详细的分析和描述，对于密码学的分析研究和应用研发起到了很好的参考作用。

本书在每章后均配有理论巩固题和上机实战题，实现了教与学的统一。

本书语言通俗易懂，内容丰富翔实，突出了以实例为中心的特点，既可作为大学本科院校计算机科学与技术专业、网络工程专业、信息安全及其相关专业的教学用书，也可作为广大密码学爱好者自学应用密码学技术时的参考用书。

## &lt;&lt;应用密码学&gt;&gt;

## 书籍目录

序前言第1章 密码学概述 1.1 密码学的基本概念 1.2 密码体制的分类 1.3 密码学的发展历史 1.4 实践检验第2章 古典密码学 2.1 古典密码学中的基本运算 2.2 几种典型的古典密码体制 2.3 古典密码的统计分析 2.4 实践检验第3章 密码学的数学基础 3.1 信息论 3.2 复杂性理论 3.3 数论 3.4 素数的产生 3.5 有限域上的离散对数 3.6 实践检验第4章 分组密码 4.1 分组密码的产生背景及意义 4.2 数据加密标准——DES 4.3 美国最新的加密标准AES 4.4 其他典型的分组密码简介 4.5 实践检验第5章 公钥加密 5.1 产生背景和基本概念 5.2 背包公钥密码算法 5.3 RSA算法 5.4 其他公钥密码简介 5.5 实践检验第6章 流密码 6.1 基本概念 6.2 有限状态机 6.3 流密码系统结构 6.4 使用LFSR的流密码算法 6.5 其他的流密码算法 6.6 实践检验第7章 密钥管理 7.1 密钥的组织结构和种类 7.2 密钥生成 7.3 密钥分配 7.4 密钥协商 7.5 实践检验第8章 数字签名 8.1 数字签名的基本概念 8.2 数字签名标准 8.3 其他签名方案 8.4 实践检验第9章 身份识别 9.1 什么是身份识别 9.2 弱身份识别 9.3 强身份识别 9.4 身份识别协议 9.5 对身份识别协议的攻击 9.6 实践检验第10章 电子货币 10.1 电子现金的出现与发展史 10.2 在线电子货币 10.3 一个电子现金方案 10.4 有监视器的钱包 10.5 实践检验参考文献

<<应用密码学>>

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>