

<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787302156796

10位ISBN编号：7302156794

出版时间：2008-1

出版时间：清华大学出版社

作者：德尔夫斯,克内贝尔

页数：266

译者：肖国镇,张宁

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>

## <<密码学导引>>

### 内容概要

《密码学导引：原理与应用》共10章，主要从两个方面介绍密码学的知识：第一部分介绍了经典密码学中的对称密码体制、非对称密码体制及相关的密码协议，重点讨论了模代数学和以模代数学为基础的非对称密码。

第二部分从Shannon经典的信息论工作出发，分析了概率算法和单向函数的安全性，并给出了基本的安全性定义。

在此基础上，对公钥加密和签名方案的可证明安全性做了详细的分析。

另外，在附录中，《密码学导引：原理与应用》还完整地介绍了密码学中需要用到的代数数论和概率信息论的基础知识。

各章的结尾声处都有相关的习题，读者可以在原著者公布的网站上查到习题的答案。

《密码学导引：原理与应用》可作为信息安全领域的大学生与研究生的相关课程的教材，也可作为密码学和信息安全领域的研究人员的参考书。

## 作者简介

肖国镇，西安电子科技大学教授，博士生导师，上海交通大学、武汉大学兼职教授，加拿大温莎大学、德国多特蒙德大学、荷兰爱因豪芬大学、法国勒芒大学、日本九州工业大学、新加坡国立大学、美国宾夕法尼亚大学客座教授。

国际著名密码学家。

长期从事密码学和信息安全的教学和科研工作。

曾任中国密码学会（筹）副理事长、中国电子信息学会信息论专业委员会副主任，中国计算机学会信息保密委员会副主任委员、中央办公厅机要局科技进步奖评审委员会副主任、国家教委数学与力学教学指导委员会委员、西安电子科技大学信息安全与保密研究所所长。

在国内外学术刊物和会议上发表论文多篇，与著名科学家Massey联合提出的肖-Massey定理是国际上流密码领域的基础性定理，对流密码的发展起着非常重要的作用。

## &lt;&lt;密码学导引&gt;&gt;

## 书籍目录

第1部分密码学的基本概念第1章引言1.1加密与保密性1.2研究密码学的目的1.3攻击1.4密码协议1.5可证明安全第2章对称密钥加密体制2.1流密码2.2分组密码2.2.1DES2.2.2运行模式习题第3章公钥密码学3.1公钥密码学基本概念3.2模算术3.2.1整数3.2.2整数模 $n$ 3.3RSA3.3.1密钥生成与加密3.3.2数字签名3.3.3对RSA的攻击3.3.4RSA加密的安全应用3.4杂凑函数3.4.1Merkle衍生法3.4.2杂凑函数的构造3.4.3概率签名3.5离散对数3.5.1ElGamal加密3.5.2ElGamal签名方案3.5.3数字签名算法3.6模平方根3.6.1Rabin加密3.6.2Rabin签名方案习题第4章密码协议4.1密钥交换和实体认证4.1.1Kerberos4.1.2Diffie-Hellman密钥协商4.1.3密钥交换和相互认证4.1.4站一站协议4.1.5公钥管理技术4.2身份识别方案4.2.1交互式证明系统4.2.2简化的Fiat-Shamir身份识别方案4.2.3零知识4.2.4Fiat-Shamir身份识别方案4.2.5Fiat-Shamir签名方案4.3承诺系统4.3.1基于平方剩余的承诺系统4.3.2基于离散对数的承诺系统4.3.3同态承诺4.4电子选举4.4.1秘密共享4.4.2多机构电子选举方案4.4.3知识证明4.4.4非交互式知识证明4.4.5扩展的多择选举4.4.6消除信任中心4.5数字现金4.5.1盲发行证明4.5.2公平的电子现金系统4.5.3潜在的问题习题第2部分密码协议的分析方法和密码的安全性第5章概率算法第6章单向函数和基本假设第7章单向函数的比特安全性第8章单向函数和伪随机性第9章可证明安全的加密第10章可证明安全数字签名附录A代数与数论附录B概率与信息论符号英文原著参考文献

<<密码学导引>>

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>