

<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787302078470

10位ISBN编号：7302078475

出版时间：2004-3

出版时间：清华大学出版社

作者：孙淑玲

页数：191

字数：237000

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>

## <<应用密码学>>

### 内容概要

应用密码技术是电子安全系统的关键技术，它主要实现保密性、完整性和不可否认性。

本书包括密码算法、密码协议及使用方面的主要内容：分组密码算法、公钥密码算法、数字签名、哈希函数、密钥建立、密钥管理、身份识别、电子现金等。

每章后附有阅读资料，部分章节配有习题。

本书是在中国科学院研究生院讲授多年的讲义的基础上形成的。

可以作为高等学校计算机科学、通信工程、信息安全等专业的研究生教材，也可以供有关工程技术人员参考。

## <<应用密码学>>

### 作者简介

孙淑玲，中国科学院研究生院教授。

1941年出生，1963年毕业于中国科学技术大学教学系并留校任教，1997年调入中国科学院研究生院。多年来一直从事语言与自动机、语言编译器自动生成、数据库分定等方向的研究工作，先后在国内外重要期刊上发表学术论文15篇。

从40年来，先后主

## &lt;&lt;应用密码学&gt;&gt;

## 书籍目录

总序出版前言序言第1章 密码学概述 1.1 引论 1.1.1 信息安全与应用密码学 1.1.2 基本术语和概念 1.1.3 密码学发展历史 1.2 对称密钥加密 1.2.1 分组密码 1.2.2 流密码 1.2.3 对称密钥密码的优缺点 1.3 数字签名, 认证与识别 1.3.1 数字签名 1.3.2 认证与识别 1.4 公钥密码学 1.4.1 公钥加密 1.4.2 公钥加密的优缺点 1.5 密码协议与密码机制 1.6 攻击分类与安全模型 1.6.1 对加密方案的攻击 1.6.2 对密码协议的攻击 1.6.3 安全模型 1.7 复杂性理论第2章 分组密码 2.1 数据加密标准DES 2.1.1 DES发展历史 2.1.2 DES算法描述 2.1.3 DES子密钥的生成 2.1.4 DES算法实现及安全性 2.1.5 DES算法的性质 2.2 IDEA算法 2.2.1 IDEA加密算法 2.2.2 密钥扩展方法 2.2.3 IDEA解密算法 2.3 RC5算法 2.4 美国最新的加密标准AES 2.4.1 AES加密算法 2.4.2 密钥扩展过程 2.5 分组密码的运行模式 2.5.1 电子密码本模式 2.5.2 密文分组链接模式 2.5.3 输出反馈模式 2.5.4 密文反馈模式 2.6 多重加密 2.7 对分组密码的分析方法 2.8 使用分组密码系统进行保密通信 2.8.1 安全薄弱环节 2.8.2 链路加密与端-端加密 习题 附录A 有限域 A.1 有限域的概念 A.2 有限域上的多项式环 阅读资料第3章 公钥密码系统 3.1 RSA系统和素因子分解 3.1.1 RSA密码系统描述 3.1.2 RSA实现过程及安全性 3.1.3 RSA在实现时要注意的问题 .....第4章 数字签名第5章 哈希函数第6章 密钥建立第7章 密钥管理技术第8章 身份识别第9章 货币第10章 密码技术标准参考文献

#### 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>