

<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787811145199

10位ISBN编号：7811145197

出版时间：2008-11

出版时间：电子科技大学出版社

作者：许春香 等著

页数：163

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>

## <<现代密码学>>

### 内容概要

《现代密码学》为信息安全系列丛书之一，系统地介绍了现代密码学基础知识，包括流密码、分组密码、公钥密码、数字签名、Hash函数，同时《现代密码学》还介绍了密码学的最新进展。

《现代密码学》可作为信息安全专业、计算机专业、通信专业本科生、研究生教材，还可以供信息安全技术领域科技人员参考。

## &lt;&lt;现代密码学&gt;&gt;

## 书籍目录

第1章 引言1.1 密码学的发展历史1.2 密码学基本概念1.2.1 保密通信系统1.2.2 密码体制分类1.2.3 密码攻击1.3 古典密码体制1.3.1 置换密码1.3.2 单表代替密码1.3.3 多表代换密码习题第2章 流密码2.1 基本概念2.1.1 一次一密与流密码2.1.2 流密码的思想2.1.3 流密码结构2.2 序列的随机性2.3 密钥流生成器2.4 线性移位寄存器2.5 两个流密码算法2.5.1 流密码算法RC42.5.2 流密码算法A5习题第3章 分组密码3.1 分组密码的基本原理3.2 分组密码的工作模式3.3 数据加密标准--DES3.1.1 DES算法的历史3.3.2 DES算法3.3.3 DES的安全性3.3.4 多重加密DES3.4 高级加密标准--AES3.4.1 AES算法的基本运算单位3.4.2 AES算法的加密解密过程3.4.3 AES的安全性3.5 SMS4 分组密码算法3.5.1 SMS4 算法的术语说明3.5.2 轮函数, 3.5.3 SMS4 的加密算法和解密算法3.5.4 密钥扩展算法3.6 IDEA分组密码算法3.6.1 IDEA算法描述3.6.2 IDEA的安全性习题第4章 公钥密码4.1 数论基础知识4.2 公钥密码的基本概念4.2.1 公钥密码体制的原理4.2.2 公钥密码体制的要求4.3 RSA公钥密码4.3.1 算法描述4.3.2 RSA的安全性4.4 ElGamal公钥密码4.4.1 算法描述4.4.2 ElGamal的安全性4.5 Rabin公钥密码4.6 椭圆曲线公钥密码4.6.1 实数域上的椭圆曲线4.6.2 有限域上的椭圆曲线4.6.3 椭圆曲线密码体制习题第5章 数字签名5.1 数字签名的基本概念5.2 RSA数字签名5.3 ElGamal数字签名5.4 数字签名标准: DSS5.5 其他数字签名5.5.1 基于离散对数问题的数字签名方案5.5.2 基于大整数分解问题的数字签名方案5.5.3 具有特殊用途的数字签名习题第6章 Hash函数6.1 Hash函数的概念6.2 Hash函数MD56.3 Hash函数SHA6.4 基于分组密码的Hash函数6.5 Hash函数的分析方法习题第7章 密码协议7.1 密钥分配 Needham-Sclaroeder协议7.2 密钥协商7.2.1 Diffie-HeUman密钥交换协议7.2.2 端到端协议7.3 认证技术与理论7.3.1 Kefberos认证协议7.3.2 X.509认证服务7.4 秘密共享7.4.1 Shamii · 门限方案7.4.2 可验证秘密共享7.4.3 无可信中心的秘密共享7.5 身份识别7.5.1 身份识别的概念7.5.2 Guillou-Quisquater身份识别方案7.6 零知识证明7.7 签密习题第8章 可证明安全性理论8.1 可证明安全性理论的基本概念8.2 可证明安全的公钥密码体制8.3 可证明安全的数字签名体制习题第9章 基于身份的公钥密码体制9.1 公钥认证方法9.2 基于身份的加密方案9.2.1 双线性对9.2.2 Boneh-Frankin加密方案9.3 基于身份的签名方案9.4 基于身份的密钥协商协议9.5基于身份的签密方案习题第10章 密码学的新方向10.1 量子密码学10.1.1 Beenett-Brassard量子密钥分配协议10.1.2 量子密码的应用与进展10.2 变量公钥密码10.2.1 多变量公钥密码体制的一般形式10.2.2 MI多变量公钥密码体制10.2.3 彩虹: 多层油醋签名体制10.2.4 多变量公钥密码体制的现状10.3 基于格的公钥密码体制10.3.1 数学背景10.3.2 NTRU公钥加密体制10.3.3 NTRLJSign数字签名体制10.4 DNA密码学10.4.1 DNA计算10.4.2 DNA加密技术10.4.3 DNA密码发展的趋势习题参考文献

## <<现代密码学>>

### 编辑推荐

《现代密码学》主要讨论现代密码学，为读者掌握和应用现代密码技术打下基础，但为了使读者全面了解密码学的历史，《现代密码学》在引言中也简单介绍了古典密码学。

《现代密码学》在后续章节即第8章、第9章和第10章讨论了密码学的新方向，包括基于身份的公钥密码、可证明安全理论、量子密码学和DNA密码学等。

这部分内容可以使读者了解密码技术的最新进展，对于一般了解密码学的读者可以不涉及。

《现代密码学》可作为信息安全专业本科生、研究生教材，还可以供信息安全技术领域科研人员参考。

<<现代密码学>>

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>