现代密码学

现代密码学_下载链接1_

著者:何大可

出版者:人民邮电

出版时间:2009-9

装帧:

isbn:9787115211576

《现代密码学》系统地讲述了密码学的基础理论与应用技术。主要内容包括密码学的信息论基础、密码学的复杂性理论、流密码、分组密码、公钥密码、Hash函数、数字签名、密码协议和密钥管理。《现代密码学》内容丰富，取材经典、新颖，概念清楚，各章后面配有大量习题。《现代密码学》可作为高等院校信息安全、通信工程等相关专业本科生的教材，也可供研究生与相关技术人员学习参考。

作者介绍:

西南交通大学教授、国家高性能计算中心(成都)主任、博士生导师、从1992年起享受国务院特殊津贴。兼任中国密码学会副理事长，华南农业大学“丁颖讲座教授”。长期从事密码学、移动通信安全、铁路信息系统安全工程等方面的教学、研究和设计工作。参与了我国首批密码学博士点申报；曾任第四届全国铁路高校电子信息类专业教学指导委员会副主任，计算机科学与技术、自动化专业教学指导组组长。先后主持、主研国家自然科学基金项目、国家“八五”攻关项目、国家863计划项目、教育部博士点基金项目及铁道部等部委科技项目约30项。是多项中国专利和美国专利US6、859、151 B2的发明人。1989年获国家自然科学四等奖，获省部级一等奖1次、省部级二等奖3次

，1997年获中国科学技术发展基金会第三届詹天佑人才奖。

目录: 第1章 概论 1.1 信息安全与密码技术 1.2 密码系统模型和密码体制 1.3 几种简单的密码体制 1.4 初等密码分析 1.5 密码学的信息论基础 1.5.1 信息量和熵 1.5.2 完善保密性 1.5.3 唯一解距离、理论保密性与实际保密性 1.6 密码学的复杂性理论基础 1.6.1 问题与算法 1.6.2 算法复杂性 1.6.3 问题按复杂性分类 注记 习题 第2章 流密码 2.1 流密码的一般模型 2.2 线性反馈移位寄存器序列 2.3 线性复杂度及B-M算法 2.4 非线性准则及非线性序列生成器 2.5 流密码算法介绍 2.5.1 RC4算法 2.5.2 A5算法 注记 习题 第3章 分组密码 3.1 分组密码的一般模型 3.2 分组密码分析方法 3.3 DES 3.3.1 DES算法描述 3.3.2 DES安全性 3.3.3 三重DES 3.4 IDEA 3.4.1 IDEA基本运算 3.4.2 IDEA算法描述 3.4.3 IDEA安全性和效率 3.5 AES算法-Rijndael 3.5.1 Rijndael算法数学基础 3.5.2 Rijndael设计原理 3.5.3 Rijndael算法描述 3.5.4 Rijndael安全性及效率 3.6 分组密码工作模式 注记 习题 第4章 公钥密码学 4.1 公钥密码系统基本概念 4.1.1 基本概念 4.1.2 背包公钥密码系统 4.2 RSA公钥密码系统 4.2.1 算法描述 4.2.2 对RSA的攻击 4.2.3 RSA系统的参数选取 4.3 离散对数公钥密码系统 4.3.1 ElGamal密码系统 4.3.2 ElGamal密码系统的安全性 4.3.3 椭圆曲线密码系统 4.4 可证明安全公钥密码系统 4.4.1 可证明安全性 4.4.2 公钥密码系统的安全性 4.4.3 可证明安全抗选择明文攻击密码系统 4.4.4 可证明安全抗选择密文攻击密码系统 注记 习题 第5章 Hash函数与消息认证 5.1 Hash函数概述 5.1.1 Hash函数定义 5.1.2 Hash函数的安全性 5.1.3 Hash函数的迭代构造法 5.2 Hash函数MD5 5.2.1 MD5算法 5.2.2 MD5的安全性 5.3 安全Hash算法SHA-1 5.3.1 SHA-1算法 5.3.2 SHA-1和MD5的比较 5.3.3 SHA-1的修订版 5.4 基于分组密码与离散对数的Hash函数 5.4.1 利用分组密码构造Hash函数 5.4.2 基于离散对数问题构造Hash函数 5.5 消息认证 5.5.1 消息认证码 5.5.2 HMAC算法 5.6 应用 注记 习题 第6章 数字签名 6.1 数字签名概述 6.2 RSA数字签名体制 6.2.1 算法描述 6.2.2 RSA数字签名的安全性 6.3 ElGamal数字签名体制 6.3.1 算法描述 6.3.2 ElGamal数字签名的安全性 6.3.3 ElGamal签名体制的变形 6.4 其他数字签名体制 6.4.1 Schnorr数字签名 6.4.2 Fiat-Shamir数字签名 6.4.3 一次性数字签名 6.4.4 不可否认数字签名 6.4.5 盲签名 6.5 数字签名标准 6.5.1 美国数字签名标准 6.5.2 俄罗斯数字签名标准 6.6 应用 注记 习题 第7章 密码协议 7.1 密码协议概述 7.2 实体认证协议 7.3 密钥认证协议 7.3.1 基于对称密码技术的密钥认证协议 7.3.2 基于非对称密码技术的密钥认证协议 7.4 比特承诺协议 7.5 零知识证明与身份识别协议 7.5.1 零知识证明 7.5.2 身份识别协议 注记 习题 第8章 密钥管理 8.1 密钥管理的基本概念 8.2 密钥生成与密钥分发 8.2.1 密钥的种类 8.2.2 密钥生成 8.2.3 密钥分配 8.3 秘密共享与密钥托管 8.3.1 秘密共享 8.3.2 密钥托管 8.4 公钥基础设施PKI 8.4.1 PKI的概念 8.4.2 PKI的组成 8.4.3 X.509认证业务 8.4.4 认证中心的体系结构与服务 8.4.5 PKI中的信任模型 注记 习题 参考文献

・・・・・・(收起)

现代密码学_下载链接1_

标签

教材

评论

保佑我通过考试吧!

现代密码学_下载链接1_

书评

现代密码学_下载链接1_