第一图书网, tushu007.com

<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787302068143

10位ISBN编号：7302068143

出版时间：2003-8-1

出版时间：清华大学出版社

作者：杨波

页数：220

字数：295000

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

第一图书网, tushu007.com

内容概要

本书旨在介绍现代密码学的基本原理及方法。
全书共分8章，第1章介绍现代密码学的基本概念，其余各间分别介绍流密码、分组密码、公钥密码、密钥分配与密钥管理、消息认证和杂凑算法、数学签字和密码协议、网络加密与认证。
　本书内容翔实，概念表述严谨，语言精练，例题丰富，切合教学之用。
　本书可作为高等院校信息安全、计算机、通信工程、密码学及相关专业大学本科和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

<<现代密码学>>

书籍目录

第1章 引言　1.1　信息安全面临的威胁　1.1.1　安全威胁　1.1.2　入侵者和病毒　1.1.3　安全业务　1.2　信息安全的模型　1.3　密码学基本概念　1.3.1　保密通信系统　1.3.2　密码体制分类　1.3.3　密码攻击概述第2章　流密码　2.1　流密码的基本概念　2.1.1　同步流密码　2.1.2　有限状态自动机　2.1.3　密钥流产生器　2.2　线性反馈移位寄存器　2.3　线性移位寄存器的一元多项式表示　2.4　m序列的伪随机性　2.5　m序列密码的破译　2.6　非线性序列　2.6.1　Geffe序列生成器　2.6.2　J-K触发器　2.6.3　Pless生成器　2.6.4　钟控序列生成器　习题第3章　分组密码体制　3.1　分组密码概述　3.1.1　代换　3.1.2　扩散和混淆　3.1.3　Feistel密码结构　3.2　数据加密标准　3.2.1　DES描述　3.2.2　二重DES　3.2.3　两个密钥的三重DES　3.2.4　三个密钥的三重DES　3.3　差分密码分析与线性密码分析　3.3.1　差分密码分析　3.3.2　线性密码分析　3.4　分组密码的运行模式　3.4.1　电码本(ECB)模式　3.4.2　密码分组链接(CBC)模式　3.4.3　密码反馈(CFB)模式　3.4.4　输出反馈(OFB)模式　3.5　IDEA　3.5.1　设计原理　3.5.2　加密过程　3.6　AES算法——Rijndae　3.6.1　Rijndael的数学基础和设计思想　3.6.2　算法说明　习题第4章　公钥密码　4.1　数论简介　4.1.1　素数和互素数　4.1.2　模运算　4.1.3　费尔玛定理和欧拉定理　4.1.4　素性检验　4.1.5　欧几里得算法　4.1.6　中国剩余定理　4.1.7　离散对数　4.1.8　平方剩余　4.2　公钥密码体制的基本概念　4.2.1　公钥密码体制的原理　4.2.2　公钥密码算法应满足的要求　4.2.3　对公钥密码体制的攻击　4.3　RSA算法　4.3.1　算法描述　4.3.2　RSA算法中的计算问题　4.3.3　RSA的安全性　4.3.4　对RSA的攻击　4.4　背包密码体制　4.5　Rabin密码体制　4.6　椭圆曲线密码体制　4.6.1　椭圆曲线　4.6.2　有限域上的椭圆曲线　4.6.3　椭圆曲线上的密码　习题第5章 密钥分配与密钥管理第6章 消息认证和杂凑算法第7章 数字签字和密码协议第8章 网络加密与认证参考文献

第一图书网, tushu007.com

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