

<<密码编码学与网络安全>>

图书基本信息

书名：<<密码编码学与网络安全>>

13位ISBN编号：9787505366046

10位ISBN编号：7505366041

出版时间：2003-12-1

出版时间：电子工业出版社

作者：William Stallings

页数：435

字数：729000

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>

## <<密码编码学与网络安全>>

### 内容概要

密码编码学与网络安全是当今通信与计算机界的热门课题。

本书内容新颖丰富，讲述了基本的数据加密原理和数论的概念、各种加密算法和常用的协议以及它们在网络中的应用。

书中各章都提供了许多习题和参考读物，并列出了推荐网站。

本书适用于髣信计算机专业的本科生或研究生，也可作为通信或计算机领域的研究人员和专业技术人员的参考书。

## <<密码编码学与网络安全>>

### 作者简介

斯大林，麻省理工学院计算机科学博士毕业，国际上颇有影响计算机网络教授。先后出版了17种不同内容的教材。

曾4次获得教科书与院校作者协会最佳计算机科学图书年度奖。

## &lt;&lt;密码编码学与网络安全&gt;&gt;

## 书籍目录

第1章 引言 1.1 攻击、服务和机制 1.1.1 服务 1.1.2 机制 1.1.3 攻击 1.2 对安全的攻击 1.2.1 被动攻击 1.2.2 主动攻击 1.3 安全服务 1.3.1 机密性 1.3.2 鉴别 1.3.3 完整性 1.3.4 不可抵赖 1.3.5 访问控制 1.3.6 可用性 1.4 网络安全模型 1.5 本书概要 1.6 推荐读物 附录IA Internet和Web资源 本书的Web站点 其他Web站点 USENET新闻组第一部分 常规加密 第2章 常规加密的经典技术 2.1 常规加密模型 2.1.1 密码编码学 2.1.2 密码分析 2.2 隐写术 2.3 经典加密技术 2.3.1 替代技术 2.3.2 置换技术 2.3.3 转子机(Rotor Machine) 2.4 推荐读物 2.5 习题 第3章 常规加密的现代技术 3.1 简化的DES 3.1.1 概述 3.1.2 S—DES密钥的产生 3.1.3 S—DES的加密操作 3.1.4对简化版DES的分析 3.1.5 与DES的关系 3.2 分组密码的原理 3.2.1 流密码和分组密码 3.2.2 Feistel密码结构的设计动机 3.2.3 Feistel密码 3.3 数据加密标准 3.3.1 DES加密 3.3.2 DES的解密 3.3.3 雪崩效应 3.4 DES的强度 3.4.1 56 bit密钥的使用 3.4.2 DES算法的性质 3.5 差分与线性密码分析 3.5.1 差分密码分析 3.5.2 线性密码分析 3.6 分组密码设计原理 3.6.1 DES的设计准则 3.6.2 循环次数 3.6.3 函数F的设计 3.6.4 密钥调度算法 3.7 分组密码的操作方式 3.7.1 电子密码本方式 3.7.2 密码分组链接方式 3.7.3 密码反馈方式 3.7.4 输出反馈方式 3.8 推荐读物。 3.9 习题 附录3A 曲折函数(bent function) 第4章 常规加密的算法 4.1 三重DES 4.1.1 双重DES 4.1.2 两个密钥的三重DES 4.1.3 使用三个密钥的三重DES 4.2 国际数据加密算法 4.2.1 设计原理 4.2.2 IDEA加密 4.2.3 IDEA的解密 4.3 Blowfish 4.3.1 子密钥和S盒子的产生 4.3.2 加密和解密 4.3.3 讨论 4.4 RC5 4.4.1 RC5的参数 4.4.2 密钥扩展 4.4.3 加密 4.4.4 解密 4.4.5 RC5的操作方式 4.5 CAST—128 4.5.1 CAST—128的加密 4.5.2 替代盒子 4.5.3 子密钥产生 4.5.4 讨论 4.6 RC2 4.6.1 密钥扩展 4.6.2 加密 4.7 先进对称分组密码的特点 4.8 习题 第5章 使用常规加密进行保密通信 5.1 加密功能的位置 5.2 通信量的机密性 5.3 密钥分配 5.4 随机数的产生 5.5 推荐读物 5.6 习题 第二部分 公开密钥加密和散列函数 第6章 公开密钥密码编码学 6.1 公开密钥密码系统的原理 6.2 RSA算法 6.3 密钥管理 6.4 Diffie—Hellman密钥交换 6.5 椭圆曲线密码编码学 6.6 推荐读物 6.7 习题 附录6A 算法的复杂性 第7章 数论导引 7.1 素数和互为素数 7.2 模运算 7.3 费马定理和欧拉定理 7.4 检测素数 7.5 欧几里德算法 7.6 中国余数定理 7.7 离散对数 7.8 推荐读物 7.9 习题 第8章 报文鉴别与散列函数 8.1 鉴别的需求 8.2 鉴别函数 8.3 报文鉴别码 8.3.1 MAC的需求 8.3.2 基于DES的报文鉴别码 8.4 散列函数 8.5 散列函数和MAC的安全性 8.6 推荐读物 8.7 习题 附录8A 生日攻击的数学基础 8A.1 相关问题 8A.2 生日悖论 8A.3 有用的不等式 8A.4 重复问题的一般性例子 8A.5 两个相交的集合 第9章 散列算法 9.1 MD5报文摘要算法 9.2 安全的散列算法 9.3 RIPEMD-160 9.4 HMAC 9.5 习题 第10章 数字签名和鉴别协议 10.1 数字签名 10.2 鉴别协议 10.3 数字签名标准 10.4 推荐读物 10.5 习题 附录10A 数字签名算法的证明 第三部分 网络安全实践 第11章 鉴别应用 11.1 Kerberos 11.2 X.509鉴别服务 11.2.1 证书 11.3 推荐读物 11.4 习题 附录11A Kerberos加密技术 11A.1 口令到密钥的转换 11A.2 传播密码分组链接模式 第12章 电子邮件的安全性 12.1 PCP加密软件 12.2 S/MIME 12.3 推荐读物 12.4 习题 附录12A 使用ZIP的数据压缩 12A.1 压缩算法 12A.2 解压算法 附录12B Radix—64转换 附录12C PGP随机数的产生 12C.1 真随机数 12C.2 伪随机数 第13章 IP的安全性 第14章 Web安全 词汇表 英文缩写词 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>