

<<密码学与网络安全>>

图书基本信息

书名：<<密码学与网络安全>>

13位ISBN编号：9787302185840

10位ISBN编号：7302185840

出版时间：2009-1

出版时间：清华大学出版社

作者：福罗赞

页数：658

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>

## 前言

互联网作为一个世界范围的通信网络，已经在许多方面改变了我们的日常生活。一个最新的商业上的例子就是每个人都可以在线购物。万维网（WWW）还可以让我们分享信息。电子邮件的技术把世界各个角落的人联系在了一起。这种必然的发展也形成了对互联网的依赖。

互联网作为一个开放的论坛，已经产生了一些安全方面的问题。互联网需要有机密性、完整性和可信性。人们需要确保网络通信是机密的。当我们在线购物时，我们需要确保出售方是真实的。当我们把交易请求发送给银行时，我们还要保证信息的完整性不被破坏。

## <<密码学与网络安全>>

### 内容概要

《密码学与网络安全》延续了Forouzan先生一贯的风格，以通俗易懂的方式全面阐述了密码学与计算机网络安全问题所涉及的各方面内容，从全局角度介绍了计算机网络安全的概念、体系结构和模式。

《密码学与网络安全》以因特网为框架，以形象直观的描述手法，详细地介绍了密码学、数据通信和网络领域的基础知识、基本概念、基本原理和实践方法，堪称密码学与网络安全方面的经典著作。

## <<密码学与网络安全>>

### 作者简介

Behrouz A. Forouzan 先生毕业于加州大学艾尔温分校，现在是迪安那大学教授，从事计算机信息系统方面的研究工作。

此外，他还是多家公司的系统开发咨询顾问。

除本书外，Forouzan还著有多部成功的编程与网络方面的书籍，有的已经成为该领域的权威性著作，例如《TCP/IP协议族（第3版）》和《密码学与网络安全》等。

## 书籍目录

第1章 导言1.1 安全目标1.1.1 机密性1.1.2 完整性1.1.3 可用性1.2 攻击1.2.1 威胁机密性的攻击1.2.2 威胁完整性的攻击1.2.3 威胁可用性的攻击1.2.4 被动攻击与主动攻击1.3 服务和机制1.3.1 安全服务1.3.2 安全机制1.3.3 服务和机制之间的关系1.4 技术1.4.1 密码术1.4.2 密写术1.5 本书的其余部分第 部分 对称密钥加密第 部分 非对称密钥加密第 部分 完整性、验证和密钥管理第 部分 网络安全1.6 推荐阅读1.7 关键术语1.8 概要1.9 习题集第 部分 对称密钥加密第2章 密码数学 第 部分：模算法、同余和矩阵2.1 整数算法2.1.1 整数集2.1.2 二进制运算2.1.3 整数除法2.1.4 整除性2.1.5 线性丢番图方程2.2 模运算2.2.1 模算符2.2.2 余集： $Z_n$ 2.2.3 同余2.2.4 在集合 $Z_n$ 当中的运算2.2.5 逆2.2.6 加法表和乘法表2.2.7 加法集和乘法集的不同2.2.8 另外两个集合2.3 矩阵2.3.1 定义2.3.2 运算和关系2.3.3 行列式2.3.4 逆2.3.5 剩余阵2.4 线性同余2.4.1 单变量线性方程2.4.2 线性方程组2.5 推荐阅读2.6 关键术语2.7 概要2.8 习题集第3章 传统对称密钥密码3.1 导言3.1.1 Kerckhoff原理3.1.2 密码分析3.1.3 传统密码的分类3.2 代换密码3.2.1 单码代换密码3.2.2 多码代换密码3.3 换位密码3.3.1 无密钥换位密码3.3.2 有密钥的换位密码3.3.3 把两种方法组合起来3.4 流密码和分组密码3.4.1 流密码3.4.2 分组密码3.4.3 组合3.5 推荐阅读3.6 关键术语3.7 概要3.8 习题集第4章 密码数学 第 部分：代数结构4.1 代数结构4.1.1 群4.1.2 环4.1.3 域4.1.4 小结4.2  $GF(2^n)$ 域4.2.1 多项式4.2.2 运用一个生成器4.2.3 小结4.3 推荐阅读4.4 关键术语4.5 概要4.6 习题集第5章 现代对称密钥密码5.1 现代分组密码5.1.1 代换与换位5.1.2 作为置换群的分组密码5.1.3 现代分组密码的成分5.1.4 换字盒5.1.5 乘积密码5.1.6 两类乘积密码5.1.7 关于分组密码的攻击5.2 现代流密码5.2.1 同步流密码5.2.2 异步流密码5.3 推荐阅读5.4 关键术语5.5 概要5.6 习题集第6章 数据加密标准 (DES) 6.1 导言6.1.1 数据加密标准 (DES) 简史6.1.2 概观6.2 DES的结构6.2.1 初始置换和最终置换6.2.2 轮6.2.3 密码和反向密码6.2.4 示例6.3 DES分析6.3.1 性质6.3.2 设计标准6.3.3 DES的缺陷6.4 多重 DES6.4.1 双重DES6.4.2 三重DES6.5 DES的安全性6.5.1 蛮力攻击6.5.2 差分密码分析6.5.3 线性密码分析6.6 推荐阅读6.7 关键术语6.8 概要6.9 习题集第7章 高级加密标准 (AES) 7.1 导言7.1.1 高级加密标准 (AES) 简史7.1.2 标准7.1.3 轮7.1.4 数据单位7.1.5 每一个轮的结构7.2 转换7.2.1 代换7.2.2 置换7.2.3 混合7.2.4 密钥加7.3 密钥扩展7.3.1 在AES-128中的密钥扩展7.3.2 AES-192和AES-256中的密钥扩展7.3.3 密钥扩展分析7.4 密码7.4.1 源设计7.4.2 选择性设计7.5 示例7.6 AES的分析7.6.1 安全性7.6.2 可执行性7.6.3 复杂性和费用7.7 推荐阅读7.8 关键术语7.9 概要7.10 习题集第8章 应用现代对称密钥 密码的加密8.1 现代分组密码的应用8.1.1 电子密码本模式8.1.2 密码分组链接 (CBC) 模式8.1.3 密码反馈 (CFB) 模式8.1.4 输出反馈 (OFB) 模式8.1.5 计数器 (CTR) 模式8.2 流密码的应用8.2.1 RC48.2.2 A5/18.3 其他问题8.3.1 密钥管理8.3.2 密钥生成8.4 推荐阅读8.5 关键术语8.6 概要8.7 习题集第 部分 非对称密钥加密第9章 密码数学 第 部分：素数及其相关的同余方程9.1 素数9.1.1 定义9.1.2 素数的基数9.1.3 素性检验9.1.4 Euler Phi- (欧拉 $\phi(n)$ ) 函数9.1.5 Fermat (费尔马) 小定理9.1.6 Euler定理9.1.7 生成素数9.2 素性测试9.2.1 确定性算法9.2.2 概率算法9.2.3 推荐的素性检验9.3 因数分解9.3.1 算术基本定理9.3.2 因数分解方法9.3.3 Fermat方法 2489.3.4 Pollard  $p-1$ 方法9.3.5 Pollard rho方法9.3.6 更有效的方法9.4 中国剩余定理9.5 二次同余9.5.1 二次同余模一个素数9.5.2 二次同余模一个复合数9.6 指数与对数9.6.1 指数9.6.2 对数9.7 推荐阅读9.8 关键术语9.9 概要9.10 习题集第10章 非对称密钥密码学10.1 导言10.1.1 密钥10.1.2 一般概念10.1.3 双方的需要10.1.4 单向暗门函数10.1.5 背包密码系统10.2 RSA密码系统10.2.1 简介10.2.2 过程10.2.3 一些普通的例子10.2.4 针对RSA的攻击10.2.5 建议10.2.6 最优非对称加密填充 (OAEP) 10.2.7 应用10.3 RABIN密码系统10.3.1 过程10.3.2 Rabin系统的安全性10.4 ELGAMAL密码系统10.4.1 ElGamal密码系统10.4.2 过程10.4.3 证明10.4.4 分析10.4.5 ElGamal的安全性10.4.6 应用10.5 椭圆曲线密码系统10.5.1 基于实数的椭圆曲线10.5.2 基于 $GF(p)$ 的椭圆曲线10.5.3 基于 $GF(2^n)$ 的椭圆曲线10.5.4 模拟ElGamal的椭圆曲线加密系统10.6 推荐阅读10.7 关键术语10.8 概要10.9 习题集第 部分 完整性、验证和密钥管理第11章 信息的完整性和信息验证11.1 信息完整性11.1.1 文档与指纹11.1.2 信息与信息摘要11.1.3 区别11.1.4 检验完整性11.1.5 加密hash函数标准11.2 随机预言模型11.2.1 鸽洞原理11.2.2 生日问题11.2.3 针对随机预言模型的攻击11.2.4 针对结构的攻击11.3 信息验证11.3.1 修改检测码11.3.2 信息验证代码 (MAC) 11.4 推荐阅读11.5 关键术语11.6 概要11.7 习题集第12章 加密hash函数12.1 导言12.1.1 迭代hash函数12.1.2 两组压缩函数12.2 SHA-51212.2.1 简介12.2.2 压缩函数12.2.3 分析12.3 WHIRLPOOL12.3.1 Whirlpool密码12.3.2 小结12.3.3 分析12.4 推荐阅读12.5 关键术语12.6

概要12.7 习题集第13章 数字签名13.1 对比13.1.1 包含性13.1.2 验证方法13.1.3 关系13.1.4 二重性13.2 过程13.2.1 密钥需求13.2.2 摘要签名13.3 服务13.3.1 信息身份验证13.3.2 信息完整性13.3.3 不可否认性13.3.4 机密性13.4 针对数字签名的攻击13.4.1 攻击类型13.4.2 伪造类型13.5 数字签名方案13.5.1 RSA数字签名方案13.5.2 ElGamal数字签名方案13.5.3 Schnorr数字签名方案13.5.4 数字签名标准 (DSS) 13.5.5 椭圆曲线数字签名方案13.6 变化与应用13.6.1 变化13.6.2 应用13.7 推荐阅读13.8 关键术语13.9 概要13.10 习题集第14章 实体验证14.1 引言14.1.1 数据源验证与实体验证14.1.2 验证的类型14.1.3 实体验证和密钥管理14.2 口令14.2.1 固定口令14.2.2 一次性密码14.3 挑战—应答14.3.1 对称密钥密码的运用14.3.2 带密钥hash函数的应用14.3.3 非对称密钥密码的应用14.3.4 数字签名的应用14.4 零知识14.4.1 Fiat-Shamir协议14.4.2 Feige-Fiat-Shamir协议14.4.3 Guillou-Quisquater协议14.5 生物测试14.5.1 设备14.5.2 注册14.5.3 验证14.5.4 技术14.5.5 准确性14.5.6 应用14.6 推荐阅读14.7 关键术语14.8 概要14.9 习题集第15章 密钥管理15.1 对称密钥分配15.2 KERBEROS15.2.1 服务器15.2.2 操作15.2.3 不同服务器的运用15.2.4 Kerberos第五版15.2.5 领域15.3 对称密钥协定15.3.1 Diffie-Hellman密钥协定15.3.2 站对站密钥协定15.4 公钥分配15.4.1 公钥公布15.4.2 可信中心15.4.3 可信中心的控制15.4.4 认证机关15.4.5 X.50915.4.6 公钥基础设施 (PKI) 15.5 推荐阅读15.6 关键术语15.7 概要15.8 习题集第 一部分 网络安全第16章 应用层的安全性: PGP和S/MIME16.1 电子邮件16.1.1 电子邮件的构造16.1.2 电子邮件的安全性16.2 PGP16.2.1 情景16.2.2 密钥环16.2.3 PGP证书16.2.4 密钥撤回16.2.5 从环中提取消息16.2.6 PGP包16.2.7 PGP信息16.2.8 PGP的应用16.3 S/MIME16.3.1 MIME16.3.2 S/MIME16.3.3 S/MIME的应用16.4 推荐阅读16.5 关键术语16.6 概要16.7 习题集第17章 传输层的安全性: SSL和TLS17.1 SSL结构17.1.1 服务17.1.2 密钥交换算法17.1.3 加密/解密算法17.1.4 散列算法17.1.5 密码套件17.1.6 压缩算法17.1.7 加密参数的生成17.1.8 会话和连接17.2 4个协议17.2.1 握手协议17.2.2 改变密码规格协议17.2.3 告警协议17.2.4 记录协议17.3 SSL信息构成17.3.1 改变密码规格协议17.3.2 告警协议17.3.3 握手协议17.3.4 应用数据17.4 传输层安全17.4.1 版本17.4.2 密码套件17.4.3 加密秘密的生成17.4.4 告警协议17.4.5 握手协议17.4.6 记录协议17.5 推荐阅读17.6 关键术语17.7 概要17.8 习题集第18章 网络层的安全: IPsec18.1 两种模式18.2 两个安全协议18.2.1 验证文件头 (AH) 18.2.2 封装安全载荷 (ESP) 18.2.3 IPv4和IPv618.2.4 AH和ESP18.2.5 IPsec提供的服务18.3 安全关联18.3.1 安全关联的概念18.3.2 安全关联数据库 (SAD) 18.4 安全策略18.5 互联网密钥交换 (IKE) 18.5.1 改进的Diffie-Hellman密钥交换18.5.2 IKE阶段18.5.3 阶段和模式18.5.4 阶段 : 主模式18.5.5 阶段 : 野蛮模式18.5.6 阶段 : 快速模式18.5.7 SA算法18.6 ISAKMP18.6.1 一般文件头18.6.2 有效载荷18.7 推荐阅读18.8 关键术语18.9 概要18.10 习题集附录A ASCII附录B 标准与标准化组织附录C TCP/IP套件附录D 初等概率附录E 生日问题附录F 信息论附录G 不可约多项式与本原多项式列举附录H 小于10 000的素数附录I 整数的素因数附录J 小于1000素数的一次本原根列表附录K 随机数生成器附录L 复杂度附录M ZIP附录N DES差分密码分析和DES线性密码分析附录O 简化DES (S-DES) 附录P 简化AES (S-AES) 附录Q 一些证明术语表参考文献

章节摘录

第1章 导言 目标 本章的几个目标是：  
· 明确三种安全目标  
· 明确威胁安全目标的几种攻击  
· 明确安全服务的内容及其和三种安全目标的联系  
· 介绍两种实现安全机制的技术：密码术和密写术  
我们生活在信息时代，在生活的各方面都需要保持信息畅通。换句话说，信息是一种资产，它和其他任何资产一样具有价值，需要被保护以避免攻击。

为了安全，信息要被隐藏起来以避免未经授权的访问（机密性），被保护起来以避免未经授权的更改（完整性），还要保证对授权实体随时可用（可用性）。

直到几十年前，信息才被组织在一起并保存在物理文档中。访问人被限制在该组织内已被授权并可信赖的少数几个人中，这样就实现了文档的机密性。

随着计算机的出现，信息储存被电子化。信息并不是存储于物理介质之中，而是存于计算机中。然而三种安全要求却并未因此而改变。

存储于计算机中的信息要求具有机密性、完整性和有效性，然而实现这三种要求的方法各不相同并具有挑战性。

过去的20年中，计算机网络在信息应用上掀起了一场革命。信息是分散的，利用计算机网络，一个被授权的人可以从很远的地方发送或接收信息。上述三种要求（机密性、完整性和可用性）不但并未改变，而且具有了新的含义。不仅在信息被保存在计算机当中时要确保其机密性，而且应当有一种方法，能使信息在由一台计算机被发送到另一台计算机的过程中，也能保证其机密性。

在本章中，我们首先讨论信息安全的三个主要目标，然后再来了解一下什么样的攻击才能对这三个目标构成威胁，并且进一步讨论与这三种安全目标有关的安全服务。最后，我们详细论述提供安全服务的机制，同时介绍用来实现安全机制的技术。

## <<密码学与网络安全>>

### 编辑推荐

《密码学与网络安全》作者Behrouz A Forouzan运用一种易于理解的写作风格和直观的表述方法，为我们全面介绍了密码学与网络安全方面的概念。他把难于理解的教学概念穿插在了中间的章节中，这样既为后面章节的学习打下必要的数学基础，又紧密结合密码学，使枯燥的数学概念变得妙趣横生。

概念阐释直观、易懂稗序可用性强，便于学生实践最新的网络安全技术，贴近实际。

《密码学与网络安全》（包括其中文导读英文版）可作为大学本科通信相关专业的教科书，也可作为对密码学与网络安全有兴趣的读者的自学用书。



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>