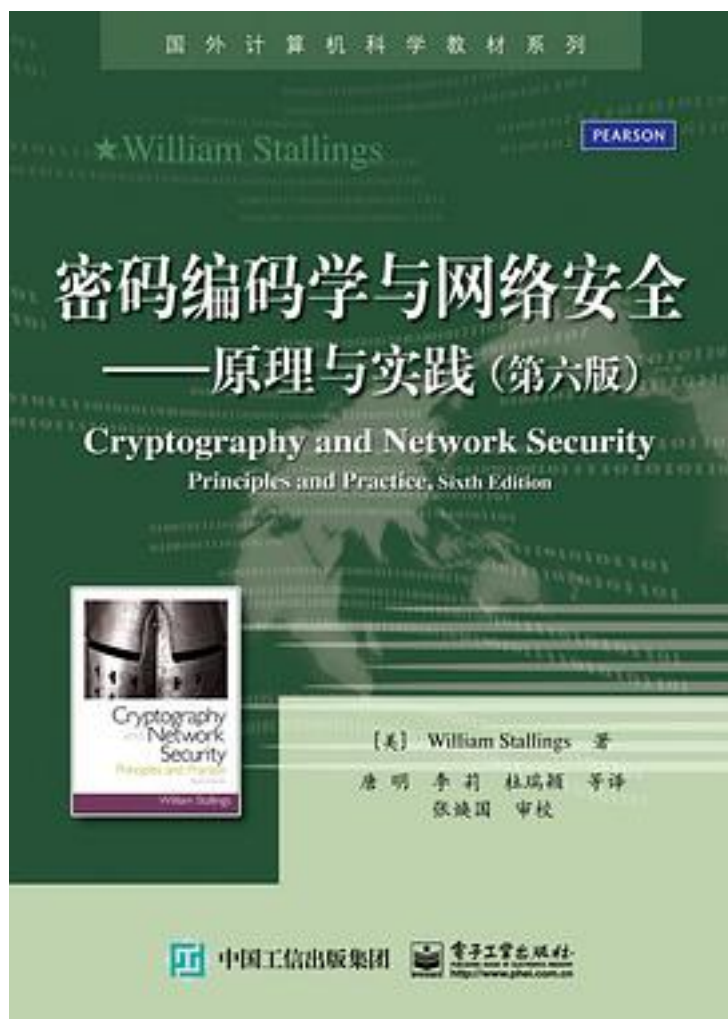


密码编码学与网络安全 (第6版)



[密码编码学与网络安全 \(第6版\) 下载链接1](#)

著者:William Stallings

出版者:电子工业出版社

出版时间:2015-3

装帧:

isbn:9787121246678

本书系统介绍了密码编码学与网络安全的基本原理和应用技术。全书的内容分为以下七

个部分：对称密码部分讨论了对称加密的算法和设计原则；公钥密码部分讨论了公钥密码的算法和设计原则；密码学中的数据完整性算法部分讨论了密码学Hash函数、消息认证码和数字签名；相互信任部分讨论了密钥管理和用户认证技术；网络安全与Internet安全部分讨论了应用密码算法和安全协议为网络和Internet提供安全；系统安全部分讨论了保护计算机系统免受各种安全威胁的技术；法律与道德问题部分讨论了与计算机和网络安全相关的法律与道德问题。本书的第六版与第五版相比，书的章节组织基本不变，但增加了许多新内容。如增加了云安全、新Hash函数标准SHA-3、真随机数产生器、移动设备安全等新内容。而且许多章节的论述方法也做了调整，使之更贴近技术实际，使读者更易理解。

作者介绍:

目录: 目录

第0章 读者导引

0.1 本书概况

0.2 读者和教师导读

0.3 Internet和Web资源

0.4 标准

第1章 概览

1.1 计算机安全概念

1.2 OSI安全框架

1.3 安全攻击

1.4 安全服务

1.5 安全机制

1.6 网络安全模型

1.7 推荐读物

1.8 关键术语、思考题和习题

第一部分 对称密码

第2章 传统加密技术

2.1 对称密码模型

2.2 代替技术

2.3 置换技术

2.4 转轮机

2.5 隐写术

2.6 推荐读物

2.7 关键术语、思考题和习题

第3章 分组密码和数据加密标准

3.1 传统分组密码结构

3.2 数据加密标准

3.3 DES的一个例子

3.4 DES的强度

3.5 分组密码的设计原理

3.6 推荐读物

3.7 关键术语、思考题和习题

第4章 数论和有限域的基本概念

4.1 整除性和除法

4.2 欧几里得算法

4.3 模运算

4.4 群、环和域

4.5 有限域GF(p)

4.6 多项式运算

4.7 有限域GF(2ⁿ)

- 4.8 推荐读物
- 4.9 关键术语、思考题和习题
- 附录4A mod的含义
- 第5章 高级加密标准
- 5.1 有限域算术
- 5.2 AES的结构
- 5.3 AES的变换函数
- 5.4 AES的密钥扩展
- 5.5 一个AES例子
- 5.6 AES的实现
- 5.7 推荐读物
- 5.8 关键术语、思考题和习题
- 附录5A 系数在GF(28)中的多项式
- 附录5B 简化AES
- 第6章 分组密码的工作模式
- 6.1 多重加密与三重DES
- 6.2 电码本模式
- 6.3 密文分组链接模式
- 6.4 密文反馈模式
- 6.5 输出反馈模式
- 6.6 计数器模式
- 6.7 用于面向分组的存储设备的XTS-AES模式
- 6.8 推荐读物
- 6.9 关键术语、思考题和习题
- 第7章 伪随机数的产生和流密码
- 7.1 随机数产生的原则
- 7.2 伪随机数发生器
- 7.3 使用分组密码的伪随机数发生器
- 7.4 流密码
- 7.5 RC4算法
- 7.6 真随机数发生器
- 7.7 推荐读物
- 7.8 关键术语、思考题和习题
- 第二部分 公钥密码
- 第8章 数论入门
- 8.1 素数
- 8.2 费马定理和欧拉定理
- 8.3 素性测试
- 8.4 中国剩余定理
- 8.5 离散对数
- 8.6 推荐读物
- 8.7 关键术语、思考题和习题
- 第9章 公钥密码学与RSA
- 9.1 公钥密码体制的基本原理
- 9.2 RSA算法
- 9.3 推荐读物
- 9.4 关键术语、思考题和习题
- 附录9A 算法复杂性
- 第10章 密钥管理和其他公钥密码体制
- 10.1 Diffie-Hellman密钥交换
- 10.2 ElGamal密码体制
- 10.3 椭圆曲线算术
- 10.4 椭圆曲线密码学
- 10.5 基于非对称密码的伪随机数发生器

- 10.6 推荐读物
- 10.7 关键术语、思考题和习题
- 第三部分 密码学中的数据完整性算法
- 第11章 密码学Hash函数
 - 11.1 密码学Hash函数的应用
 - 11.2 两个简单的Hash函数
 - 11.3 需求和安全性
 - 11.4 基于分组密码链接的Hash函数
 - 11.5 安全Hash算法 (SHA)
 - 11.6 SHA-3
 - 11.7 推荐读物
 - 11.8 关键术语、思考题和习题
- 第12章 消息认证码
 - 12.1 对消息认证的要求
 - 12.2 消息认证函数
 - 12.3 对消息认证码的要求
 - 12.4 MAC的安全性
 - 12.5 基于Hash函数的MAC：HMAC
 - 12.6 基于分组密码的MAC：DAA和CMAC
 - 12.7 认证加密：CCM和GCM
 - 12.8 密钥封装
 - 12.9 使用Hash函数和MAC的伪随机数发生器
 - 12.10推荐读物
 - 12.11关键术语、思考题和习题
- 第13章 数字签名
 - 13.1 数字签名简介
 - 13.2 ElGamal数字签名方案
 - 13.3 Schnorr数字签名方案
 - 13.4 数字签名标准
 - 13.5 椭圆曲线数字签名算法
 - 13.6 RSA-PSS数字签名算法
 - 13.7 推荐读物
 - 13.8 关键术语、思考题和习题
- 第四部分 相互信任
- 第14章 密钥管理和分发
 - 14.1 基于对称加密的对称密钥分发
 - 14.2 基于非对称加密的对称密钥分发
 - 14.3 公钥分发
 - 14.4 X.509证书
 - 14.5 公钥基础设施
 - 14.6 推荐读物
 - 14.7 关键术语、思考题和习题
- 第15章 用户认证
 - 15.1 远程用户认证原理
 - 15.2 基于对称加密的远程用户认证
 - 15.3 Kerberos
 - 15.4 基于非对称加密的远程用户认证
 - 15.5 联合身份管理
 - 15.6 个人身份验证
 - 15.7 推荐读物
 - 15.8 关键术语、思考题和习题
- 第五部分 网络安全与Internet安全
- 第16章 网络访问控制和云安全
 - 16.1 网络访问控制

- 16.2 可扩展认证协议
- 16.3 IEEE 802.1X基于端口的网络访问控制
- 16.4 云计算
- 16.5 云安全所面临的威胁和对策
- 16.6 云中的数据保护
- 16.7 云安全即服务
- 16.8 推荐读物
- 16.9 关键术语、思考题和习题
- 第17章 传输层安全
- 17.1 Web安全性思考
- 17.2 安全套接层
- 17.3 传输层安全
- 17.4 HTTPS
- 17.5 SSH
- 17.6 推荐读物
- 17.7 关键术语、思考题和习题
- 第18章 无线网络安全
- 18.1 无线网络安全概述
- 18.2 移动设备安全
- 18.3 IEEE 802.11无线网络概述
- 18.4 IEEE 802.11i无线局域网安全
- 18.5 推荐读物
- 18.6 关键术语、思考题和习题
- 第19章 电子邮件安全
- 19.1 PGP
- 19.2 S/MIME
- 19.3 DKIM
- 19.4 推荐读物
- 19.5 关键术语、思考题和习题
- 附录19A Radix-64转换
- 第20章 IP安全性
- 20.1 IP安全概述
- 20.2 IP安全策略
- 20.3 封装安全有效载荷
- 20.4 组合安全关联
- 20.5 Internet密钥交换
- 20.6 密码学套件
- 20.7 推荐读物
- 20.8 关键术语、思考题和习题
- 附录A 用于密码学和网络安全教学的项目
- 附录B Sage示例
- 参考文献
- 索引
- 在线部分
- 第六部分 系统安全
- 第21章 恶意软件
- 21.1 恶意软件类型
- 21.2 传播-感染内容-病毒
- 21.3 传播-利用漏洞-蠕虫
- 21.4 传播-社会工程-垃圾邮件和特洛伊木马
- 21.5 有效载荷-系统破坏
- 21.6 有效载荷-攻击代理-僵尸程序
- 21.7 有效载荷-信息窃取-键盘记录器、网络钓鱼和间谍软件
- 21.8 有效载荷-隐藏

21.9 防范措施
21.10 分布式拒绝服务攻击
21.11 推荐读物
21.12 关键术语、思考题和习题
第22章 入侵者
22.1 入侵者概述
22.2 入侵检测
22.3 口令管理
22.4 推荐读物
22.5 关键术语、思考题和习题
第23章 防火墙
23.1 防火墙的必要性
23.2 防火墙的特性
23.3 防火墙的分类
23.4 防火墙基础
23.5 防火墙的位置与配置
23.6 推荐读物
23.7 关键术语、思考题和习题
第七部分 法律与道德问题
第24章 法律与道德
24.1 网络犯罪和计算机犯罪
24.2 知识产权
24.3 隐私
24.4 道德问题
24.5 推荐读物
24.6 关键术语、思考题和习题
附录24A 信息隐私权实践标准
附录C Sage习题
附录D 标准和标准化组织
附录E 线性代数的基本概念
附录F 保密和安全的测度
附录G 简化DES
附录H AES的评估准则
附录I 简化AES的补充
附录J 背包公钥算法
附录K 数字签名算法的证明
附录L TCP/IP和OSI
附录M Java密码函数API
附录N MD5 Hash函数
附录O 使用ZIP的数据压缩
附录P PGP的补充
附录Q 国际参考字母表
附录R RSA算法的证明
附录S 数据加密标准 (DES)
附录T Kerberos加密技术
附录U 生日攻击的数学基础
附录V SHA-3评估标准
术语表
常用首字母缩略词
• • • • • ([收起](#))

标签

密码学

信息安全

计算机

密码

编程

加密

黑客

技术

评论

好书，但是中文版被张焕国老师的一群研究生翻译毁了，很多语句都不通，翻译很晦涩

教材，书是好书，翻译多处不通，怀疑译者自己懂了么.....

原书还不错，这本翻译晦涩，错别字多

安全学课上用的教材，简明易懂，啃得很开心～

[密码编码学与网络安全 \(第6版\) 下载链接1](#)

书评

[密码编码学与网络安全 \(第6版\) 下载链接1](#)