

<<程序员密码学>>

图书基本信息

书名：<<程序员密码学>>

13位ISBN编号：9787111216605

10位ISBN编号：7111216601

出版时间：2007-7

出版时间：机械工业

作者：丹尼斯

页数：328

译者：沈晓斌

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>

## <<程序员密码学>>

### 内容概要

是目前市面上惟一一本把密码学算法的理论和实现结合在一起的书，也是惟一一本能够如此深入浅出地把这两个方面融合到一起的书，没有深厚的程序设计功力和广博的密码学理论知识是不可能写出这样一书的。

无论对于需要开发安全产品的开发者，还是密码学相关研究人员来说，《程序员密码学》均值得一读，它能对安全产品开发工作以及密码学理论研究工作起到辅助作用，并可以达到事半功倍的效果。

## 书籍目录

第1章 概述 1.1 简介 1.2 威胁模型 1.3 什么是密码学 1.4 资产管理 1.4.1 保密性和认证 1.4.2 数据的生命周期 1.5 常识 1.6 开发工具 1.7 总结 1.8 本书的组织结构 1.9 常见问题 第2章 ASN.1 2.1 ASN.1概述 2.2 ASN.1语法 2.2.1 ASN.1显式值 2.2.2 ASN.1容器 2.2.3 ASN.1修改器 2.2.4 ASN.1数据类型 2.3.1 ASN.1头字节 2.3.2 ASN.1长度编码 2.3.3 ASN.1布尔类型 2.3.4 ASN.1整数类型 2.3.5 ASN.1位串类型 2.3.6 ASN.1八位位组串类型 2.3.7 ASN.1空类型 2.3.8 ASN.1对象标识符类型 2.3.9 ASN.1序列和集合类型 2.3.10 ASN.1可打印字符串和IA5String类型 2.3.11 ASN.1世界协调时类型 2.4 实现 2.4.1 ASN.1长度程序 2.4.2 ASN.1原始编码器 2.5 总结 2.5.1 创建链表 2.5.2 链表 2.5.3 Flexi链表 2.5.4 其他提供者 2.6 常见问题 第3章 随机数生成 3.1 简介 3.2 熵的度量 3.2.1 位计数 3.2.2 字计数 3.2.3 间隙计数 3.2.4 自相关测试 3.3 它能有多糟 3.4 RNG设计 3.4.1 硬件 3.4.2 RNG数据收集 3.4.3 RNG处理和输出 3.4.4 RNG估算 3.4.5 RNG的设置 3.5 PRNG算法 3.5.1 PRNG的设计 3.5.2 PRNG的攻击 3.5.3 Yarrow PRNG 3.5.4 Fortuna PRNG 3.5.5 NIST的DRBG 3.6 总结 3.6.1 RNG与PRNG 3.6.2 PRNG的使用 3.6.3 示例平台 3.7 常见问题 第4章 高级加密标准 4.1 简介 4.1.1 分组密码 4.1.2 AES的设计 4.2 实现 4.2.1 一个8位的实现 4.2.2 优化的8位实现 4.2.3 优化的32位实现 4.3 实用的攻击 4.3.1 侧信道 4.3.2 处理器缓存 4.3.3 Bernstein攻击 4.3.4 Osvik攻击 4.3.5 挫败侧信道 4.4 链接模式 4.4.1 密码分组链接 4.4.2 计数器模式 4.4.3 选择一个链接模式 4.5 总结 4.5.1 荒诞的说法 4.5.2 提供者 4.6 常见问题 第5章 散列函数 5.1 简介 5.1.1 散列摘要长度 5.2 SHS的设计与实现 5.2.1 MD强化 5.2.2 SHA-1的设计 5.2.3 SHA-256的设计 5.2.4 SHA-512的设计 5.2.5 SHA-224的设计 5.2.6 SHA-384的设计 5.2.7 零复制散列 5.3 PKCS #5 密钥衍生 5.4 总结 5.4.1 散列算法可以做哪些事 5.4.2 散列算法不能用来做哪些事 5.4.3 和口令一起工作 5.4.4 性能上的考虑 5.4.5 PKCS #5的例子 5.5 常见问题 第6章 消息认证码算法 6.1 简介 6.2 安全准则 6.3 标准 6.4 分组消息认证码 6.4.1 CMAC的安全性 6.4.2 CMAC的设计 6.5 散列消息认证码 6.5.1 HMAC的设计 6.5.2 HMAC的实现 6.6 总结 6.6.1 MAC函数可以做哪些事 6.6.2 MAC函数不能用来做哪些事 6.6.3 CMAC与HMAC 6.6.4 重放保护 6.6.5 先加密再MAC 6.6.6 加密和认证 6.7 常见问题 第7章 加密和认证模式 7.1 简介 7.1.1 加密和认证模式 7.1.2 安全目标 7.1.3 标准 7.2 设计与实现 7.2.1 额外的认证数据 7.2.2 GCM的设计 7.2.3 GCM的实现 7.2.4 GCM的优化 7.2.5 CCM的设计 7.2.6 CCM的实现 7.3 总结 7.3.1 这些模式可以用来做哪些事 7.3.2 选择一个Nonce 7.3.3 额外的认证数据 7.3.4 MAC标记数据 7.3.5 构造举例 7.4 常见问题 第8章 大整数算术 8.1 简介 8.2 什么是BigNum 8.3 算法 8.3.1 表示 8.3.2 乘法 8.3.3 平方 8.3.4 Montgomery约简 8.4 总结 8.4.1 核心算法 8.4.2 大小与速度 8.4.3 BigNum库的性能 8.4.4 TomsFastMath算法库 8.5 常见问题 第9章 公钥算法 9.1 简介 9.2 公钥密码的目标 9.2.1 保密性 9.2.2 不可否认和真实性 9.3 RSA公钥密码 9.3.1 RSA简述 9.3.2 PKCS #1 9.3.3 RSA的安全 9.3.4 RSA参考资料 9.4 椭圆曲线密码学 9.4.1 什么是椭圆曲线 9.4.2 椭圆曲线代数 9.4.3 椭圆曲线加密系统 9.4.4 椭圆曲线的性能 9.5 总结 9.5.1 ECC与RSA 9.5.2 标准 9.5.3 参考资料 9.6 常见问题

## 编辑推荐

信息安全越来越受到人们的重视，对信息安全的基石：密码学的研究也是如火如荼。但是，许多信息安全软硬件产品的开发者并不是专业的密码学研究人员。

虽然他们擅长程序设计，而且现在也有许多各种各样的密码学算法库，如LibTomCrypt、Crypto++，但是，由于缺少一定的密码学理论知识以及对密码学算法的准确理解，因此在实现各种复杂的密码学算法时，经常会对算法进行不当的使用，而这又往往会导致在其开发的产品中存在各种潜在的漏洞及安全风险。

另一方面，许多密码学理论工作者在实现密码学算法时，由于缺少程序设计方面的知识，在算法实现的易用性和高效性上遇到了不少障碍，从而也会导致其实现上存在不少的安全缺陷。

《程序员密码学》的出版恰好可以解决上述问题，它在程序员和密码学研究人员之间架起了一座桥梁，使他们能够轻松地在理论和实践之间进行角色转换，并且将会缓解信息安全业界的种种尴尬。书中涉及密码学的各个研究方向，分组密码、散列函数、公钥密码以及相关的攻击，同时也讲解了密码学算法实现上常用的ASN.1编码、大整数算术相关内容。

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>