

<<信息安全工程>>

图书基本信息

书名：<<信息安全工程>>

13位ISBN编号：9787560624327

10位ISBN编号：7560624324

出版时间：2010-9

出版时间：李晖、庞辽军、裴庆祺、李慧贤 西安电子科技大学出版社 (2010-09出版)

作者：李晖等著

页数：406

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>

## <<信息安全工程>>

### 内容概要

《信息安全工程》由庞辽军、裴庆祺、李慧贤主编，并以信息安全理论为基础，以实际工程应用为目标，有针对性、有选择性地介绍了已经被普遍应用且实用有效的安全算法、协议和系统，并给出了一些实际工程应用中积累的经验和教训。

《信息安全工程》首先介绍了当前信息安全的概念及其内涵和外延、信息安全的框架模型和安全需求、信息安全的相关技术等；然后介绍了当前解决信息安全问题常用的一些策略和实用技术，如密码算法、PKI技术、完整性技术、信息隐藏技术、生物认证技术等；接着结合系统工程方法，介绍了信息安全标准状况和现有的安全模型；最后给出了国内外解决信息安全问题的一些成功案例，包括WLAN、WMAN和WSN安全技术及WAPI方案等。

《信息安全工程》的特点是：以工程应用为载体，融理论于工程；借助于流行的安全系统，而不是孤立地介绍各种安全算法。

《信息安全工程》可作为高等院校相关专业的本科生教材，也可作为相关专业的研究生教材，同时还可作为从事网络与信息安全技术工作的广大科技人员的参考书。

## 书籍目录

第1章 信息安全概述1.1 信息安全的重要性1.2 信息安全的基本概念1.2.1 安全威胁1.2.2 ISO信息安全属性1.2.3 美国NIJ信息安全属性1.2.4 实际可用的信息安全属性1.2.5 信息安全的内容1.2.6 ISO信息安全体系结构1.3 信息安全的基本措施1.3.1 密码技术1.3.2 安全控制技术1.3.3 安全防范技术第2章 密码学概述2.1 基本概念2.2 密码体制分类2.3 代换密码2.3.1 简单的代换密码2.3.2 多表密码2.3.3 弗纳姆密码2.4 换位密码2.5 古典密码第3章 信息安全数学基础3.1 信息论3.1.1 基本概念3.1.2 熵的性质3.2 数论3.2.1 素数与互素数3.2.2 同余与模算术3.2.3 大素数求法3.3 有限域3.3.1 基本概念3.3.2 有限域上的线性代数3.4 指数运算和对数运算3.4.1 快速指数运算3.4.2 离散对数计算第4章 分组密码算法4.1 基本概念4.2 DES算法4.2.1 历史背景4.2.2 算法描述4.2.3 加解密过程4.2.4 DES的变型4.3 RC4算法4.3.1 历史背景4.3.2 算法描述4.3.3 WEP协议和TKIP协议4.4 AES算法4.4.1 历史背景4.4.2 Rijndael密码概述4.4.3 Rijndael密码的内部函数4.4.4 快速而安全的实现4.4.5 AES对应用密码学的积极影响4.5 IDEA算法4.5.1 概述4.5.2 算法原理4.5.3 IDEA的安全性4.6 SMS4算法4.6.1 术语说明4.6.2 轮函数F4.6.3 加解密算法4.6.4 密钥扩展算法4.6.5 加密实例4.7 加密模式4.7.1 电码本(ECB)模式4.7.2 密码分组链接(CBC)模式4.7.3 密码反馈(CFB)模式4.7.4 输出反馈(OFB)模式4.7.5 补偿密码本(OCB)模式4.7.6 计数器(CTR)模式4.7.7 工作模式比较4.7.8 两种安全实用的混合模式第5章 公钥密码算法5.1 公钥密码技术5.1.1 公钥密码算法的基本原理5.1.2 基本概念5.1.3 公钥的优点5.1.4 基本服务5.1.5 理论基础5.2 单向陷门函数5.2.1 单向函数的定义5.2.2 单向陷门函数的定义5.2.3 公钥系统5.2.4 用于构造双钥密码的单向函数5.3 Diffie-Hellman密钥交换协议5.3.1 历史背景5.3.2 协议描述5.3.3 算法说明5.3.4 安全性分析5.3.5 DH协议应用的典型案例5.4 RSA算法5.4.1 历史背景5.4.2 算法描述5.4.3 算法说明5.4.4 RSA实现方法5.4.5 RSA的安全性5.5 ElGamal算法5.5.1 算法描述5.5.2 安全性5.6 Rabin算法和Williams算法5.6.1 Rabin算法5.6.2 Williams算法5.7 NTRU算法5.7.1 NTRU算法参数5.7.2 NTRU密码算法5.7.3 安全性5.8 椭圆曲线密码体制(ECC)5.8.1 基本原理5.8.2 基础知识5.8.3 椭圆曲线5.8.4 椭圆曲线上的加法5.8.5 密码学中的椭圆曲线5.8.6 简单的加密 / 解密5.8.7 ECC与RSA的比较5.9  $1:n$  公钥体制5.9.1 历史背景 : 5.9.2 基于分组算法的  $1:n$  公钥体制5.9.3 基于Hash函数的  $1:n$  公钥体制5.10  $(t, n)$  秘密共享体制5.10.1 历史背景5.10.2 Shamir的门限秘密共享方案5.10.3 Zheng的签密方案及其改进5.10.4 基于ID的秘密共享方案第6章 数字签名6.1 数字签名的相关概念6.2 数字信封和数字签名6.2.1 数字签名原理6.2.2 数字签名应用实例6.3 RSA签名算法6.3.1 算法描述6.3.2 安全性6.4 ElGamal签名算法6.4.1 算法描述6.4.2 安全性6.5 Schnorr签名算法6.5.1 算法描述6.5.2 Schnorr签名与ElGamal签名的不同点6.6 Rabin签名算法6.6.1 算法描述6.6.2 安全性6.7 DSS签名算法6.7.1 概况6.7.2 基本框图6.7.3 算法描述6.7.4 DSS签名和验证框图6.7.5 相关说明6.8 盲签名6.8.1 安全盲签名6.8.2 盲签名的应用6.8.3 信封6.8.4 盲签名算法6.9 门限数字签名6.9.1 系统参数6.9.2 密钥生成协议6.9.3 个体签名生成协议.....第7章 杂凑函数第8章 公钥基础设施第9章 基于身份的公钥体制第10章 信息隐藏与数字水印第11章 基于生物认证技术第12章 安全协议第13章 安全标准及模型第14章 常见的安全系统第15章 信息安全评估参考文献

## 章节摘录

版权页：插图：1.密钥的产生和分配在密钥的产生过程中，关键是随机性，要求尽可能用客观的、物理的方法产生密钥，并尽可能用完备的统计方法检验密钥的随机性，使不随机的密钥序列的出现概率能够最小。

密钥的分配是密钥管理中最大的问题。

密钥必须通过最安全的信道进行分配，指派非常可靠的信使携带密钥来分配给互相通信的各用户的人工方式不再适用，因为随着用户的增多和通信量的增大，密钥更换十分频繁（密钥必须定期更换才能做到安全可靠），所以密钥在网内的自动分配方法便应运而生。

在网内，密钥可在用户之间直接实现分配，也可通过密钥分配中心（KDC，KeyDistributionCenter）分配。

用户甲向密钥分配中心发送明文，说明想和用户乙通信，也就是向KDC申请会话时使用的会话密钥。KDC收到申请后，从用户专用的主密钥文件中找出用户甲和乙的主密钥，同时产生甲和乙通信所用的会话密钥，分别用甲、乙的主密钥加密会话密钥并发送给甲、乙双方，甲和乙即可用会话密钥进行保密通信。

KDC可以为每对用户每次通信时产生一个新的会话密钥，这就使得破译密文变得十分困难。

主密钥是用来保护会话密钥的，因此主密钥也不能在不进行更换的情况下长期使用。

2.密钥的注入密钥的注入可采用键盘、软盘、磁卡、磁条、智能卡、USB.Key、专用设备等方式。

对密钥的注入应予以严格保护，注入过程应在一个封闭的、保密的环境，注入人员应当可靠。

操作时，只有在输入合法的口令后才可开始注入，重要的密钥应当由多人、多批次分开注入完成，不允许存在任何可能导出密钥的残留信息，一旦窃取者试图读出或分析推算出注入的密钥，密钥就会自行销毁。

3.密钥的存储与销毁在密钥产生以后，需要以密文形式存储密钥。

密钥的存储方法有两种：一种是让密钥存储在密码装置中，这种方法需大量存储和频繁更换密钥，实际操作过程十分繁琐；另一种方法是运用一个主密钥来保护其他密钥，这种方法可将主密钥存储在密码装置中，而将数量相当多的数据加密密钥存储在限制访问权限的密钥表中，从而既保证了密钥的安全性与保密性，又有利于密钥的管理。

此外，在密钥的存储过程中，加、解密的操作口令应由密码操作人员掌握；加密设备应有物理保护措施，如失电保护等；非法使用加密设施时应有审核手段；采用软件加密形式时，应有软件保护措施。

对使用时间过长或已经失效的密钥，应及时销毁。

<<信息安全工程>>

编辑推荐

《信息安全工程》：高等学校电子与通信类专业规划教材

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>