

<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787030258410

10位ISBN编号：703025841X

出版时间：2009-11

出版时间：科学出版社

作者：林东岱，曹天杰 著

页数：215

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>

## &lt;&lt;应用密码学&gt;&gt;

## 前言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

” 计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。

数字化的生存方式席卷全球。

农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。

古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。

电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。

治水、训火、利用核能都曾经经历了多么漫长的时日。

不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。

但是，工具的不完善，会限制这些使用价值的真正发挥。

信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾驭技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。

传统社会存在的不文明、暴力，在信息空间也同样存在。

在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产；以达到其贪婪的目的。

人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。

因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。

什么是信息安全？

怎样才能保障信息安全？

这些问题都是严肃的科学和技术问题。

面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。

我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

## <<应用密码学>>

### 内容概要

《应用密码学》是在作者多年从事应用密码学教学和科研工作基础上撰写而成，书中全面、系统、准确地讲述了现代密码学的基本概念、理论和算法。

全书共分11章，内容包括：密码学概述、经典密码学、密码学的信息论基础、序列密码、分组密码、Hash函数、消息认证码、公钥密码、数字签名、侧信道攻击以及密码协议。每章均配有习题，以帮助读者掌握本章重要知识点并加以巩固。

《应用密码学》语言精炼，概念准确，内容全面，讲述的算法既包括密码学的经典算法，也包括了密码学领域的最新标准化算法。

《应用密码学》可作为高等院校信息安全、信息对抗、计算机科学与技术、数学等专业的本科生及研究生教材，也可供信息安全领域的工程技术人员参考。

## &lt;&lt;应用密码学&gt;&gt;

## 书籍目录

第1章 密码学概述1.1 密码学的基本概念1.2 密码体制1.3 密码分析1.3.1 攻击密码系统的方法1.3.2 破译密码的类型1.4 密码体制的安全性习题第2章 经典密码学2.1 替换密码体制2.1.1 单表替换密码2.1.2 多表替换密码2.2 置换密码体制2.3 经典密码体制的分析2.3.1 统计特性2.3.2 单表密码体制的统计分析2.3.3 多表密码体制的统计分析习题第3章 密码学的信息论基础3.1 概率论基础3.2 完全保密性3.3 信息的度量(信息熵)3.3.1 信息论的相关概念3.3.2 信息的度量3.4 熵的基本性质3.5 伪密钥与唯一解距离3.6 乘积密码体制习题第4章 序列密码4.1 序列密码的基本概念4.2 密钥流与密钥生成器4.3 线性反馈移位寄存器序列4.4 线性移位寄存器的一元多项式表示4.5 随机性概念与m序列的伪随机性习题第5章 分组密码5.1 分组密码的基本概念5.2 数据加密标准DES5.2.1 DES加密算法概述5.2.2 DES加密过程描述5.2.3 DES解密过程5.2.4 DES子密钥生成5.2.5 DES的安全性5.2.6 三重DES5.3 高级加密标准AES5.3.1 AES的加密变换5.3.2 AES的解密变换5.3.3 AES密钥编排5.4 国际数据加密算法IDEA5.4.1 IDEA算法描述5.4.2 IDEA算法的解密5.4.3 IDEA密钥生成5.5 SMS4密码算法5.5.1 算法描述5.5.2 密钥扩展5.6 分组密码的工作模式5.6.1 电子密码本模式(ECB)5.6.2 密码分组链接模式(CBC)5.6.3 密码反馈模式(CFB)5.6.4 输出反馈模式(OFB)5.6.5 记数模式(CTR)5.7 分组密码分析技术5.7.1 代换-置换网络5.7.2 线性密码分析5.7.3 差分密码分析习题第6章 Hash函数6.1 Hash函数的性质6.1.1 Hash函数的性质6.1.2 生日攻击6.1.3 迭代Hash函数的结构6.2 Hash函数实例6.2.1 MD5散列函数6.2.2 安全Hash算法6.3 Hash函数的应用举例习题第7章 消息认证码7.1 消息认证码的构造7.1.1 基于分组密码的MAC7.1.2 基于带密钥的Hash函数的MAC7.2 MAC函数的安全性7.3 消息认证码的应用习题第8章 公钥密码8.1 公钥密码的基本概念8.1.1 公钥密码体制的原理8.1.2 公钥密码算法应满足的要求8.1.3 对公钥密码的攻击8.2 RSA密码体制8.2.1 加密算法描述8.2.2 RSA算法中的计算问题8.2.3 对RSA的攻击8.2.4 RSA-OAEP加密标准8.3 ElGamal密码体制8.3.1 ElGamal算法8.3.2 ElGamal公钥密码体制的安全性8.4 椭圆曲线密码体制8.4.1 Diffie-Hellman公钥系统8.4.2 Menezes-Vanstone公钥密码体制8.4.3 椭圆曲线密码体制的优点8.5 基于身份的加密体制8.5.1 基于身份的密码学概述8.5.2 基于身份的加密方案的定义8.5.3 BF-IBE方案习题第9章 数字签名9.1 数字签名的基本概念9.2 RSA签名9.2.1 利用RSA密码实现数字签名9.2.2 对RSA数字签名的攻击9.2.3 RSA签名标准PSS9.3 数字签名标准DSS9.3.1 DSS的基本方式9.3.2 数字签名算法DSA9.4 其他数字签名方案9.4.1 离散对数签名体制9.4.2 利用椭圆曲线密码实现数字签名9.5 基于身份的签名方案9.5.1 Shamir的基于身份的数字签名方案9.5.2 Cha-Cheon的基于身份的数字签名方案习题第10章 密码学侧信道攻击10.1 基本概念10.2 入侵型攻击10.2.1 一般的篡改方法10.2.2 保护措施10.3 错误攻击10.3.1 简单错误分析攻击10.3.2 差分错误分析(DFA)攻击10.3.3 错误引入10.3.4 错误攻击的对策10.4 时间攻击10.4.1 对平方-乘算法的时间攻击10.4.2 对多位窗口平方-乘算法的时间攻击10.4.3 时间攻击的对策10.5 能量攻击10.5.1 简单能量分析(SPA)攻击10.5.2 差分能量分析(DPA)攻击10.5.3 能量攻击的对策10.6 电磁攻击习题第11章 密码协议11.1 什么是密码协议11.2 密码协议的安全性11.3 身份认证协议11.3.1 身份认证概述11.3.2 基于口令的认证11.3.3 基于对称密码的认证11.4 秘密共享11.4.1 秘密共享的思想11.4.2 Shamir门限秘密共享方案11.5 阈下信道11.5.1 阈下信道的基本原理11.5.2 ElGamal签名的阈下信道11.6 比特承诺11.6.1 什么是比特承诺11.6.2 使用对称密码算法的比特承诺11.6.3 使用单向函数的比特承诺11.7 零知识证明11.7.1 基本构建11.7.2 交互零知识证明和非交互零知识证明11.7.3 身份的零知识证明习题主要参考文献

## 章节摘录

对一个保密系统采取截获密文进行分析的这类攻击称为被动攻击 ( passive attack )。被动攻击本质上是在传输中偷听或监视, 其目的是从传输中获得信息。

两类被动攻击分别是析出消息内容和通信量分析。

析出消息内容容易理解: 电话交谈、电子邮件消息和传送的文件可能包括敏感或机密信息, 我们希望防止对手从这些传输中得知相关内容。

第二种被动攻击是通信量分析, 它更为微妙。

假定我们用某种方法屏蔽了消息内容, 即使敌手获取了该信息也无法从消息中提取信息。

屏蔽内容的常用技术是加密。

如果我们已经用加密进行保护, 对手也许还能观察这些消息的模式。

该对手能够测定通信主机的位置和标识, 能够观察被交换消息的频率和长度。

这些信息对猜测正在发生的通信的性质是有用的。

密码系统还可能遭受的另一类攻击是主动攻击 ( active attack )。

非法入侵者主动向系统干扰, 采用删除、更改、增添、重放和伪造等方法向系统加入假消息。

主动攻击还能进一步划分为四类: 伪装、重放、篡改消息和拒绝服务。

伪装, 即一个实体被另一个实体假冒。

这种攻击引诱受害者相信与之通信的是另一实体。

重放涉及一个数据单元的被动获取以及后继的重传, 以产生一个未授权的效果。

消息的篡改只不过意味着一个合法消息的某些部分被改变, 或消息被延迟或改变顺序, 以产生一个未授权效果。

拒绝服务, 即长时间地阻止服务。

拒绝服务阻止通信设施的正常使用或管理。

这种攻击可能具有一种特定目标, 例如, 一个实体可能抑制所有的消息指向某个特殊的目的地 ( 如安全审计服务 )。

另一种形式的拒绝服务是使整个网络崩溃, 或者通过使网络不能工作的手段, 或者滥发消息使之过载, 以达到降低性能的目的。

1.3.1 攻击密码系统的方法 对密码进行分析的尝试称为攻击。

Kerckhoffs最早在19世纪阐明密码分析的一个基本假设, 这个假设就是秘密必须完全寓于密钥中。

Kerckhoffs假设密码分析者已有密码算法及其实现的全部详细资料。

密码分析者攻击密码系统的方法主要有以下三种。

编辑推荐

本书不仅介绍了密码学的经典算法，也介绍了密码学领域的最新标准化算法。例如，在公钥密码体制中，已有的教材仅仅介绍经典的RSA算法，这种经典算法存在许多缺陷，不能在实际应用中使用，本书在分析经典的RSA的缺陷之后，介绍了RSA-OAEP加密标准和RSA签名标准PSS。

本书选材上注意到了密码学领域的最新研究成果，如在分组密码中对我国官方公布的第一个商用密码算法SMS4进行了讨论，介绍了线性与差分密码分析，在公钥密码中介绍了基于身份的密码学，此外，第10章重点讨论了密码学侧信道攻击的概念和一些攻击模式，此前的国内教材都没有涉及这些内容。

<<应用密码学>>

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>