<<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

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。

<<应用密码学>>

书籍目录

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碍信息。
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。

<<应用密码学>>

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。

版权说明