<<密码学>>

图书基本信息

书名：<<密码学>>

13位ISBN编号：9787121087042

10位ISBN编号：7121087049

出版时间：2009-6

出版时间：电子工业出版社

作者：郑东，李祥学，黄征　编著

页数：202

<<密码学>>

内容概要

在过去的三十余年里，现代密码学的研究获得了突飞猛进的发展，是当今通信与计算机界的热门课题。
本书主要介绍密码学的基本原理与设计方法,其中包括对称密码算法与非对称密码算法、数字签名算法及哈希函数的设计原理、密钥管理体制设计方法、高级数字签名协议设计模型等，最后给出了一些密码技术在网络应用中的实际例子。

本书既可作为高等学校计算机、通信及信息安全专业高年级本科生的教材，也可作为电子信息与通信和信息管理等专业研究生的教材，同时还可以作为相关工程技术人员学习密码学知识的入门读物。

<<密码学>>

书籍目录

章节摘录

第1章　密码学引论　　1.1　密码学在信息安全中的作用　　信息安全涉及的范围很广，无论在军事方面，还是在人们的日常生活方面，都会涉及信息安全的问题。

就计算机通信而言，其处理的信息可以归纳成两类：一类是仅在计算机内部处理和存储的信息；另一类是在计算机之间相互传递的信息。

对于仅在计算机内部处理和存储的信息，希望不被非法人员访问，即如何控制非法客户读取计算机内的信息；关于后一类，发送者希望能够控制在公开信道上传输的信息具有完整性和机密性等。

1.1.1　信息安全面临的威胁　　信息安全面临多方面的威胁，如意外事故、自然灾害、人为恶意攻击等。

人为的恶意攻击是有目的的破坏，可以分为主动攻击和被动攻击。

主动攻击是指以各种方式有选择地破坏信息（如修改、删除、伪造、添加、重传、乱序、冒充、传播病毒等）。

被动攻击是指在不干扰信息系统正常工作的情况下，进行截获、窃取、破译和业务流量分析等。

人为恶意攻击有下列几种手段。

（1）窃听：攻击者通过监视网络数据获得敏感信息。

（2）重传：攻击者事先截获部分或全部信息，以后将此信息发送给接收者。

（3）伪造：攻击者伪造一个信息，将伪造的信息以其他人的身份发送给接收者。

（4）篡改：攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者。

（5）行为否认：通信实体否认已经发生的行为。

（6）拒绝服务攻击：攻击者通过某种方法使系统响应变慢甚至瘫痪，阻止合法用户获得服务。

（7）非授权访问：不按照设定的安全策略要求使用网络或计算机资源的行为都可以看做非授权访问。

非授权访问主要有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等几种形式。

（8）传播病毒：通过网络传播计算机病毒，其破坏性非常大，而且很难防范。

如众所周知的CIH病毒、“爱虫”病毒都具有极大的破坏性。

版权说明