<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787115211576

10位ISBN编号：7115211574

出版时间：2009-9

出版时间：人民邮电

作者：何大可,彭代渊,唐小虎

页数：203

前言

密码学（Cryptology）包括密码编码学（Cryptography）和密码分析学（Cryptanalytics），后者的研究内容，也称为密码破译（cipher-break），密码是在非安全信道中为保证交换信息的机密性而诞生的。

人类使用密码已经有几千年了，在历史上它往往和军事、间谍等工作联系在一起。

由于成功的密码编码、密码使用或密码分析，使密码工作者多次在世界军事史上留名并且影响到历史的进程。

纳瓦霍语密码是密码编码的传奇；破译德国“恩尼格玛”密码和破译日本“紫密”密电是密码分析的传奇——它们已经成为脍炙人口的故事。

以战争为主要驱动力的密码学，和通信理论、电子学一样在第二次世界大战后得到高度重视，随着社会日益增长的保密需求，其研究在更大范围内受到关注和支持。

在近代密码学的发展史上，以下几个事件具有特殊的意义。

1949年C.E.Shannon发表了“Communication theory of secrecy system’，将密码学的研究引入了科学的轨道——虽然该文在20多年后才得到密码学界足够的重视。

20世纪70年代，有两个可以称为里程碑的事件：一是美国国家标准局（NBS）正式公布实施美国数据加密标准（DES），由此导致密码的广泛商业应用和密码研究的平民化；另一个是W.Diftie和M.E.Hellman公开发表“New directions incryptography”一文，提出了不同于传统对称密码体制的非对称密码体制或双钥密码体制——由于加密与解密密钥中的一个可以公开，所以也被称为公钥密码体制。

它们是现代密码学诞生的主要标志。

将公钥密码体制改用于认证时，唯一拥有秘密密钥的一方如果用该密钥加密授权书（或其压缩映像），则既定的验证者均可利用对应的公钥解密以上结果得到原来的授权书（或其压缩映像）。

上述过程可以提供加密者拥有该秘密密钥的证据，同时也能达到防止他人篡改其原始文件的目的——这就是数字签名得以立法的理论基础（我国法律名为“中华人民共和国电子签名法”）。

于是，利益不一致的参与者之间要求个人信誉保证的所有商务、金融活动等交易，都可能从传统的在契约上以手书签名的运作方式，转移到网络上来进行——因为数字签名可以代替手书签名甚至效果更佳，而将交易信息加密又可以保证交易的机密性。

不难想象，这样的变革对人类社会的影响是多么巨大，因为需要“签署”以证明信用或便于审计的不止是商业和金融业，政府、军队也是如此。

于是，电子政务、电子商务近年得以迅猛发展，事实上还包括“电子军务”。

密码编码学的任务与密码分析学的任务如同制造坚固的盾与制造锋利的矛。

同古老的盾与矛一样，它们也逃不出“相互争斗，永无休止”的哲学。

自然，在这里需要的不再是铁与火，而是数学、电子学、信息论、计算复杂性理论等，以及在此基础上表现出的智力、技巧、微电子制造甚至。

DNA技术，同时还需要一点谦逊、谨慎和预见——因为现实社会中参与密码搏弈的对手对其真实的密码设计水平与密码破译能力始终是秘而不宣。

<<现代密码学>>

内容概要

本书系统地讲述了密码学的基础理论与应用技术。
主要内容包括密码学的信息论基础、密码学的复杂性理论、流密码、分组密码、公钥密码、Hash函数、数字签名、密码协议和密钥管理。
本书内容丰富，取材经典、新颖，概念清楚，各章后面配有大量习题。
本书可作为高等院校信息安全、通信工程等相关专业本科生的教材，也可供研究生与相关技术人员学习参考。

作者简介

何大可，西南交通大学教授、国家高性能计算中心（成都）主任、博士生导师、从1992年起享受国务院特殊津贴。
兼任中国密码学会副理事长，华南农业大学“丁颖讲座教授”。
长期从事密码学、移动通信安全、铁路信息系统安全工程等方面的教学、研究和设计工作。
参与了我国首批密码学博士点申报；曾任第四届全国铁路高校电子信息类专业教学指导委员会副主任，计算机科学与技术、自动化专业教学指导组组长。
先后主持、主研国家自然科学基金项目、国家“八五”攻关项目、国家863计划项目、教育部博士点基金项目及铁道部等部委科技项目约30项。
是多项中国专利和美国专利US6、859、151 B2的发明人。
1989年获国家自然科学四等奖，获省部级一等奖1次、省部级二等奖3次，1997年获中国科学技术发展基金会第三届詹天佑人才奖。

<<现代密码学>>

书籍目录

章节摘录

第1章　概论　　本章介绍信息安全基本概念、密码系统模型、密码体制分类、简单密码算法、初等密码分析、密码学的信息论基础和计算复杂性理论基础。

1.1 信息安全与密码技术　　随着人类步人信息时代的21世纪，信息安全变得越来越重要。这里，不可避免地要涉及信息（Information）、数据（Data）、知识（Knowledge）、信息系统几个概念。

信息的一般定义属于哲学范畴。

信息是事物运动的状态与方式，是事物的一种区别于物质与能量的属性。

信息与物质、能量的概念处于同一层次，成为组成世界的三大要素。

消息是信息的外壳或表象，信息是消息的内核；信号是信息的载体；数据是记录信息的一种形式。

知识是认识主体（人、猩猩等）加工、序化的信息。

信息系统是指有目的、和谐地处理信息的人—机系统（人、传感器、通信设备、计算机硬件、软件等），它能对一定形态、形式的信息进行处理（如采集、发送、传递、接收、检测、度量、变换、存储），并且最终转换为可以由人类感知器直接感知的结果（传统的感知器有视觉、听觉、触觉感知器；而嗅觉、味觉感知器已经或者即将被利用）。

下面是信息系统的一些实例：公众移动通信系统，民航／铁路客运售票系统，地理信息系统，保安监控系统，地震、海啸监测预警系统（可能包含以某些动物作为探测器的预警子系统）。

信息系统按社会功能可分为：企业生产／营销业务系统，党政内部网络系统，电子政务系统，电子商务系统，军队信息系统（如指挥-控制-通信-计算机-情报系统C4I，信息作战系统），大国间的战略导弹核查系统等。

目前的一个趋势是：若干信息系统经集成或互联（比如经互联网），形成了十分复杂的网络拓扑结构，使信息安全保障的形势变得更加严峻。

<<现代密码学>>

编辑推荐

经典密码学内容　　更强调网络背景　　概念清楚、论述严谨　　例题、习题丰富

版权说明