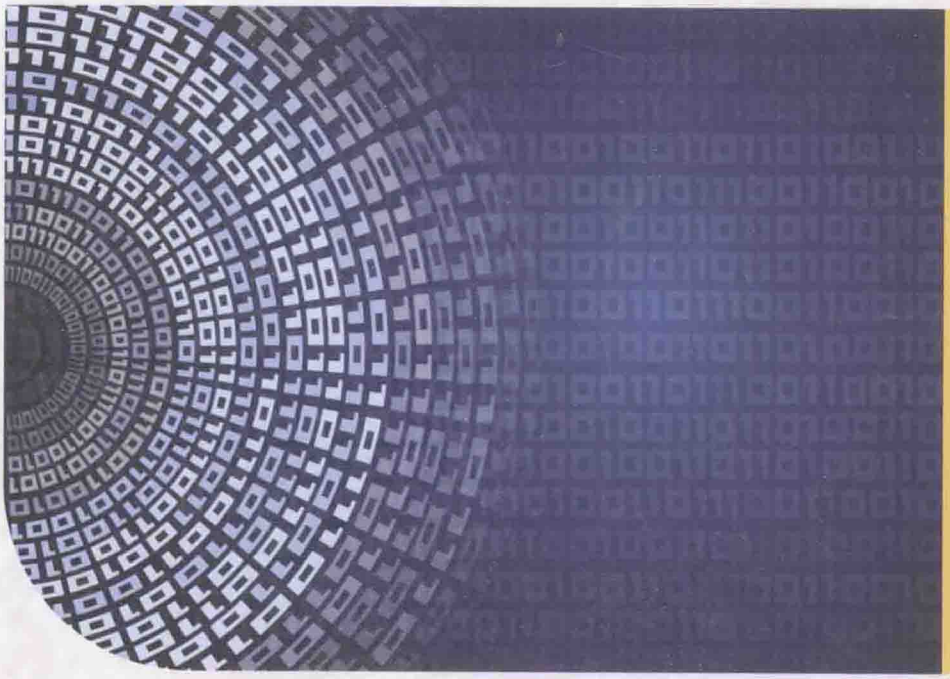
普通高等教育“十一五”国家级规划教材
信息安全专业系列教材

现代密码学教程

MODERN CRYPTOGRAPHY

谷利泽　郑世慧　杨义先 ⊙ 编著

（第2版）



北京邮电大学出版社
www.buptpress.com

普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

现代密码学教程

（第 2 版）

谷利泽　郑世慧　杨义先　编著

北京邮电大学出版社

内 容 简 介

本书是一本关于现代密码学的基础教材，全书共有 12 章，主要分成 4 个部分。第一部分（第 1～3 章）主要介绍现代密码学的发展概况、基本概念和思想、早期密码算法以及密码学用到的信息论与复杂度理论基本知识。第二部分（第 4～8 章）主要介绍现代密码学的加密和认证基本原语，包括对称密码方案（分组密码、序列密码、Hash 函数、消息认证码）和非对称密码方案（包括公钥加密、数字签名）。第三部分（第 9～11 章）主要介绍密钥管理协议、密码学协议和密码应用协议。第四部分（第 12 章）简单介绍了现代密码学的一些新的发展方向。

本书重点突出，抓住核心；通俗易懂，容易入门；例证丰富，快速理解；习题多样，牢固掌握。

本书是信息安全专业的专业基础课教材，适合作为高等院校信息科学专业或其他相关专业本科生和研究生的教材，也可作为相关领域的教师、科研人员以及工程技术人员的参考书。

图书在版编目(CIP)数据

现代密码学教程/谷利泽，郑世慧，杨义先编著. --2 版. --北京：北京邮电大学出版社，2015.3

ISBN 978-7-5635-4307-6

Ⅰ.①现… Ⅱ.①谷…②郑…③杨… Ⅲ.①密码术—高等学校—教材 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2015)第 045789 号

书　　名：现代密码学教程(第 2 版)
著作责任者：谷利泽　郑世慧　杨义先　编著
责 任 编 辑：崔　珞　张珊珊
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京鑫丰华彩印有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：23
字　　数：614 千字
版　　次：2009 年 8 月第 1 版　2015 年 3 月第 2 版　2015 年 3 月第 1 次印刷

ISBN 978-7-5635-4307-6

定　价：47.00 元

前　言

本书第1版出版于2009年8月，该书被众多高校信息安全专业及信息安全相关专业作为专业教材或教学参考书籍，受到广大师生的好评；并于2010年获“全国电子信息类优秀教材”一等奖。

密码学是一门随着时间和计算机技术发展不断推陈出新的学科，在本书第1版出版后5年中，涌现出很多新的研究成果。因此，作者总结在北京邮电大学教学和科研中的经验和体会，并结合很多读者的反馈意见，在第1版的基础上，对书籍的内容进行调整，修订成为第2版。第2版添加了近年来密码学的一些新技术，进一步丰富了本书的习题，并纠正了第1版中的一些错误。在第2版的撰写过程中，作者尽力使教材内容较全面阐述密码学的基本概念、基本模型和基本原理；纳入新的实用密码技术代替那些已经不太安全的密码技术；并对密码学的一些探索研究做简单的、启发式介绍。

主要修订内容如下。

(1) 信息安全标准化以及立法工作，越来越受到国家的重视，因此，在第2版的第1章加入了密码相关政策法规及标准。

(2) 限于篇幅，无法细致论述密码学的数学基础(数论及近世代数)，因此第1版中的3.1节和3.2节较难理解。在第2版中删减此两节。

(3) 在第2版中，将密码学基础一章调整到传统密码体制之前。此外，将第1版中1.3节调整到此处，结合后面几节内容，对密码设计和分析学进行全面概述。特别地，由于认证性是信息安全三要素之一，第2版在第1版保密体制的基础上，特别补充了认证体制的相关概念及模型。

(4) 序列密码是一种重要的对称加密体制，在高级加密标准确立之后，序列密码的公开研究也逐渐兴起，出现了很多算法，第2版中介绍了estream工程推荐的7个序列密码算法替换了第1版中的SEAL等算法。

(5) 第2版中第7章删减了基于身份密码体制，因为基于身份是与基于CA相对应的，CA在密钥管理一章才介绍。替换成基于编码的密码体制，这是目前后量子密码一个重要的研究分支。

(6) 第1版第10章的密钥分发技术和密钥协商技术整合成第2版中密钥建立一节，并在密钥分发部分着重介绍会话密钥分发，对其具体技术进行了补充和完善；此外，在第1版分发技术中的公钥分发技术基础上，添加PKI相关技术，完整介绍公钥的管理流程。

(7) 第2版中新加入安全协议一章，旨在以此为例介绍密码技术在实际计算机网络中的应用方式。

(8) 第2版中，在密码学新进展一章，添加了密码学研究热点——后量子密码的简单

介绍。

南京邮电大学的王少辉副教授参与了第 2 版第 2 章的编写，北京邮电大学的王励成副教授参与了第 2 版第 2、7、12 章的编写，在此向两位老师表示衷心感谢。同时，向为本书的编写付出辛勤工作的苏丽裕、张好、田原等同学表示感谢。

本书第 2 版的编写工作由谷利泽和郑世慧完成，由于作者水平有限，书中难免存在不足与错误，恳请读者批评指正。

作　者

目　录

第1章　密码学概论

密码学的英文为 Cryptology，来源于希腊语 kryptós 和 gráphein，意指“隐藏地书写”，这也表明了早期的密码技术主要为了隐密地传递信息。而现代密码技术已经延伸到了信息安全诸多领域，例如身份认证，数据完整性检测等，是信息安全的基础与核心。此外，随着密码学在网络信息系统的广泛应用，密码技术的标准化和管理的规范化也初具雏形，为信息安全保障提供了坚实的后盾。本章将概况介绍密码学与信息安全的关系，密码学发展简史，以及密码技术的相关标准与政策规范。

1.1　信息安全与密码学

信息，也称之为消息，被香农(C. E. Shannon)定义为“凡是在一种情况下能减少不确定性的任何事物”。人类通过获得、识别自然界和社会的不同信息来区别不同事物，同时信息不同于物体，它可以无限复制，广泛传播。随着计算机和网络的普及，信息的传播呈现出速度快、形态多样和范围广的特性，使得信息作为一种资源，成为推动社会进步和促进经济增长的重要力量。然而，一旦信息落入了其竞争对手手中，就可能会导致企业、政府、国家不可估量的损失。因此，保护信息的机密性，对国家、企业、个人都具有重要的意义。

早期信息传递中，外交官和军队首脑就已经使用一些技巧来保证通信的机密以及获知其是否被篡改。例如，四千多年前，斯巴达人奴隶的腰带缠绕在木棍上，顺着木棍书写信息，腰带展开之后，置乱的字符被当成一些无意义的装饰，以此来防止奴隶落入敌人手中时秘密消息被读取。之后，随着电子机械技术的发展，信息的传递和保护开始采用程序化操纵控制的应用程序实现。20 世纪末以及 21 世纪初，通信、计算机硬件和软件技术飞速发展，用于信息加工处理的小巧且廉价的计算设备在小公司和家庭用户中普及，同时这些计算机被网络连接起来。在因特网上快速增长的电子数据处理和电子商务应用，以及不断出现的网络攻击事件，增加了对更好地保护计算机及其存储、加工和传输的信息的需求。在此背景下，信息安全(Information Security)技术迅速发展起来。

维基百科对“信息安全”的定义为保护信息免受未经授权的进入、使用、披露、破坏、修改、阅读、检视、记录及销毁。它主要涵盖两个领域。

(1) 计算机安全。这里的计算机并不一定意味着就是个人电脑，它可以是任何一台拥有处理器和内存的设备。囊括了非网络独立的计算器，可联网的移动计算机设备，如智能手机和平板电脑。信息安全技术负责保障其免遭恶意网络攻击，例如，试图偷看其中的私人信息或者获得内部系统的控制权。

(2) 信息保障。当威胁出现时，确保数据不丢失。威胁包括但不限于自然灾害，计算机/服务器故障，物理盗窃，或任何其他的数据潜在地被丢失的情况。

1.1.1 信息安全的目标

经典的信息安全三要素——机密性、完整性和可用性(Confidentiality, Integrity & Availability,CIA)是信息安全的核心原则,在字面上可以指安全属性、安全目标、信息标准、关键的信息特征和基本的构造因素。关于扩展这个经典的三要素概念,一直都有争论。

1992 年提出并于 2002 年修订的经济合作与发展组织(Organisation for Economic Cooperation and Development,OECD)信息系统与网络安全指导方针,提出了九个被人们接受的原则,即感知、责任、响应、行为准则、民主、风险评估、安全设计和实现、安全管理、重新评估。2004 年,在这些原则的基础之上,NIST 信息技术安全工程原则提出了 33 条原则。

2002 年,Donn Parker 提出了一个可供替代经典的"CIA 三要素"的模型,他称该模型为信息的六要素。这些要素分别是机密性、所有权、完整性、可认证性、可用性和实用性。Parker 提出的六要素的价值在于,它正是安全专家们的争论主题。

2013 年,作为 CIA 三要素的扩展,进一步提出了信息保障和安全(Information Assurance & Security,IAS)的八要素,它包括机密性、完整性、可用性、隐私性、可认证性与可信任性、不可抵赖性、可说明性、可审计性。目前,IAS 八要素是信息保障与安全参考模型(Reference Model of Information Assurance & Security,RMIAS)的四个维度之一。作为当今与安全相关的一系列目标,它已经通过一系列安全专家和学者的评估。至此,信息安全的概念从早期只关注信息保密和通信保密的信息内涵时代,发展到关注信息及信息系统的机密性、完整性、可用性和不可否认性的信息安全时代,再发展到今天的信息保障时代。本书主要关注以密码学为基础的信息安全的五个主要方面,即信息及信息系统的机密性、完整性、可用性、认证性和不可否认性。

(1) 机密性(Confidentiality)

机密性又称保密性,是指保证信息不泄露给非授权的用户或实体,确保存储的信息和被传输的信息仅能被授权的各方得到,而非授权用户即使得到相关数据也无法知晓信息内容。通常通过加密变换阻止非授权用户获知信息内容。

(2) 完整性(Integrity)

完整性是指在数据整个生命周期维持其准确和一致,也就是说,信息未经授权不能进行篡改的特征,或者说信息在生成、传输、存储和使用过程中发生的人为或非人为的非授权篡改(插入、修改、删除、重排序等)均可以被检测到。一般通过生成一个改动检测码来检验信息是否被篡改。

(3) 认证性(Authentication)

认证性是指一个消息的来源或消息本身被正确地标识,同时确保该标识没有被伪造。认证分为实体认证和消息认证。消息认证指数据、文档等来源真实可靠;而实体认证是指能证实所有参与的实体是可信的,即每个实体确实与它们宣称的身份相符。通常,认证的参与方持有一个秘密,一方面,秘密和消息混合可以生成消息的认证标签来确保消息认证性;另一方面,参与方可以使用秘密来正确回应对方的挑战,以此来向对方实体证明自己的身份。

(4) 不可抵赖性(Non-Repudiation)

不可抵赖性(也称为不可否认性)是指用户无法在事后否认曾经进行的信息的生成、签发、接收等行为。当发送一个消息时,接收方能证实该消息确实是由既定的发送方发来的,称为源不可抵赖性;同样,当接收方收到一个消息时,发送方能够证实该消息确实已经送到了指定的接收方,称为宿不可抵赖性。然而,虽然密码技术有助于实现不可抵赖性,但是不可抵赖的核

心还是凌驾于技术之上的法律概念。例如，一个消息连同其有效签名并不足以证明消息来自于持有私钥的签名者，因为持有私钥的用户可以通过证明签名系统存在漏洞，或者他的私钥之前已经泄露。上述事实说明，签名不一定能保证消息认证性和完整性，从而防止抵赖。持有私钥的用户最终是否可以洗脱罪责，还是要依靠法律裁定。

(5) 可用性(Availability)

可用性是指保障信息资源随时可提供服务的能力特性，任何信息系统都必须满足这个属性。这意味着存储和处理信息的计算系统，防止非授权访问的控制系统，以及传输信息的通信系统必须运行正常。高可用性的系统不仅需要在停电、硬件故障和软件升级时保持信息资源可用，还需要能够抵制拒绝服务攻击。

1.1.2 攻击的主要形式和分类

对信息进行保护，首先要熟知信息可能面临的安全威胁，对信息系统的攻击有很多，国际标准化组织 ISO 对开放系统互联 OSI 环境中计算机网络进行深入研究以后，定义了以下 11 种威胁。

(1) 伪装。威胁源成功地假扮成另一个实体，随后滥用这个实体的权利。

(2) 非法连接。威胁源以非法的手段形成合法的身份，在网络实体与网络之间建立非法连接。

(3) 非授权访问。威胁源成功地破坏访问控制服务，如修改访问控制文件的内容，实现了越权访问。

(4) 拒绝服务。阻止合法的网络用户或其他合法权限的执行者使用某项服务。

(5) 抵赖。网络用户虚假地否认递交过信息或接收到信息。

(6) 信息泄露。未经授权的实体获取到传输中或存放着的信息，造成泄密。

(7) 通信量分析。威胁源观察通信协议中的控制信息，或对传输过程中信息的长度、频率、源及目的进行分析。

(8) 无效的信息流。对正确的通信信息序列进行非法修改、删除或重复，使之变成无效信息。

(9) 篡改或破坏数据。对传输的信息或存放的数据进行有意的非法修改或删除。

(10) 推断或演绎信息。由于统计数据信息中包含原始的信息踪迹，非法用户利用公布的统计数据，推导出信息源的来源。

(11) 非法篡改程序。威胁源破坏操作系统、通信软件或应用程序。

以上所描述的种种威胁大多由人为造成，威胁源可以是用户，也可以是程序。除此之外，还有其他一些潜在的威胁，如电磁辐射引起的信息失密、无效的网络管理等。信息安全的研究目的就是防止和消除上述威胁。

1. 攻击的主要形式

根据对信息流造成的影响，可以把攻击分为五类：中断、截取、篡改、伪造和重放，进一步可概括为两类：主动攻击和被动攻击。

攻击的主要形式如图 1-1 所示，图中(a)是正常的信息流，其他(b)、(c)、(d)、(e)、(f)是 5 种针对信息安全性攻击的表现形式。

(1) 中断(Interruption)

中断也被称为拒绝服务，是指阻止或禁止通信设施的正常使用，这是对可用性的攻击。这种攻击一般有两种形式：一是攻击者删除通过某一连接的所有协议数据单元，从而抑制所有的

消息指向某个特殊的目的地。另一种是通过对特定目标滥发消息使之过载，使整个网络瘫痪或崩溃。或者有些攻击者还可能实施物理攻击，例如破坏通信设备，切断通信线路等。

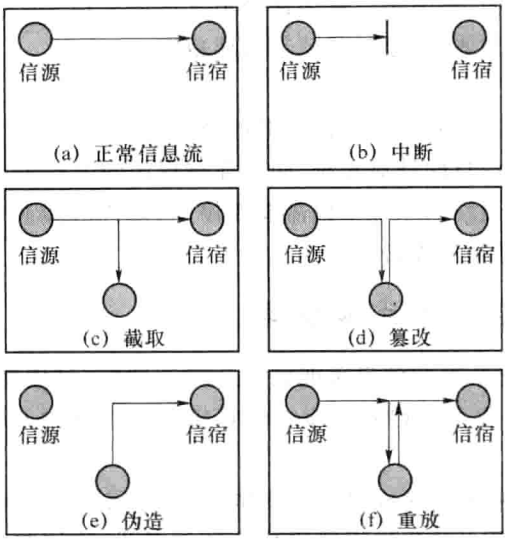


图 1-1　针对信息安全攻击的主要形式

(2) 截取(Interception)

截取是未授权地窃听或监测传输的消息，从而获得对某个资源的访问，这是对机密性的攻击，一般分为析出信息内容和通信量分析两种情况。

析出消息内容是指当人们通过网络进行通信或传输消息时，如果不采取任何保密措施，攻击者就有可能在网络中"搭线"窃听，以获取他们通信的内容。

通信量分析则是假定通信双方已用某种方法屏蔽了消息内容，使得攻击者即使获取了该消息也无法从消息中提取有用信息。但即使已用加密进行保护，攻击者还能观察这些消息的结构模式，即通过测定通信主机的位置和标识，攻击者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性质是有用的。

(3) 篡改(Modification)

篡改也就是未授权地更改数据流，它是针对连接的协议数据单元的真实性、完整性和有序性的攻击。意指一个合法消息的某些部分被改变、消息被延迟或改变顺序，以产生一个有特殊目的的消息。

(4) 伪造(Fabrication)

伪造是指将一个非法实体假装成一个合法的实体，这往往是对身份认证性的攻击。它通常与其他主动攻击形式结合在一起才具有攻击效果，如攻击者重放以前合法连接初始化序列的记录，从而获得自己本身没有的某些特权。

(5) 重放(Replay)

重放将一个数据单元截获后进行重传，产生一个未授权的消息。在这种攻击中，攻击者记录下某次通信会话，然后在以后某个时刻，重放整个会话或其中的一部分。

2. 攻击的分类

如图 1-2 所示，根据信息安全攻击的作用形式及其特点，可以将信息安全攻击分为两大类：主动攻击和被动攻击。其中被动攻击主要包括析出消息内容和通信量分析的截取攻击。主动攻击主要包括中断、篡改、伪造和重放攻击。

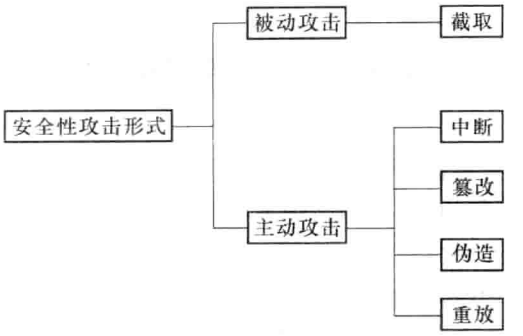


图 1-2　攻击的分类

被动攻击中，攻击者只是观察通过一个连接的协议数据单元以便了解所交换的数据，进而获取他人信息，并不干扰信息流，如“搭线”窃听和对文件或程序的非法复制等。被动攻击只威胁数据的机密性，典型的被动攻击形式就是截取。被动攻击通常难于检测，因为它们并不会导致数据有任何变化，所以对付被动攻击的重点是防止。

主动攻击是指攻击者对连接中通过的协议数据单元进行各种处理。这些攻击涉及某些数据流的篡改或一个虚假信息流的产生，如有目的地更改、删除、增加、延迟、重放等，还可将合成的或伪造的协议数据单元送入到一个连接中去。主动攻击的目的是试图改变或影响系统的正常工作，它威胁数据的完整性、认证性和可用性等。主动攻击主要包括四类：中断、篡改、伪造和重放，它表现出与被动攻击完全相反的特点。完全防止主动攻击是相当困难的，对于主动攻击，可采取适当措施加以检测，并从攻击引起的破坏或时延中予以恢复。

1.1.3　密码学在信息安全中的作用

自密码术产生到第二次世界大战之前，密码技术始终处于一种不公开的保密状态，让人感到既神秘又畏惧，信息技术的发展改变了这一切。随着计算机网络和通信技术的迅猛发展，大量的敏感信息通过信道或计算机网络进行传输。特别是随着互联网的广泛应用，电子商务及电子政务的迅速发展，网络间交互的用户需要相互核实身份以防止非授权的访问。正是这种对信息的机密性和身份的真实性（身份认证）的要求使得密码学逐渐揭开了它神秘的面纱，走进人们日常的生活和工作中。密码学的加密技术使得即使信息流被截取，攻击者也无法获取信息的内容；上面提到的信息被未授权篡改的攻击，密码学的散列函数能够检测到；防止一个非法实体假装成一个合法的实体，可以利用密码学的认证（鉴别）技术来实现。此外，数字签名技术具有防否认的功能，以电子证据的形式存在，具有法律效力。

密码学是保障信息安全的核心，信息安全是密码学研究与发展的目的。保证数字信息机密性的最有效的方法是使用密码算法对其进行加密；保证信息完整性的有效方法是利用密码函数生成信息“指纹”，实现完整性检验；保证信息认证性的有效方法是密钥和认证函数相结合来确定信息的来源；保证信息不可抵赖性的有效方法对信息进行数字签名。此外，利用密码机制以及密钥管理可有效地控制信息，以使信息系统只为合法授权用户所用。

虽然密码学在信息安全中起着举足轻重的作用，但密码学也绝不是确保信息安全的唯一技术，也不可能解决信息安全中出现的所有问题。在信息安全领域，除技术之外，对信息系统的管理也是非常重要的，在信息安全领域普遍认同一种理念：信息安全三分靠技术，七分靠管理。