普通高等教育“十一五”国家级规划教材

现代密码学教程

MODERN CRYPTOGRAPHY

谷利泽　郑世慧　杨义先　编著

（第3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

现代密码学教程

（第 3 版）

谷利泽　郑世慧　杨义先　编著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书是一本关于现代密码学的基础教材，主要分为4个部分，共12章。第1部分(第1～3章)主要介绍现代密码学的发展概况、基本概念和基本思想，密码学用到的信息论与复杂度理论以及早期密码算法等基本知识。第2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，包括分组密码、序列密码、Hash函数、消息认证码、公钥密码、数字签名等。第3部分(第9～11章)主要介绍现代密码学的应用，包括密码协议、密钥管理协议和网络安全协议等。第4部分(第12章)简单介绍现代密码学的一些新的研究进展。

本书通俗易懂、例证丰富、重点突出、习题多样，可使读者轻松入门、快速理解核心内容、牢固掌握重点知识。

本书是网络空间安全专业的一本专业基础课教材，可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．-- 3版．-- 北京 ：北京邮电大学出版社，2023.7
ISBN 978-7-5635-6939-7

Ⅰ．①现… Ⅱ．①谷… ②郑… ③杨… Ⅲ．①密码学－教材 Ⅳ．①TN918.1

中国国家版本馆CIP数据核字(2023)第122009号

策划编辑：彭 楠 **责任编辑**：刘春棠 **责任校对**：张会良 **封面设计**：七星博纳

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
邮政编码：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：保定市中画美凯印刷有限公司
开　　本：787 mm×1 092 mm 1/16
印　　张：23
字　　数：602千字
版　　次：2009年8月第1版 2015年3月第2版 2023年7月第3版
印　　次：2023年7月第1次印刷

ISBN 978-7-5635-6939-7 **定价**：59.00元

前言

Foreword

Foreword

近年来，信息安全越来越受到人们的重视，成为经济发展、社会稳定、国家安全的重要因素，而信息安全的核心技术源于现代密码学，越来越多的研究和应用涉及密码技术，越来越多的人渴望获得密码学方面的知识。为了满足实际需求，众多大专院校开设了“现代密码学”课程，为我国密码学人才培养和传播密码学知识发挥了重要作用。作者根据已公开的书籍和资料，结合 20 多年的“现代密码学”课程教学实践，编写了《现代密码学教程》。《现代密码学教程》具有如下特点。

(1) 通俗易懂：对于初学者，现代密码学的内容有些深奥和难以理解，《现代密码学教程》采用背景介绍、生动类比等多种方法，让读者能深入浅出地理解相关知识。

(2) 例证丰富：现代密码学的理论性强、推理复杂，需要学习者具备一定的抽象思维能力。《现代密码学教程》的重点内容都提供了具体的例子，让读者能够快速地掌握其基本原理和设计思路。

(3) 重点突出：现代密码学涉及的内容很多，《现代密码学教程》紧紧围绕现代密码学的核心内容，从基本原理、设计思路、分析方法等多方面进行了阐述。

(4) 习题多样：为了方便读者巩固所学内容，每章后都设置了多种形式的习题(如判断题、选择题、填空题、简答题等)并附有答案，这些习题涵盖了本章的知识要点。

《现代密码学教程》第 1 版于 2009 年 8 月出版，第 2 版于 2015 年 3 月出版，已被众多高等院校网络空间安全专业及其相关专业作为专业基础课教材或教学参考书籍，受到广大师生的好评，是“现代密码学”国家精品课程的教材，获得过“全国电子信息类优秀教材”一等奖。近几年，随着信息技术的不断推陈出新以及 2020 年 1 月《中华人民共和国密码法》的实施，密码技术的发展和实际应用有了一些变化，尤其重视密码国产化；另外，网上出现了《现代密码学教程》(第 2 版)各章习题的答案，但有些答案不够严谨，容易误导读者。为此，结合作者“现代密码学”课程的教学实践和读者对第 2 版的反馈建议，作者对第 2 版的内容进行了小幅调整，修订成为第 3 版，其主要修订内容具体如下。

（1）增加了国家密码局认定的国产密码算法。

在现代密码学中，基本密码算法包括对称密码算法、公钥密码算法和Hash函数，其中对称密码算法又分为分组密码算法和序列密码算法。本书将与这些基本密码算法相对应的国产密码算法增加到相关章节，如4.4.1节SM4算法、5.4.1节ZUC算法、6.2.5节SM3算法、7.4.4节SM2算法、7.5.4节SM9算法等。

（2）丰富和完善了各章习题并增加了习题答案。

在原有习题的基础上，本书进一步优化各章习题的内容和形式，以便更准确地检验读者对每章知识要点的掌握程度。由于每章习题答案的篇幅较大，为了不增加本书的篇幅，我们将习题答案以二维码的形式放于书中，读者可扫描二维码获取习题答案。

（3）紧跟目前的研究热点以及密码学相关的新进展。

本书修改了8.3.5节其他数字签名中的内容，增添了9.4.3节隐私保护的不经意传输协议等，修改和增加了1.3节标准及法律法规和第12章密码学新进展中的一些内容等。

（4）限于篇幅，删减了一些较难理解、与本书核心内容联系不太密切的算法。

本书删减了Salsa20、Sosemanuk、Grain v1、MICKEY 2.0、Trivium、McEliece密码算法、一次性签名等内容。

本书更加全面地阐述了密码学的基本概念、基本原理和基本实现方法，并能紧跟密码技术的发展趋势，习题及其答案能准确地检验读者对知识要点的掌握程度。在本书的撰写过程中，北京邮电大学的博士生段珺珂参与了国产密码算法、相关章节（如3.2.3节、12.4.2节等）以及部分习题答案的校对工作，在此向段珺珂同学表示衷心感谢，同时，向为本书的编写付出辛勤工作的王励成老师、闫星宇同学、马晓宇同学、王浩丰同学等表示感谢。

在本书的编写过程中，除了引用了作者自己的研究内容和研究成果外，还参考了大量国内外优秀论文、书籍以及在互联网上公布的相关资料，我们尽量在参考文献中列出了上述资料，但由于互联网上资料数量众多，出处杂乱，可能无法对所有文献一一注明出处，在此我们对这些资料的作者表示由衷的感谢，同时声明，原文版权属于原作者。

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。作者的电子邮箱：glzisc@bupt.edu.cn。

目录

Contents

第 1 章

密码学概论

密码学的英文为 Cryptology，来源于希腊语 kryptós（隐藏的）和 gráphein（书写），这表明早期的密码技术主要是为了隐秘地传递信息。而现代密码技术已经延伸到了信息安全的诸多领域，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初具雏形，为保障信息安全提供了坚实的后盾。本章概括介绍信息安全与密码学、密码学发展史以及密码技术的相关标准与法律法规。

1.1 信息安全与密码学

信息，也称为消息，被 C. E. 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的事物。信息不同于物体，它可以无限复制和广泛传播。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，一旦信息落入竞争对手手中，就可能导致国家、企业、个人不可估量的损失。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。

在早期的信息传递中，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性以及获知其是否被篡改。例如，公元前 400 年，斯巴达人将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获取。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计算机控制的应用程序来实现。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机在公司和家庭用户中得到普及，同时这些计算机通过网络连接起来。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，保护信息及信息系统免受未经授权的进入、使用、披露、破坏、修改、检视、记录及销毁。它主要涵盖以下两个领域。

（1）计算机安全

这里的计算机并不一定就是个人计算机，它可以是任何一台拥有处理器和内存的设备，囊括了所有独立的非网络计算器和可联网的移动计算机设备（如智能手机和平板电脑等）。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、物理盗窃以及任何其他的数据潜在丢失的情况。

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，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。关于这个经典的三要素概念的扩展一直都有争论。

经济合作与发展组织(Organization for Economic Cooperation and Development,OECD)1992年提出并于2002年修订的信息系统与网络安全指导方针提出了9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，在这些原则的基础上，美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)提出了33条信息技术安全工程原则。

2013年，作为CIA三要素的扩展，Donn Parker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、不可否认性、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4个维度之一，作为当今与安全相关的一系列目标，已经通过了安全专家和学者的一系列评估。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4个主要方面，即信息及信息系统的机密性、完整性、认证性和不可否认性。

(1) 机密性

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的内容。通常通过加密变换阻止非授权用户获知信息的内容。

(2) 完整性

完整性是指在数据的整个生命周期维持其准确性和一致性，也就是说，未经授权不能对信息进行修改，或者说在信息生成、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

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。认证分为消息认证和实体认证。消息认证是指数据、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，参与方将秘密和消息混合生成消息的认证标签来确保消息的认证性；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) 不可否认性

不可否认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，这称为源不可否认性；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，这称为宿不可

否认性。然而，虽然密码技术有助于实现不可否认性，但不可否认性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持有私钥的签名者，因为持有私钥的签名者可以证明签名系统存在漏洞，或者其私钥之前已经被泄露。上述事实说明，持有私钥的签名者最终是否可以洗脱罪责，还要由法律裁定。

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种，国际标准化组织(International Organization for Standardization，ISO)对开放系统互连(Open System Interconnection，OSI)环境中的计算机网络进行深入研究后，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 11 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，攻击主要分为 5 种形式：中断(Interruption)、截取(Interception)、篡改(Modification)、伪造(Fabrication)和重放(Replay)。

攻击的主要形式如图 1-1 所示，图 1-1(a)所示为正常的信息流，其他是 5 种攻击的表现形式。

(1) 中断

中断也被称为拒绝服务，是指阻止或禁止通信设施被正常使用，这是对可用性的攻击。这种攻击一般有两种形式：一种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，从而使整个网络瘫痪或崩溃。有些攻击者还可能实施物理攻击，如破坏通信设备、切断通信线路等。

(2) 截取

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

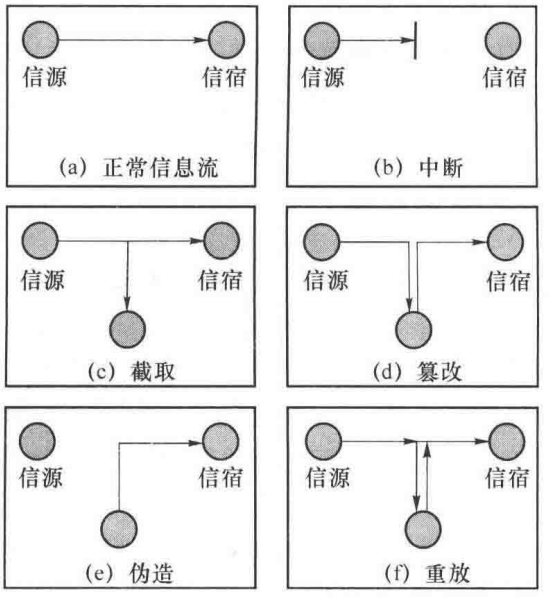

图 1-1　攻击的主要形式

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，以获取人们通信的内容。

通信量分析则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的信息。但即使已进行加密保护，攻击者还能观察到这些消息的结构模式，即通过测定通信主机的位置和标识，攻击者能够观察到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

篡改就是未授权地更改数据流，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。其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

伪造是指将一个非法的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。它只有与其他主动攻击形式结合在一起才具有攻击效果。例如，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

重放是指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，攻击者先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，根据攻击的作用形式及特点，可以将信息安全攻击分为两大类：被动攻击和主动攻击。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。

在被动攻击中，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

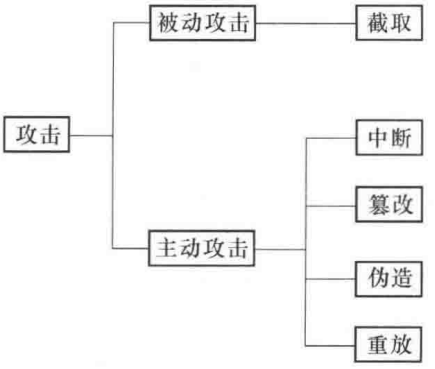

图 1-2　攻击的分类

威胁数据的机密性，典型的被动攻击是截取。被动攻击通常难以检测，因为它并不会导致数据的任何变化，所以对付被动攻击的办法是加密。

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。这些攻击涉及对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，还包括将合成的或伪造的协议数据单元送到一个连接中去。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、认证性等。主动攻击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

自密码技术产生到计算机出现之前，密码技术始终处于一种不公开的保密状态，让人感到既神秘又可怕，而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。正是这种对信息机密性和身份真实性（身份认证）的要求使得密码学逐渐揭开了它神秘的面纱，走进了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；对于上面提到的信息被未授权篡改的攻击，可以利用密码学的散列函数进行检测；防止一个非法实体假装成一个合法实体，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。保证信息机密性目前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将密钥和认证函数相结合来确定信息的来源；保证信息不可否认性的有效方法是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，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，但它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的一种理念是：信息安全三分靠技术，七分靠管理。