XIANDAI
MIMAXUE YUANLI
JI YINGYONG

现代密码学原理及应用

李海峰 马海云 徐燕文 编著

国防工业出版社
National Defense Industry Press

现代密码学原理及应用

李海峰　马海云　徐燕文　编著

国防工业出版社
·北京·

内容简介

本书是作者在多年从事信息安全与密码学的科研工作与一线教学实践的基础上，按照高等院校的培养目标和基本要求，结合平时的教学体会和学生的反馈意见，编写而成的一本关于“现代密码学原理及应用”的教材。

本书围绕着现代密码学提供的基本安全特性（信息的机密性、完整性、认证性、访问控制、不可否认性等），主要从密码学基本理论、密码算法和密码算法应用三方面介绍了现代密码学的基本原理及其应用。全书共分为四大部分，内容涉及密码学基本理论、信息加密技术（古典密码学、对称密码体制、公钥密码体制）、信息认证技术（消息认证、数字签名、身份认证）、密钥管理技术（密钥分配、秘密共享、密钥托管、公钥基础设施（PKI）技术）等。

本书面向应用型本科专业，适合用作普通高等院校信息安全、密码学、计算机科学与技术、网络工程、通信工程、信息工程、信息管理与信息系统、电子商务、软件工程、电子信息科学与技术、物流管理等相关专业的高年级本科学生和硕士研究生“信息安全”课程的教学用书。本书也可作为信息安全工程师、网络安全管理人员和信息技术类用户的培训或自学教材及上述相关人员的技术参考书。

本课程的先修课程有“程序设计”、“数据结构”、“计算机网络”、“信息安全数学基础”等。

图书在版编目（CIP）数据

现代密码学原理及应用/李海峰，马海云，徐燕文编著. —北京：国防工业出版社，2013.6
ISBN 978-7-118-08873-1

Ⅰ.①现… Ⅱ.①李…②马…③徐… Ⅲ.①密码-理论 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字（2013）第 123519 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号 邮政编码 100048）
北京奥鑫印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 22 字数 450 千字
2013 年 6 月第 1 版第 1 次印刷 印数 1—3000 册 定价 56.00 元

（本书如有印装错误，我社负责调换）

国防书店：（010）88540777 发行邮购：（010）88540776
发行传真：（010）88540755 发行业务：（010）88540717

前　言

随着全社会各行各业信息化进程的加快，信息安全问题越来越成为世人关注的社会焦点和信息科学技术领域的研究热点。而作为信息安全的核心技术——密码学则是信息安全应用领域所有人员必须具备的基础知识。为此，国内不少高校、不少专业已经将密码学列为信息安全等相关专业的学生必修的专业基础课程或专业课程。高校作为人才培养的主要阵地，肩负着为我国现代化建设输送优秀人才的重要使命。因此，为了切实提高高等院校密码学课程的教学质量，编写一本真正适合自己国情、校情的“信息安全”的好教材至关重要。正是基于上述考虑，在作者多年从事信息安全与密码学的科研工作与一线教学实践的基础上，按照高等院校的培养目标和基本要求，结合平时的教学体会和学生的反馈情况，着手编写了本书。

本书围绕着现代密码学提供的基本安全特性（信息的机密性、完整性、认证性、访问控制、不可否认性等），主要从密码学基本理论、密码算法和密码算法的直接应用——安全协议三方面介绍了现代密码学的基本原理及其应用，内容涉及密码学基本理论、信息加密技术（古典密码学、对称密码体制、公钥密码体制）、信息认证技术（消息认证、数字签名、身份认证）、密钥管理技术（密钥分配、秘密共享、密钥托管、公钥基础设施技术）等。本书分为四大部分，共12章，各部分内容简述如下：

第1部分（第1～2章）为密码学基本理论。

第1章介绍了信息安全面临的威胁、信息安全问题产生的原因、信息安全的定义与目标、信息安全的基本模型。

第2章介绍了密码学的基本概念、密码体制的分类、密码分析、密码系统的安全性。

第2部分（第3～5章）主要介绍了密码学最基本的应用——信息加密技术。

第3章介绍古典密码学，包括替换密码和置换密码。

第4章介绍了对称密码体制，包括序列（流）密码和分组密码。

第5章主要介绍了公钥密码体制，包括公钥密码体制概述和两种常见的、重要的密码体制：RSA密码体制和椭圆曲线密码体制。

第3部分（第6～8章）介绍了密码学的另外一个重要应用——认证技术。

第6章介绍了消息认证技术。消息认证技术可以实现对消息的来源和完整性认证。

第7章介绍了数字签名技术。数字签名是一种取代手写签名的电子签名技术，它也是一种特殊的认证技术，数字签名模拟文件中的亲笔签名或印章以保证文件的真实性。

第8章介绍了身份认证技术。身份认证可以验证用户的真实身份，是构建信息安全体系的第一道大门。

第4部分（第9～12章）介绍了保证密码系统安全的关键因素——密钥管理技术。

第9章介绍了密钥分配技术，包括对称加密体制的密钥分配、公钥加密体制的密

钥分配。

第10章介绍了秘密共享技术。秘密共享是基于分散保管秘密的思想而出现的一种秘密管理方案,使用秘密共享技术可以有效地增强密钥的安全性。

第11章介绍了密钥托管技术。密钥托管最主要的两个功能是可以实现政府的监听和帮助用户恢复密钥,此外,还可以实现防止用户抵赖的功能。

第12章介绍了公钥基础设施技术。公钥基础设施是一种利用公钥密码体制的理论和技术建立起来的提供信息安全服务的、具有普适性的安全基础设施,旨在从技术上解决网上身份识别与认证、信息的保密性、信息的完整性和不可抵赖性等安全问题。

与其他密码学教材相比,本书力求突出以下几个特色:

(1) 逻辑严密,结构合理。密码学的内容众多,处理好各部分内容的关系至关重要。本书不仅逻辑性好,而且组织结构更加合理。本书按照密码学的基本理论、密码算法、密码算法的直接应用——安全协议的逻辑顺序来编排内容,全书共分为密码学的基本理论、信息加密技术、信息认证技术、密钥管理技术四个部分。

(2) 图文并茂,深入浅出。本书突出的特色是将复杂的密码算法原理分析得深入浅出,便于读者花少量的时间入门并尽快掌握应用密码学的精髓。

本书由李海峰组织编写并进行统稿,其中第1~5章、第7章、第8章、第10章、前言和总目录由李海峰编写;第6章、第9章、第11章、第12章和附录由马海云编写。

在本书的编写过程中,参考了大量资料,除书后附录的参考文献外,本书还参考了许多作者的书籍、论文、著作以及其他在互联网上公布的相关资料等,从中得到了不少帮助和启发,由于篇幅所限,恕无法一一列出,在此也对他们表示衷心的感谢。写作过程中所参考的这些书籍资料,其原文版权属于原作者,特此声明。

由于作者学识和水平有限、时间仓促,加之现代密码学的理论与技术涵盖的内容非常广泛,发展非常迅猛,新的知识、原理和技术层出不穷,本书是在此领域教学工作的一次努力尝试,尽管尽了最大努力,但书中难免存在一些缺点和错误,恳请广大读者与同行专家、学者批评指正,以利再版修订,让更多读者受益。

最后,谨向每一位关心和支持本书编写工作的各方面人士表示感谢!国防工业出版社的领导和编辑为本书的及时出版做了大量的工作,在此表示衷心的谢意!

编 著 者

2013年5月

目　录

第 1 部分　密码学基本理论

第2部分　信息加密技术

第3部分 信息认证技术

第 4 部分 密钥管理技术

第 1 部分

密码学基本理论

信息是当今社会发展的重要战略资源，也是衡量一个国家综合国力的重要标志。对信息的开发、控制和利用已经成为国家间相互争夺的内容；同时，信息的地位和作用也在随着信息技术的快速发展而急剧上升，信息安全的问题也同样因此而日益突出。

本部分主要介绍了信息安全面临的威胁、信息安全问题产生的原因、信息安全的定义与目标、信息安全的基本模型、密码学的基本概念、密码体制的分类、密码分析、密码系统的安全性。

第 1 章　信息安全概述

1.1　信息安全面临的威胁

1.1.1　信息安全的重要性

在当今社会，人们的所有活动都离不开信息，信息已经是最重要的资源之一，人们将信息与能源、物质并列为人类社会活动的三大要素，我们所在的时代被称为信息时代。

信息作为一种无形的资源，在社会生活中起着越来越重要的作用，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。

随着信息技术的迅猛发展，信息技术的应用几乎涉及到了社会的各个领域，信息技术极大地改变了人们的日常生活和工作方式，给人们带来了前所未有的便利，如网上购物、网上银行等，信息技术推动着全球经济的迅速发展，信息产业已经成为新的经济高速增长点。但信息技术是一把双刃剑，互联网不可避免地存在着信息安全隐患。互联网的最大特点就是开放性，对于安全来说，这又是它致命的弱点。伴随信息化的广泛应用而来的信息安全问题越来越引人关注。随着社会信息化步伐的加快，人们对信息系统和信息服务的依赖性也越来越强，这意味着信息系统更容易受到信息安全威胁的攻击，因此，信息资源一旦遭受破坏，将给国家、单位或者个人造成严重的损失。如人们日常遇到的各种计算机病毒，QQ 密码、账号等被盗，大一些的比如单位的网站被黑，无法访问特别是关于企业的经济信息、银行电子资金业务等，更大的乃至一个国家的国家机密、军事信息等重要信息，哪怕它们的任何一点信息的泄露和差错都会给国家安全造成不可估量的损失和灾难。所有这些都属于信息安全所研究讨论的范畴。可以说，信息安全事关国家安全、社会稳定，如何保证信息的安全性已成为我国信息化建设过程中急需要解决的重要问题。在未来的竞争中，谁获得信息优势，谁就能掌握竞争的主动权。因此，信息安全已经成为影响国家安全、经济发展、社会稳定、个人利益的重大关键问题。

如果信息系统的安全性不能得到保证，将大大制约信息化的深度发展，同时也将威胁到国家的政治、经济、军事、文化和社会生活的各个方面，影响国家安全及社会的稳定、和谐发展。

1.1.2　信息安全问题产生的原因

信息安全问题产生的原因非常复杂，涉及到网络信息系统中相关的硬件设备、软件技术以及人为因素等多个方面。

1．硬件设备的物理安全

信息系统中硬件设备的可靠、稳定与安全是信息安全的必要条件之一。硬件设备的

安全是其他安全的基础。不能保障硬件设备的物理安全，其他的安全就无从谈起。硬件设备的安全主要包括以下几方面的内容：

(1) 硬件设备的存放位置，防盗和访问控制措施。

(2) 硬件设备的环境安全威胁，做好防火、防静电、防雷击等防护措施。

(3) 防电磁泄漏，屏蔽是防电磁泄漏的有效措施，主要有电屏蔽、磁屏蔽和电磁屏蔽。

2. 软件技术安全

软件技术安全主要包括网络协议的设计缺陷和系统软件与应用软件的各种安全漏洞带来的各种安全问题。

1) 网络协议的设计缺陷

网络的运行机制是基于各种通信协议。TCP/IP 协议最初设计的应用环境是美国国防系统的内部网络，这一网络环境是互相信任的，网络的设计者在设计网络的时候设计者的目标主要是定位于“网络互联”，保证网络的互联互通，因而，没有过多地考虑安全问题，例如，互联网广泛使用的协议 TCP/IP 协议，它传输的信息采用的是明文方式。因此，TCP/IP 协议的设计存在天生的缺陷。但是由于网络的开放性和共享性，吸引了形形色色的人们接入网络，里面难免有欺诈者、冒充者、破坏者等不怀好意的使用者。由于互联网的发展速度远远超出人们的想象，以至于当人们意识到 TCP/IP 协议的缺陷时，已经不太可能研制一个全新的安全的网络协议来替换 TCP/IP 协议，因为 TCP/IP 协议的用户太多，谁都无法推翻它。于是，只能是在原有的 TCP/IP 协议基础上“修修补补”地解决网络上的安全问题。而且，为了实现异构网络信息系统间信息的通信，往往要牺牲一些安全机制的设置和实现，从而提出更高的网络开放性的要求。开放性与安全性正是一对相生相克的矛盾。因此，互联网上充满了各种安全隐患。

2) 系统软件与应用软件的各种安全漏洞

由于软件程序的复杂性和多样性以及人们的认知能力和实践能力的局限性，在网络信息系统的各种系统软件与应用软件中，很容易有意或者无意地留下一些不容易被发现的安全漏洞。操作系统的漏洞是人们面临的最大风险。无论是 Windows 操作系统还是 UNIX 操作系统等几乎都存在或多或少的安全漏洞。特别是 Windows 操作系统是目前使用最为广泛的系统，但经常发现存在漏洞。过去 Windows 操作系统的漏洞主要被黑客用来攻击网站，对普通用户没有多大影响，但近年来一些新出现的网络病毒利用 Windows 操作系统的漏洞进行攻击，能够自动运行、繁衍、无休止地扫描网络和个人计算机，然后进行有目的的破坏。比如“红色代码”、“尼姆达”、“蠕虫王”以及“冲击波”等。随着 Windows 操作系统越来越复杂和庞大，出现的漏洞也越来越多，利用 Windows 操作系统漏洞进行攻击造成的危害越来越大，甚至有可能给整个互联网带来不可估量的损失。此外，众多的各类服务器(最典型的如微软的 IIS 服务器)、浏览器、数据库、一些桌面软件等都被发现存在安全隐患。可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是信息系统安全问题的主要根源之一。据调查，国内 80%以上的网站存在明显的漏洞。漏洞的存在给网络上不法分子的非法入侵提供了可乘之机，也给网络安全带来了巨大的风险。据美国 CERT/CC 统计，2006 年总共收到系统漏洞报告 8064 个，平均每天超过 22 个(自 1995 年以来，漏洞报告总数已经达到 30780 个)。这些软件的安全漏洞将会给网络信息的安全与保密带来严重的安全威胁。

3. 人为因素

信息系统的运行是依靠人员来具体实施的，他们既是信息系统安全的主体，也是系统安全管理的对象。信息安全中涉及的人为因素主要包括三方面的内容：

1) 人为的无意失误

人为的无意失误虽然没有主观的恶意，但很多时候也会对网络信息安全带来极大的威胁。它包括三个方面：一是配置和使用中的失误，例如，系统操作人员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不恰当，用户将自己的账号随意转借给他人或信息共享等都会对网络安全带来威胁；二是管理中的失误，比如用户安全意识薄弱，对网络安全不重视，安全措施不落实，导致安全事故发生，据调查表明，在发生安全事件的原因中，居前两位的分别是“未修补软件安全漏洞”和“登录密码过于简单或未修改”，这表明了大多数用户缺乏基本的安全防范意识和防范常识；三是各种各样的用户的误操作，典型的误操作有文件的误删除、因为粗心输入错误的数据等。

2) 人为的恶意攻击

人为的恶意攻击是当前计算机及网络系统面临的最大威胁，主要分为主动攻击和被动攻击两大类，关于人为的恶意攻击的具体内容，我们将在 1.1.3 节中详细介绍。

3) 疏于安全方面的管理

一般来说，网络安全不能单靠数学算法和安全协议等技术手段来解决，还需要妥善的法律法规、管理制度共同作用才能达到期望的目标。目前，系统的管理不善也为一些不法分子的入侵破坏制造了可乘之机。据权威机构的统计资料表明：网络与信息安全事件中大约 70%以上的问题是由于管理方面的原因造成的，这正应了人们常说的那句话：“三分技术，七分管理”。因此，解决网络与信息安全问题，不仅应从技术方面入手，更应该加强网络信息安全的管理工作，建立完善的信息安全管理体系。

1.1.3 信息安全面临的攻击

如前所述，虽然硬件设备的物理安全、软件技术安全以及人的因素都会给计算机和信息系统的安全带来极大的安全威胁，但精心设计的人为恶意攻击对信息安全的威胁最大，也最难防备。本节主要介绍人为恶意攻击的情况。

人为恶意攻击通常简称为人为攻击。对网络系统的各种人为攻击，通常都是通过寻找信息系统在存储、共享和传输过程中的弱点，以非授权的方式达到非法窃听、欺骗、篡改和破坏等目的。采用不同的分类标准(如攻击手段、攻击目标等)，会得出不同的分类结果。根据人为攻击对信息系统的影响和不同危害，通常把人为攻击分为主动攻击和被动攻击两大类。

1. 被动攻击

被动攻击通常也称为窃听或截取，它是指在不影响计算机及网络系统正常工作的情况下，攻击者未经用户同意和允许通过搭线窃听、无线截获甚至是采用病毒木马等方式对他人传输的信息进行窃听、监测、截获、破译等，以获取文件或程序的非法拷贝等机密信息。攻击者的目标是获得传输的信息，不会对双方通信的信息做任何改动。

正常的信息流动如图 1-1(a)所示，被动攻击如图 1-1(b)所示。

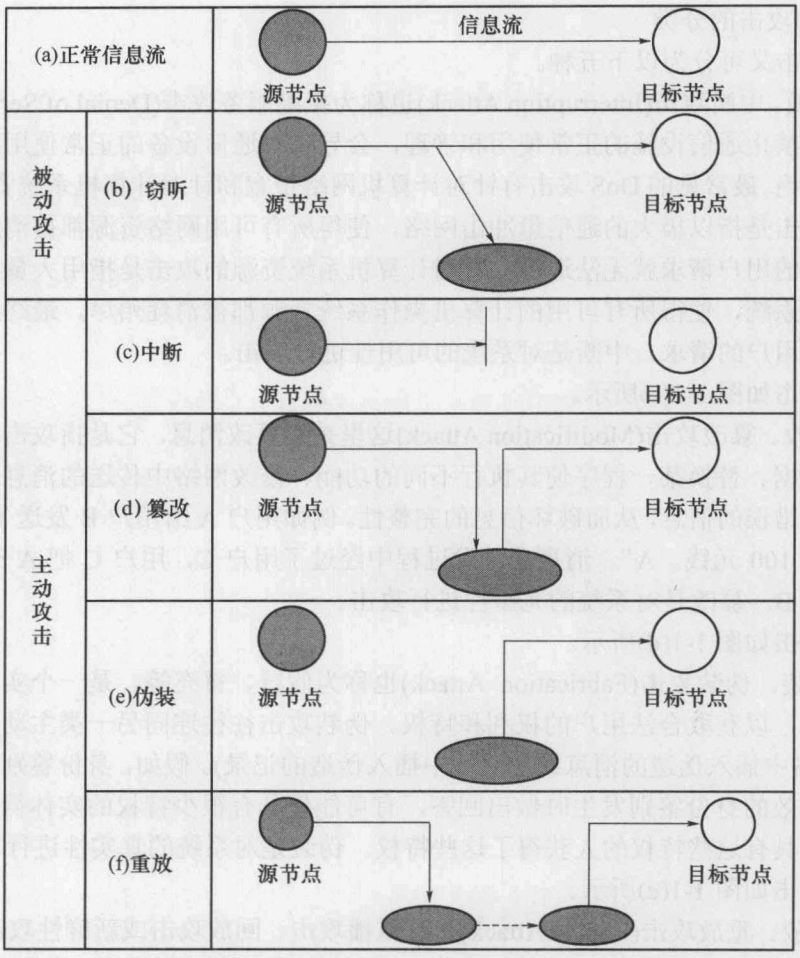

图 1-1　安全攻击的几种主要形式

被动攻击是对系统的保密性进行攻击，使得信息的保密性遭到破坏、信息泄露而用户又无法察觉，因此，会给用户带来巨大的损失。

被动攻击不易被发现，常常是主动攻击的前期侦察阶段，用来收集信息。由于被动攻击不对消息做任何修改，基本不会留下任何痕迹，因而是难以检测的，所以抗击这种攻击的重点在于预防而非检测。预防被动攻击的具体措施包括采用加密技术来保护信息、使用虚拟专用网 VPN 来增强系统的安全性或者使用加保护的分布式网络等。

被动攻击又分为两类：一类是获取通信信息的内容，这很容易理解；另一类是进行业务流分析(也称为流量分析)，这种情况比较微妙，假如我们通过某种手段，例如，加密屏蔽了信息的内容或者其他通信量，使得攻击者从截获的消息中无法得到消息的真实内容，然而攻击者却有可能获得消息的格式、确定通信双方的位置和身份以及通信的次数和消息的长度，这些信息可能对通信双方来说是敏感的，不希望被攻击者得知。

2. 主动攻击

主动攻击是指通过对数据流的某些篡改或产生某些假的甚至中断数据流等各种攻击方式有选择地破坏信息的完整性、有效性和可用性等。

1) 主动攻击的分类

主动攻击又可分为以下五种。

(1) 中断。中断攻击(Interruption Attack)也称为拒绝服务攻击(Denial of Service，DoS)，是指阻止或禁止通信设施的正常使用和管理，会导致对通信设备的正常使用或者管理被无条件地拒绝。最常见的 DoS 攻击有针对计算机网络带宽和针对计算机系统资源的攻击。网络带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求就无法通过。针对计算机系统资源的攻击是指用大量的连接请求冲击计算机系统，使得所有可用的计算机操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。中断是对系统的可用性进行攻击。

中断攻击如图 1-1(c)所示。

(2) 篡改。篡改攻击(Modification Attack)这里是指篡改消息，它是指攻击者修改数据文件中的数据、替换某一程序使其执行不同的功能、修改网络中传送的消息内容等，使接收方得到错误的信息，从而破坏信息的完整性。例如用户 A 给用户 B 发送了一份消息："请给我汇 100 元钱。A"。消息在转发过程中经过了用户 C，用户 C 把 A 改成 C 了，然后发送给 B。篡改是对系统的完整性进行攻击。

篡改攻击如图 1-1(d)所示。

(3) 伪装。伪装攻击(Fabrication Attack)也称为假冒、冒充等，是一个实体假装成另外一个实体，以获取合法用户的权利和特权。伪装攻击往往连同另一类主动攻击一起进行(如在网络中插入伪造的消息或在文件中插入伪造的记录)。假如，身份鉴别的序列被捕获，并在有效的身份鉴别发生时做出回答，有可能使具有很少特权的实体得到额外的特权，这样不具有这些特权的人获得了这些特权。伪装是对系统的真实性进行攻击。

伪装攻击如图 1-1(e)所示。

(4) 重放。重放攻击(Replay Attack)又称重播攻击、回放攻击或新鲜性攻击(Freshness Attack)，是指攻击者恶意的欺诈性的重复或拖延正常的数据传输，主要用于身份认证过程中捕获认证信息，并在其后利用旧的认证进行重放，这样就可以获得比其他实体更多的权限，从而破坏认证的正确性。重放是对系统的真实性进行攻击。

重放攻击如图 1-1(f)所示。

(5) 分布式拒绝服务。分布式拒绝服务(Distributed Denial of Service ，DDoS)攻击，又称为洪水攻击，顾名思义，就是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者(黑客)使用一个偷窃账号将 DDoS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通信，代理程序已经被安装在 Internet 上的许多被攻陷的计算机上，这些被攻陷的计算机通常称作"傀儡机"、"僵尸"或者"肉鸡"。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行，使许多分布的主机同时攻击一个目标，用以把目标计算机的网络带宽资源及计算机系统资源耗尽，以达到瘫痪网络以及系统的目的，从而导致目标瘫痪。DDoS 攻击是对系统的可用性进行攻击。例如，黑客可以通过将众多"肉鸡"组成一个僵尸网络(Botnet)，发动大规模 DDoS 攻击，进行带有利益的刷网站流量、E-mail 垃圾邮件群发，瘫痪预定目标受雇攻击竞争对手等商业活动。

图 1-2 给出了 DDoS 攻击过程的示意图。

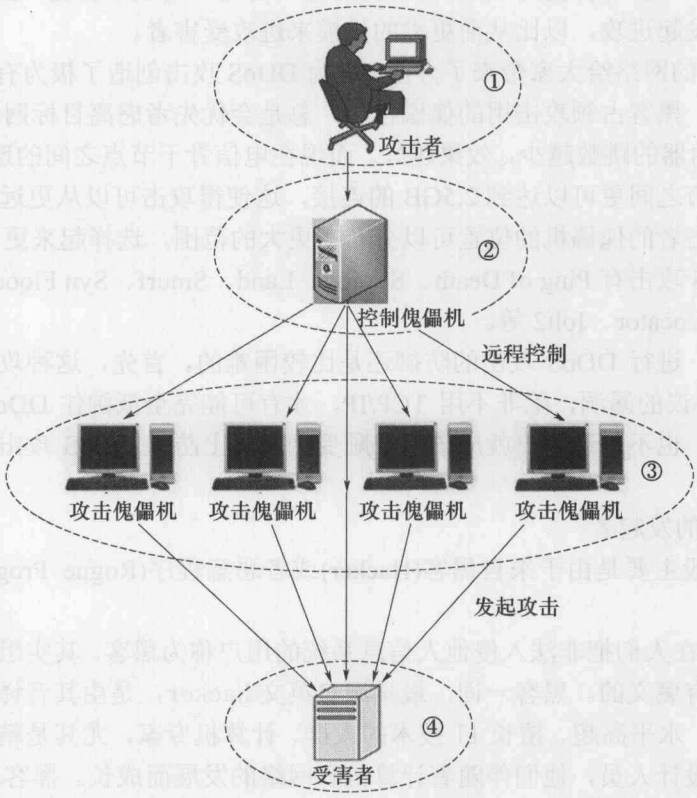

图 1-2 DDoS 攻击过程示意图

从图 1-2 可以看到，一个比较完善的 DDoS 攻击体系一般包括攻击者、控制傀儡机、攻击傀儡机、受害者四个部分，其中最重要的是第②部分和第③部分，分别用于控制和实际发起 DDoS 攻击。对于第④部分的受害者来说，DDoS 的实际攻击包是从第③部分攻击傀儡机上发出的，第②部分的控制傀儡机只发布命令而不参与实际的 DDoS 攻击。对于第②部分和第③部分的计算机，攻击者有控制权或者是部分控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与平常的程序一样允许并等待来自攻击者的指令。在平时，这些傀儡机并没有什么异常，只是一旦攻击者连接到它们并进行控制，且发出指令的时候，这些傀儡机就会发起攻击。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高时它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了，目标对恶意攻击包的“消化能力”加强了不少，例如，攻击软件每秒钟可以发送 3000 个攻击包，但受攻击的主机与网络带宽每秒钟可以处理 10000 个攻击包，这样一来攻击就不会产生什么效果。

这时候分布式的拒绝服务攻击手段(DDoS)就应运而生了。理解了 DoS 攻击的过程，