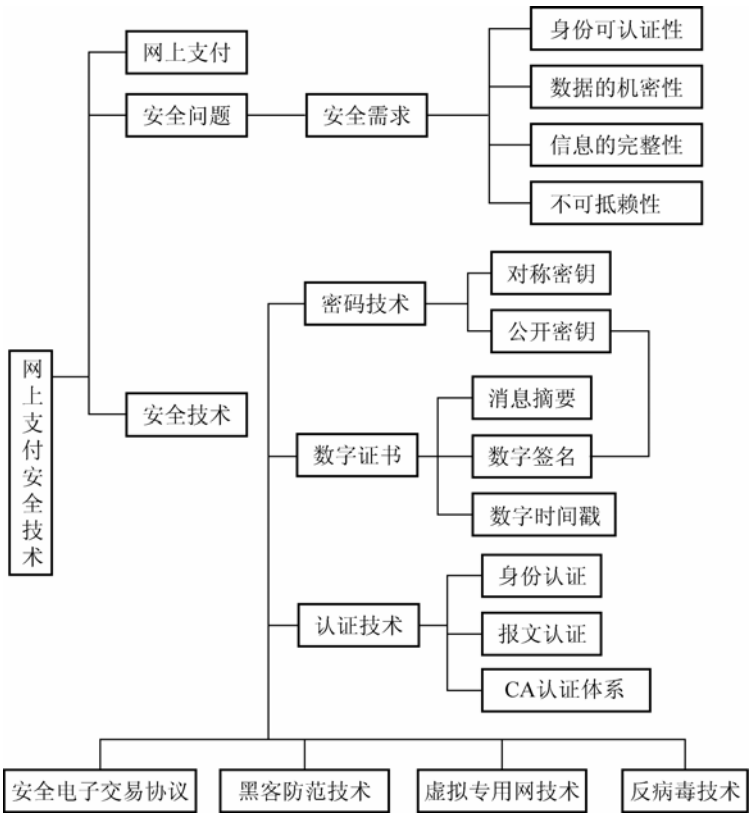
第9章　网上支付安全技术

教学目标与要求

- 了解网上支付中可能存在的风险，掌握网上支付的相关安全需求；
- 了解保障网上支付安全的多种技术；
- 掌握对称密钥体制原理及其常用的加密算法 DES；
- 掌握公开密钥体制原理及其常用的加密算法 RSA；
- 了解数字签名的概念及原理；
- 掌握数字证书的主要内容及其实现技术；
- 了解消息摘要、数字时间戳等安全技术；
- 了解网上支付中常用的几种认证技术。

知识架构



导入案例

“真假工行”事件

2006 年 4 月，不少市民反映收到邮件，邮件称“工行于 2006 年 4 月 22 日对电子银行系统进行升级，系统升级后，网上银行的注册用户需自行登录网上银行一次，以便认证您的网上支付资格”。记者发现，发件人的邮箱是 cwebmaster@icbc.com.cn，而工行平时给客户发送信息的邮箱统一为 webmaster@icbc.com.cn，二者只有一个字母之差。当记者登录 http://mybank.icbc.com.cn，在假冒网页中随意输入一组数字，单击“同意”按钮，网页显示登录成功，然后跳转至真正的工行网站。精通计算机的人士告诉记者，假冒网站很可能是通过这种手段盗取用户信息，如果输入的是真实信息，使用这些信息就会很容易盗走用户卡上的现金，导致严重后果。

一个用户告诉记者，他昨天上午首次登录该网址时能够进入假网站，但再次登录时就会自动跳转至真网站。把假的网址和真的网址串在一起，其用意是即使受骗人上当，也不会发现它是假的，而是认为工行出了问题。

随后，记者从工商银行官方网站进入个人网上银行。对比发现，假冒网站和工商银行的官方网站极为相似，但真正的工行网上银行在首次进入时会提示安装安全控件，而假冒的网站没有提示，可直接进入；真正的工行网站登录前需要填写注册卡号、登录 ID、验证码，而假冒的网站除了这 3 项，还需要填写证件号码。

工商银行总行电子银行部市场推广处副处长周永林表示，没有一家银行会以邮件或短信的方式向客户发布网银系统升级信息。同时，查询或进行网银交易时一定不要使用公共计算机。建议使用网上银行业务的个人用户，申请带有数字认证的U盘进行网上业务的办理。

值得注意的是，通常在这些假银行网站上暗藏了事先种下的木马程序或间谍程序。计算机防御能力弱的用户，只要点开了假网银的界面，计算机就会被植入木马或间谍程序。任意网银用户在该机上使用网银时就会被这些恶意程序监控到，并以数据包的形式传到不法分子预先设定的邮箱里。

资料来源：北京晚报。

“真假工行”事件给人们提出了疑问，网上银行、网上支付真的安全吗？应该采取哪些措施来保证电子商务中的支付安全呢？

9.1 网上支付安全概述

随着信息技术日新月异的发展，人类正在进入以网络为主的信息时代，基于 Internet 开展的电子商务已逐渐成为人们进行商务活动的新模式。电子商务作为一种新型网上在线贸易方式，使企业与消费者摆脱了传统的商业中介的束缚，但是电子商务交易中最为重要的环节——网上支付，其安全问题依然是阻碍电子商务快速发展的瓶颈之一。如何建立一个安全、便捷的网上支付环境，保证整个支付过程中信息的安全性，使基于 Internet 的电子支付方式与传统方式一样安全可靠，已经成为人们十分关心的热门话题。

网上支付不同于传统支付方式，它是基于互联网的一种实时支付结算活动。互联网开放式的信息交换方式使其网络安全具有很大的脆弱性。而互联网这种自身的开放性，决定了网上支付活动将面临不同类型的网络安全方面的挑战。不过，随着信息技术的进一步发

展，有理由相信，网上支付面临的各种安全性问题必将得到逐步解决。

本章首先从分析网上支付面临的各种安全性威胁出发，讨论了基于 Internet 进行的支付活动提出的安全需求，并由此提出相应的安全控制要求。在此基础上，概要地介绍用于网上支付的相关安全保密技术。

9.1.1 网上支付的安全问题

网上支付是电子支付的一种形式，是在信息时代诞生的一种全新的实时支付结算方式。广义地讲，网上支付是指客户、商家、网络银行(或第三方支付)之间使用安全电子手段，利用电子现金、银行卡、电子支票等支付工具通过互联网传送到银行或相应的处理机构，从而完成支付的整个过程。

网上支付的安全性是网上交易的核心和关键。由于 Internet 本身的开放性以及目前网络技术发展的局限性，使网上交易面临着种种安全性威胁，也带来了交易过程中的各种安全问题。下面首先讨论在互联网上进行商务交易过程中的安全问题。

当前网上支付较为普遍的方式是在网上交易过程中，使用银行卡(包括信用卡、借记卡和支付卡等)等支付工具，通过浏览器输入必要的支付认证信息，经发卡行认证授权后扣款完成在线支付。但不管网上支付活动采取什么样的方式、流程，人们最关心的问题还是支付安全，它是网上支付的基础，也是网上交易技术的难点。

由于网络自身的开放性和脆弱性，决定了网上支付活动将面临不同类型的网络安全方面的挑战。一般表现在对网络和网络服务器进行攻击。攻击的手段大致分为主动攻击和被动攻击。主动攻击指通过截获 IP 包，更改数据、伪造数据、伪造连接等手段欺骗用户或商家。被动攻击是指通过非法窃听、数据流分析等手段截取网络数据、非法获得信息。因此，现阶段的支付风险主要存在以下几个方面。

1. 支付被中断

在缺乏必要的安全防范措施情况下，攻击者通过非法入侵等方式攻击支付系统的可用性。这种情形下，攻击者可能破坏系统中的硬件或文件系统使系统无法正常工作，导致正常的计算机处理被破坏、延迟或完全拒绝服务。这种支付过程被中断的攻击往往会导致灾难性的后果。例如，某客户在上午 10 点向在线的证券交易公司发送委托购买 10 000 股某公司股票的指令，由于某种原因，证券公司在下午 1 点才收到这个指令，这时股票已经涨了 10%，这个指令的延迟就使客户蒙受占交易额 15%的损失。

2. 身份识别问题

在传统支付方式中，交易双方往往是面对面的，这样很容易确认对方的身份。即使不熟悉对方，也可以通过签名、印章、证书等一系列有形的身份凭证来确认对方身份。然而在网上交易中，双方在整个交易过程中都可能不见一面。如果不采取特殊的识别、防护等安全措施，就非常容易引起假冒、诈骗等违法活动。例如，在使用网上银行进行支付时，对于网上银行来说，怎样才能验证发出支付指令的客户是合法用户？对于客户来说，又该如何判断计算机屏幕上显示的网上银行支付中心不是黑客设计的钓鱼网站呢？

在网上支付中，如果不进行身份识别，第三方就有可能假冒交易一方的身份以破坏交易、破坏被假冒一方的信誉或盗取被假冒一方的交易成果等。

3. 支付信息被伪造、篡改

攻击者可以通过修改互联网传输中的数据，破坏数据的真实性和完整性，将伪造的假消息注入系统、假冒合法人介入系统、重放截获的合法消息或篡改支付指令的内容以实现非法牟取私利的目的。在无防护的网上支付过程中，非法侵入攻击者可以修改支付信息中的付款银行卡号、支付金额、收款人账号、支付指令序列，延迟或重放支付指令等。例如，某次网上支付中，客户给网上银行发出支付指令：“支付商户 A 1 000 元”。支付指令在公网传输过程中被黑客截获，将商户 A 篡改为商户 B。这样网上银行收到后就成了“支付商户 B 1 000 元”。其结果是非法商户 B 而不是合法商户 A 得到了银行划拨的资金。如果截获支付指令的黑客选择在网上反复重放该支付指令“支付商户 A 1 000 元”，结果是商户 A 将非法得到多笔由银行划拨的资金。

4. 支付信息被泄漏

在传统支付方式中，一般都是通过面对面的信息交换，或者通过可靠的通信渠道发送支付信息。而网上支付中的各方(如商户、银行、客户等)均存在于互联网中。当支付各方通过这个开放的公用互联网络交换信息时，如果不采取适当的保密措施，那么重要的支付信息则有可能被黑客窃取，导致巨大财产损失。

在网上支付中支付信息的泄漏主要包括两个方面：支付双方进行支付的内容被第三方窃取；一方提供给另一方使用的文件被第三方非法使用。例如，一旦攻击者通过某种方式得到持卡人的支付密码，可以轻易地冒充持卡人通过互联网进行消费，给持卡人带来损失。这是人们对网上支付安全的主要担心所在。

5. 支付信息被抵赖

在传统交易中，交易双方通过在交易合同、契约或支付凭据等书面文件上的手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。这也就是人们常说的白纸黑字。

网上支付是一个通过商业银行提供的网上结算服务将资金从付款人账户划拨到收款人账户的过程。对于资金划出操作，若付款人否认发出资金划出指令，商业银行将处于被动局面；对于资金划入操作，若商业银行否认资金划入操作，收款人将处于不利境地。在电子支付过程的各个环节中都必须是不可否认的，即支付一旦达成，发送方不能否认其发送的信息，接收方则不能否认其所收到的信息。

9.1.2 网上支付的安全需求

从上述可知，要保障网上支付过程安全有序地执行，必须建立一定的安全基础设施，能为不同的用户按不同安全需求提供多种安全服务。这些服务主要包括身份的可认证性、数据完整性、数据机密性、不可否认性、公正及时间戳服务等。这些安全因素从不同角度突出地反映了整个网上交易的安全问题。

1. 身份的可认证性

网上支付的首要安全需求就是要保证身份的可认证性。身份的可认证性意味着支付各

方可以相互认证彼此的真实身份，确认对方就是本次支付中所称的真正主体。认证是证实一个声称的身份或者角色，如用户、机器、节点等是否真实的过程。这一过程是网上支付安全系统不可缺少的组成部分。

2. 数据的机密性

数据的机密性是针对网络面临的被动攻击一类威胁而提出的安全需求。网上支付活动中一定要对敏感信息进行加密，即使别人截获或窃取了数据，也无法识别信息的真实内容，这样就可以使支付中的机密信息难以被泄露。

在网上支付过程中，数据的机密性非常重要。

3. 信息的完整性

保证信息的完整性是网上支付活动中的一个重要的安全需求。在开放的公网上进行支付活动不仅会遭受数据被截获、窃取、观察、监听等被动攻击，还会遭受支付信息被篡改、信息的完整性和有效性被破坏等主动攻击。

这意味着支付各方必须要能够验证收到的信息是否完整，即信息是否被人篡改过，或者在数据传输过程中是否出现信息丢失、信息重复等差错。

4. 不可抵赖性

保证不可抵赖性也是网上安全需求中的一个重要方面。在无纸化的网上交易方式下，通过手写签名和印章进行贸易方的鉴别已是不可能的。必须要在交易信息的传输过程中为参与交易的个人、企业提供可靠的标识，使得对支付信息的内容及传输，信息主体不可抵赖。

9.1.3 网上支付的安全保密技术

针对前面介绍的网上支付所面临的安全性威胁，以及由此提出的安全需求，迄今为止，国内外学术界和相关厂商已指出了很多相应的解决方案，并且基本上满足了人们在 Internet 上开展安全的支付活动的愿望。在许许多多的解决方案中，涉及的安全保密技术主要有密码技术、认证技术、CA 安全认证体系、安全电子交易协议、虚拟专用网技术、反病毒技术、黑客防范及其他相关的网络安全技术。下面分别简要加以介绍。

1. 密码技术

通常信息加密的途径是通过密码技术实现的。密码技术是网上支付活动中采取的主要安全技术手段。密码技术的基本思想是伪装明文以隐藏它的真实内容，即将明文 X 伪装成密文 Y，伪装的操作称为加密，加密时所使用的信息变换规则称为密码算法。采用密码技术可以满足信息保密性的安全需求，避免敏感信息泄露的威胁。

密码技术是保护信息的保密性、完整性、可用性的有力手段，它可以在一种潜在不安全的环境中保证通信及存储数据的安全，密码技术还可以有效地用于报文认证、数字签名等，以防止种种电子欺骗。密码技术是认证技术及其他许多安全技术的基础，也是信息安全的核心技术。

2. 认证技术

认证技术是信息安全理论与技术的一个重要方面，也是网上支付安全的主要实现技术。采用认证技术可以直接满足身份认证、数据的机密性、信息的完整性、不可抵赖性等多项网上交易的安全需求，较好地避免了网上交易面临的假冒、篡改、抵赖、伪造等种种威胁。

认证技术主要涉及身份认证、报文认证、CA 认证等方面的内容。身份认证用于鉴别用户身份，报文认证用于保证通信双方的不可抵赖性和信息的完整性。在某些情况下，信息认证比信息保密更为重要。例如，在很多情况下用户并不要求购物信息保密，而只需要确认网上商店不是假冒的(这就需要身份认证)，确保自己与网上商店交换的信息未被第三方修改或伪造，并且网上商家不能赖账(这就需要报文认证)；商家也是如此。

报文认证用于保证通信双方的不可抵赖性和信息的完整性，它是指通信双方之间建立通信联系后，每个通信者对收到的信息进行验证，以保证所收到的信息是真实的过程。验证的内容包括：①证实报文是由预定的发方产生的；②证实报文的内容没有被修改过(即证实报文的完整性)；③确认报文的序号和时间是正确的。

目前，在网上支付活动中广泛使用的认证方法和手段主要有数字签名、数字摘要、数字证书、PKI 安全体系，以及其他一些身份认证技术和报文认证技术。将在 9.4 节中详细讨论网上活动中涉及的认证技术。

3. 安全电子交易协议

电子交易可以说是电子商务活动的核心内容。如何在开放的公用网上构筑安全的交易模式，一直是业界研究的热点。毫无疑问，只有建立在密码技术和认证技术的基础上，才有可能构筑一个安全的电子交易模式。例如，在线交易安全的首要前提是要保证能正确识别和验证参与交易活动的各个主体，如验证持卡消费者、商家和支付网关的身份合法性。

目前有两种安全在线支付协议被广泛采用，即安全套接层(Secure Sockets Layer，SSL)协议和安全电子交易(Secure Electronic Transaction，SET)协议。二者均是成熟和实用化的协议，能为电子商务提供有力的安全保障。SSL 协议是由网景(Netscape)公司推出的一种安全通信协议，它能够对信用卡和个人信息提供较强的保护。SET 协议是由 MasterCard 和 VISA 以及其他一些业界主流厂商联合推出的一种规范，用来保证在公共网络上银行卡支付交易的安全性。SET 是一个非常复杂的协议，它定义了加密信息的格式和完成一笔卡支付交易过程中各方传输的规则。将在第 10 章中对 SET 协议和 SSL 协议进行详细讨论。

4. 黑客防范技术

目前，黑客攻击已成为网络安全所面临的最大威胁，同时黑客防范技术也成为网络安全的主要内容，受到了各国政府和网络业界的高度重视。

为了有效地防范黑客，首先需要掌握黑客入侵使用的一些技术。这些技术主要包括缓冲区溢出攻击、特洛伊木马、端口扫描、IP 欺骗、网络监听、口令攻击、拒绝服务(Dos)攻击等。只有很好地掌握了这些黑客技术，才有可能做到“知彼知己，百战不殆”。在了解黑客技术的基础上，目前人们已提出了许多相应有效的反黑客技术，主要包括安全扫描工具、防火墙技术、入侵检测技术、防病毒技术等。下面对上述几种反黑客技术简要加以介绍。

1) 安全扫描工具

安全扫描工具又称为扫描器，是一种自动检测远程或本地主机和网络安全性弱点的程序。通过使用扫描器可以不留痕迹地发现远程或本地服务器的各种 TCP 端口的分配、服务软件及其版本。通过安全扫描工具，可以间接地或直观地了解到远程或本地主机所存在的安全问题。例如，是否能用匿名登录、是否有可写的 FIP 目录、是否能用 TELNET、HTTPD 是用 root 还是用 nobody 在运行。

商品化的安全扫描工具为网络安全漏洞的发现提供了强大的支持。安全扫描工具通常分为基于服务器和基于网络的扫描器。基于服务器的扫描器主要扫描服务器相关的安全漏洞，如 password 文件、目录和文件权限、共享文件系统、敏感服务、软件、系统漏洞等，并给出相应的解决办法。基于网络的安全扫描主要扫描设定网络内的服务器、路由器、网桥、交换机、访问服务器、防火墙等设备的安全漏洞，并可设定模拟攻击，以测试系统的防御能力。

2) 防火墙

当一个网络接上 Internet 之后，系统的安全除了考虑计算机病毒、系统的健壮性之外，更重要的是防止非法用户的入侵。而目前防止的措施主要是靠防火墙技术完成。网络防火墙是一种用来加强网络之间访问控制的特殊网络设备，它对两个或多个网络之间传输的数据包和连接方式按照一定的安全策略进行检查，从而决定网络之间的通信是否被允许。其中，被保护的网络称为内部网络或私有网络，而另一方则被称为外部网络或公用网络。防火墙能有效地控制内部网络与外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤不良信息的目的。

3) 入侵检测技术

入侵检测系统(IDS)是对计算机和网络资源的恶意使用行为进行识别和相应处理的系统。它通过对计算机系统进行监视，提供实时的入侵监测，并采取相应的防护手段。它的目的在于监测可能存在的攻击行为，包括来自系统外部的入侵行为和来自内部用户的非授权行为。

入侵检测技术是一种主动保护自己免受黑客攻击的一种网络安全技术。入侵检测系统在发现入侵后，会及时做出响应，包括切断网络连接、记录事件和报警等。入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测技术帮助系统对付网络攻击，扩展了系统管理员的安全管理能力，提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，判断是否有违反安全策略的行为和遭到袭击的迹象。入侵检测在不影响网络性能的情况下能对网络进行监测，提供对内部攻击、外部攻击和误操作的实时保护。

入侵检测系统使系统管理员能随时了解网络系统(包括程序、文件和硬件设备等)的任何变更，还能为网络安全策略的制定提供指南。更为重要的是，入侵检测系统管理、配置简单，从而使非专业人员也能非常容易地对网络实施安全保护。

5. 虚拟专用网技术

虚拟专用网(VPN)技术是一种在公用互联网络上构造企业专用网络的技术。通过 VPN 技术，可以实现企业不同网络的组件和资源之间的相互连接。虚拟专用网络技术支持客户

计算机在 Internet 等公共互联网络上，以安全的方式与位于企业内部网内的服务器建立连接。VPN 对用户端透明，用户如同使用专用网络一样进行数据的传输。

VPN 网络可以利用 IP 网络、帧中继网络和 ATM 网络建设。VPN 的具体实现是采用隧道技术，将企业的数据封装在隧道中进行传输。隧道协议可分为第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 GRE、IPSec 等。

这种跨越 Internet 建立的 VPN 连接在逻辑上等同于两地之间使用专用广域网建立的连接。VPN 利用公共网络基础设施为企业各部门提供安全的网络互联服务，它能够使运行在 VPN 之上的商业应用享有几乎和专用网络同样的安全性、可靠性、优先级别和管理性。

6. 反病毒技术

在网络环境下，计算机病毒具有不可估量的威胁性和破坏力，已成为威胁网上支付安全的一个的重要因素。防范计算机病毒是网络安全性建设中重要的一环。

反病毒技术主要包括预防病毒、检测病毒和清除病毒 3 种技术：①预防病毒技术，它通过自身常驻系统内存优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏，这类技术有加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡)等；②检测病毒技术，它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等；③清除病毒技术，它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

从目前病毒入侵系统的情况来看，病毒入侵的途径主要有电子邮件、Internet 的下载文件、光盘和软盘。尤其是随着网络技术的广泛应用，通过电子邮件传染病毒已经逐渐取代磁盘而成为病毒传播的主流途径。在新技术环境下，病毒的存在形式也发生了变化。它除了以正常的文件形式进行传播外，压缩文件及可执行文件也成了目前病毒传染的重要途径。

随着系统环境、应用环境和网络环境的不断庞大，病毒种类呈多样化发展，其破坏性也在不断增强。一个安全的网上支付系统首先应具备实时防毒和定时杀毒的技术，在系统的整个工作过程中，针对病毒传播的途径和方式提供全方位的防护，形成一个完善的防护体系。只有随时防止病毒从外界侵入系统，才能全面提高支付系统的可靠性和安全性，达到防患于未然的目的。

9.2 密 码 技 术

密码技术使用密码算法对数据作变换，使得只有密钥持有人才能恢复数据面貌，主要目的是防止信息的非授权泄漏。现代密码学的基本原则是：一切密码寓于密钥之中，即算法公开，密钥保密。常用密码体制可分为对称密钥体制、公开密钥体制两大类。

9.2.1 对称密钥体制

对称密码体制(也叫做单钥密码体制)是指加密密钥和解密密钥为同一密钥或者虽然不相同，但是由其中任意一个可以很容易地推导出另一个的密码算法。早期使用的加密算法大多是对称密码体制，所以对称密码体制通常也称作传统密码体制，或常规密码法则。在

这种密码体制下，有加密(或解密)的能力就意味着必然也有解密(或加密)的能力。因此，信息的发送者和信息的接收者在进行信息的传输与处理时，必须共同持有该密码(称为对称密码)。

对称密码体制的优点是使用的加密算法简短高效，且具有很高的保密强度，破译极其困难；处理速度快(加/解密速度能达到数十 Mb/s 或更高)，算法简单，计算开销小，尤其适合加密大量数据。

由于对称密钥系统的保密性主要取决于密钥的安全，进行安全通信前需要以安全可靠的方式进行密钥交换。密钥交换的规模复杂、管理十分困难。在公开的计算机网络上安全地传送和保管密钥更是一个严峻的问题。因为任何人拥有了密钥就可以解开加密信息。密钥管理成为影响系统安全的关键性因素，使对称密码体制难以满足系统的开放性要求。

对称密码体制按照对明文数据的加密方式不同，可以分为序列密码和分组密码两类。分组密码体制与序列密码体制相比，在设计上的自由度比较小，但它具有容易检测出对信息的篡改、不需要密钥同步等优点，使其具有很强的适应性和广泛的用途。常用的对称密钥算法有 DES(Data Encryption Standard)算法、TDES(Triple DES)算法、IDEA(International Data Encryption Algorithm)算法、Blowfish 算法等。下面主要讨论几种常用的分组密码算法。

1. DES 算法

DES(Data Encryption Standard)加密算法是由 IBM 公司研制的，经过美国政府的加密标准筛选后，于 1977 年被美国正式定为联邦信息标准。随后，DES 在国际上受到了极大的重视，ISO 曾将 DES 作为非机密数据的加密标准。它是商业领域使用最广泛的密钥系统，特别是在保护金融数据的安全中。例如，自动取款机(Automated Teller Machine，ATM)就使用 DES。

DES 算法是一个分组加密算法，它以 64 位(8B)为分组对数据加密，其中有 8 位奇偶校验，有效密钥长度为 56 位。64 位一组的明文从算法的一端输入，64 位的密文从另一端输出。DES 是一个对称算法，加密和解密用的是同一算法。DES 的安全性依赖于所用的密钥。

DES 是一种分组密码体制，它对 64 位二进制数据加密，产生 64 位密文数据。使用的密钥为 64 位，实际密钥长度为 56 位(有 8 位用于奇偶校验)，即其中的第 8，16，24，32，40，48，56，64 位用于奇偶校验。DES 加密算法的过程如图 9.1 所示。它主要由以下 3 步组成。

1) 初始变换

其中 64 位的明文 X 按表 9-1 中 IP 换位表进行初始置换。

表 9-1　换位表

(a) IP 换位表								(b) IP^{-1} 换位表							
58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27

续表

(a) IP 换位表								(b) IP^{-1} 换位表							
61	53	45	37	29	21	13	5	34	2	42	10	50	18	58	26
63	55	47	39	31	22	15	7	33	1	41	9	49	17	57	25

置换的意思是指重新排列明文。表 9–1 中的初始置换 IP 就是把原明文的第 58 位放到第 1 位，原第 50 位放到第 2 位，原第 7 位放到第 64 位。这里第 x 位是从最高有效位到最低有效位数(左到右)。

明文经过初始置换(IP)后得出 X_0，其前 32 位作 L_0，后 32 位作 R_0。

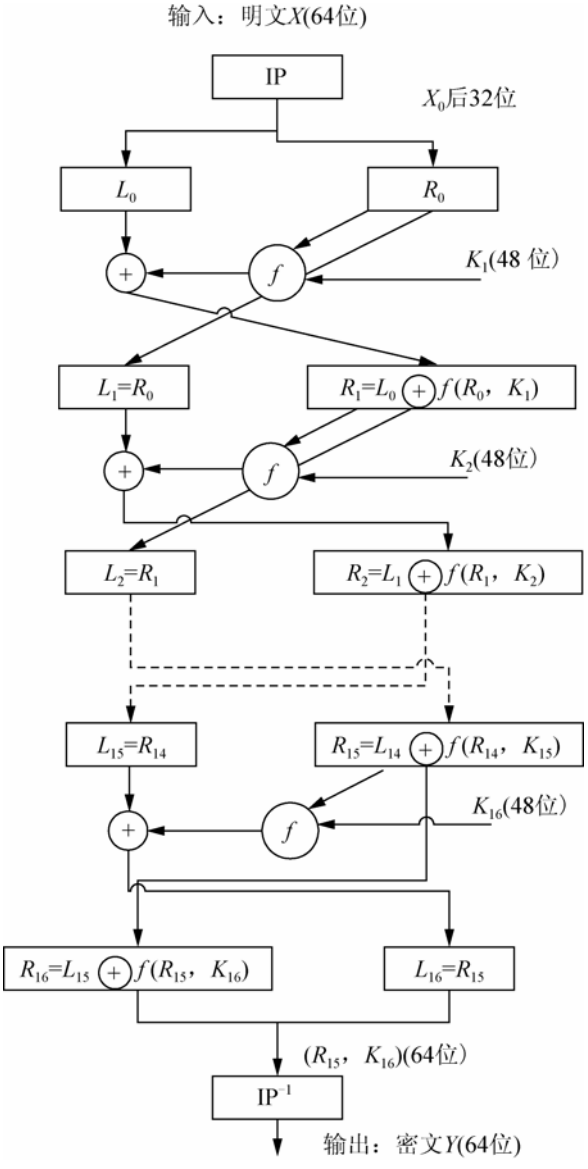


图 9.1　DES 加密标准

2) 迭代变换

经过初始换位后得到的 X_0(分为 L_0 和 R_0)，再经过 16 次完全相同的依赖于密钥的迭代变换。图中用 $X_i=L_iR_i$ 来表示第 i 次的迭代结果，同时令 L_i 和 R_i 分别代表 X_i 的前 32 位和后 32 位，其中 $1\leqslant i\leqslant 16$，则

$$L_i=R_{i-1}$$

$$R_i=L_{i-1}\oplus f(R_{i-1},K_i)$$

其中 $\oplus$ 代表两个比特串的异或运算。K_i 是一些由初始的 56 位密钥经过密钥函数产生的 48 位的子密钥。在每次迭代中要进行函数 f 的变换、模 2 加运算以及左右半边交换。

3) 逆初始变换

在最后的一次迭代之后左右半边没有交换，而是将 R_{16} 和 L_{16} 合成为 64 位的 $R_{16}L_{16}$，然后经逆置换 IP^{-1}(表 9-1)，得到密文输出。

DES 加密中起关键作用的是函数 f。它是一个非常复杂的变换，这些复杂变化的细节都没有画在图中。$F(R_{i-1}，K_i)$先将 32 位的 R_{i-1} 进行变换，扩展成 48 位，记为 $E(R_{i-1})$。48 位的 $E(R_{i-1})$与 48 位的 K_i 按位异或以后，所得的 48 位结果顺序地划分为 8 个 6 位长的组 B_1，B_2，…，B_8，即

$$E(R_{i-1})\oplus K_i = B_1B_2\ldots B_8$$

然后将 6 位长的组经过称为“S 变换”的替代转换为长 4 位的组(S 也是一个复杂的函数)，或写为 $B_j\rightarrow S_j(B_j)$，(j=1,2,…,8)。这里要用到 8 个不同的 S 函数($S_1,S_2,\cdots,S_8$)。将所得的 8 个 4 位长的 $S_j(B_j)$按顺序排好，再进行一次置换得出 32 位的 $f(R_{i-1}，K_i)$。

解密过程和加密相似，但生成 16 个密钥的顺序正好相反。

上述的 DES 的一个明显的缺点就是它实际上就是一种单字符替代，而这种字符的长度是 64 位。也就是说，对于 DES 算法，相同的明文就产生相同的密文。这对 DES 的安全性来说是不利的。为了提高 DES 的安全性，可采用加密分组链接的方法，如图 9.2 所示。

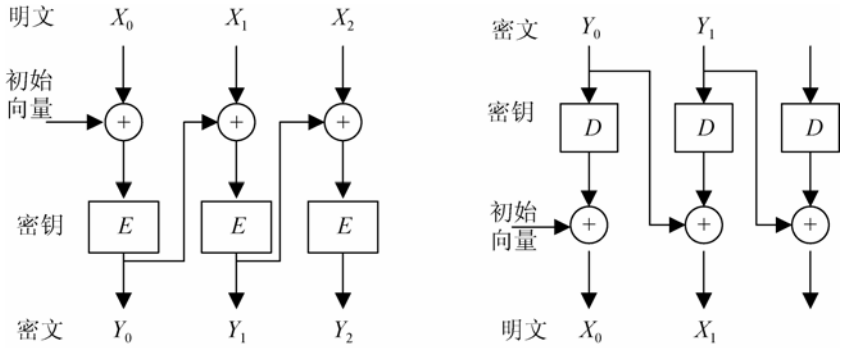


图 9.2 加密分组的链接

图 9.2 左部是加密过程。64 位的明文分组 X_0 先和初始向量逐位进行异或运算，然后进行加密操作得到密文 Y_0。再将 Y_0 和下一个明文分组 X_1 进行异或运算后再加密，得出密文 Y_1。以后都用相同的方法进行操作。不难看出，即使出现明文相同的分组，加密后得到的密文也是不一样的。

图 9.2 右部是解密过程。密文分组 Y_0 先解密，再和初始向量进行异或运算，得出明文 X_0。

下一个密文分组在经过解密后，要和密文 Y_0 进行异或运算后才得出第二个明文分组 X_1。以后都用相同的方法进行操作。

DES 一度是世界上最知名的、使用最广泛的分组密码算法。自诞生之日起，一直不断地被人们研究和攻击。随着密码学家们对 DES 攻击的深入研究和计算机计算能力的飞速进步，DES 的安全性越来越让人们担忧。目前较为严重的问题是 DES 的密钥的长度。56 位长的密钥意味着共有 256 种可能的密钥，也就是说，共约有 7.6×1 016 种密钥。近年来，已经设计出来搜索 DES 密钥的专用芯片。如使用流水线技术的芯片，每秒可搜索 5 000 万个密钥。包含 5 760 个密钥搜索芯片的计算机，预期的搜索时间仅为 35h。

显然由于密钥长度太短，传统的 DES 标准已不再适用于要求加密强度高的应用场合。但是因为确定一种新的加密算法是否真的安全是极为困难的，而且 DES 的主要密码学缺点就是密钥长度相对比较短，所以人们并没有放弃使用 DES 算法，而是想出了一些解决其密钥长度问题的方法。

2. TDES 算法

近年来，关于如何改进 DES 的建议和新的算法已有不少。其中，Tuchman 提出的 TDES(Triple DES)算法运用较为普遍。TDES 是 DES 的一种替代物，它保持了软件中已有的投资，又使得蛮力攻击更加困难。TDES 使用两个密钥(每个 56 位)，对明文进行 3 次 DES 算法。假设这两个密钥是 K_1 和 K_2，其算法的步骤如图 9.3 所示。

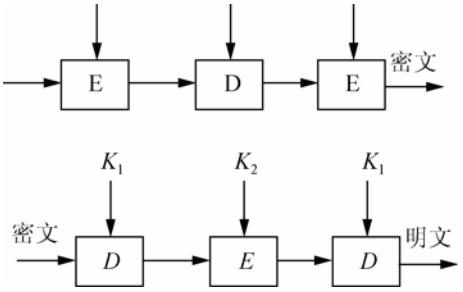


图 9.3 TDES 算法

(1) 用密钥 K_1 进行 DES 加密。

(2) 用密钥 K_2 对步骤(1)的结果进行 DES 解密。

(3) 用步骤(2)的结果使用密钥 K_1 进行 DES 加密。

这个过程称为 EDE，因为它遵循加密-解密-加密(Encrypt-Decrypt-Encrypt)次序。这种三重 DES 方法的加密强度相当于具有 112 位密钥长度的 DES 强度。不过，它的缺点是要比原来的 DES 多花费 3 倍时间。

3. IDEA 算法

IDEA(International Data Encryption Algorithm)是 1992 年由瑞士联邦技术学院 X.J.Lai 和 Massey 提出的。类似于 DES，IDEA 算法也是一种数据块加密算法。它是对 64 位大小的数据块进行加密的分组加密算法，密钥长度为 128 位。它基于“相异代数群上的混合运算”设计思想，算法用硬件和软件实现都很容易，且比 DES 在实现上快得多。IDEA 自问

世以来，已经经历了大量的详细审查，对密码分析具有很强的抵抗能力，在多种商业产品中被使用。

这种算法是在 DES 算法的基础上发展出来的，类似于三重 DES。设计者尽最大努力使该算法不受差分密码分析的影响，数学家已证明 IDEA 算法在其 8 圈迭代的第 4 圈之后便不受差分密码分析的影响。假定穷举法攻击有效，那么即使设计一种每秒可以试验 10 亿个密钥的专用芯片，并将 10 亿片这样的芯片用于此项工作，仍需 1 013 年才能解决问题；另外，若用 1 024 片这样的芯片，有可能在一天内找到密钥，不过人们还无法找到足够的硅原子来制造这样一台机器。目前，尚无一篇公开发表的试图对 IDEA 进行密码分析的文章。因此，就现在来看应当说 IDEA 是非常安全的。

9.2.2 公开密钥体制

1976 年 Whitfield Diffie 和 Martin Hellman 发表《密码学的新方向》一文，提出了公开密钥的思想。公钥密码体制是指加密密钥和解密密钥为两个不同密钥的密码算法，又称非对称密码术。不同于对称密码算法，它使用了一对密钥：一个用于加密信息，另一个则用于解密信息，通信双方无须事先交换密钥就可进行保密通信。其中加密密钥不同于解密密钥，加密密钥公之于众，谁都可以用；解密密钥只有解密人自己知道。

这两个密钥之间存在着相互依存关系，即用其中任一个密钥加密的信息只能用另一个密钥进行解密。若以公钥作为加密密钥，以用户专用密钥(私钥)作为解密密钥，则可实现多个用户加密的信息只能由一个用户解读；反之，以用户私钥作为加密密钥而以公钥作为解密密钥，则可实现由一个用户加密的信息可由多个用户解读。前者可用于数字加密，后者可用于数字签名。

相对于对称密钥算法，公钥密码体制的优点是使用非对称算法时通信双方事先不需要通过保密信道交换密钥；并且由于公钥可公开，使得密钥持有量大大减少，便于密钥管理、分发；此外它还提供了对称密钥体制无法或很难提供的数字签名服务等。但其缺点也很明显：加/解密速度慢、耗用资源大。一般来说只针对少量数据加密。由于进行的都是大数计算，使得 RSA 最快的情况也比 DES 慢上 100 倍。无论是使用软件或硬件实现加/解密，速度一直是 RSA 的缺陷。

常用的非对称密钥算法有 RSA 算法、DH 算法、ECC 算法等。下面主要讨论几种常用的非对称密钥算法。

1. RSA 算法

RSA 算法是由美国 MIT 的 3 位科学家 Rivest、Shamir 和 Aleman 于 1976 年提出，并在 1978 年正式发表的。它是一种公认十分安全的公钥密码算法，也是目前网络上进行保密通信和数字签名的最有效的安全算法。下面简单地介绍 RSA 算法的基本原理及应用。

RSA 算法是根据寻求两个大素数比较简单，而将它们的乘积分解开则极其困难这一原理来设计的。在这一算法中，每个用户有两个密钥：加密密钥 PK=(e,n)和解密密钥 SK=(d,n)。用户把加密密钥公开，使得系统中的任何其他用户都可以使用，而对解密密钥保密。这里，n 为两个大素数 p 和 q 的乘积(素数 p 和 q 一般为 100 位以上的十进制数)，e 和 d 满足一定的关系，当已知 e 时不能求出 d。其具体算法描述如下。

(1) 任意选取两个大素数 p 和 q，为了获得最大限度的安全性，两数的长度一样。

(2) 计算乘积：$n=p\times q$。

(3) 计算 n 的欧拉函数$(p-1)\times(q-1)$。

(4) 随机选取加密密钥 e，使 e 和$(p-1)\times(q-1)$互素。

(5) 计算解密密钥 d，以满足 $e\times d=1 \bmod((p-1)\times(q-1))$。其中，公钥=$(e,n)$，私钥=$(d,n)$。

(6) 选好这些参数后，将明文划分成长度小于 $\log n$ 位的明文块。若用 m 表示明文，用整数 c 表示密文，则加密过程是

$$c=m^e \bmod n$$

解密过程是

$$m=c^d \bmod n$$

可以证明，在 RSA 密码体制下，e 和 d 在功能上可以互相交换。在产生密钥时，可以先设一个 e，再由 e 求出 d；也可以先设 d，再由 d 求出 e。

下面举一个具体的运用 RSA 密码体制的简单例子。

假设甲和乙想要通过公开途径进行机密信息的传输。甲可以用以下的方式来产生一个公钥和一个密钥：取两个质数 p=11，q=13，p 和 q 的乘积为 $n=p\times q$=143，算出另一个数 $s=(p-1)\times(q-1)$=120；再选取一个与 s=120 互质的数，例如，e=7，对于这个 e 值，可以算出另一个值 d=1 039，满足 $e\times d=1 \bmod s$；其实可验证 7×103=721 除以 120 确实余 1。(n,e)和(n,d)这两组数分别为“公开密钥”和“秘密密钥”。

假设乙给甲送一个机密信息(明文，即未加密的报文)，在产生密文信息时，甲可使用预先与乙约好的格式将机密信息 H 转换为一个小于 n 的整数 m，比如他可以将每一个字转换为这个字的 Unicode 码，然后将这些数字连在一起组成一组数字。假如他的信息非常长，可以将这个信息分为几段，然后将每一段转换为 m。然后用公式 $c=m^e \bmod n$，可以将 n 加密为 c。甲得到乙的消息 c 后就可以利用密钥 d 来解码 $m=c^d \bmod n$，将 c 转换为 m，然后就可以将原来的信息 H 重新复原。

假设乙发出的机密信息 n=85，并且乙已经从公开媒体得到了甲的公开密钥(n,e)=(143，7)，于是计算出加密值 $c=m^e \bmod n=85^7 \bmod 143=123$ 发送给甲。甲在收到“密文”(即经加密的报文)c=123 后，利用只有他自己知道的秘密密钥(n,d)=(143，103)计算 $123^{103} \bmod 143$，得到的值就是明文(值)85，这样就实现了解密。

RSA 也可以用来进行数字签名。假如甲想给乙传递一个经过数字签名的消息的话，那么可以用消息计算一个散列值，然后用自己的私钥加密这个散列值并将这个“数字签名”加在消息的后面。这个消息只有用甲的公钥才能被解密。乙获得这个消息后可以用甲的公钥解密这个散列值，然后将这个数据与自己为这个消息计算的散列值相比较。假如两者相符的话，那么他就可以知道发信人持有甲的私钥，以及这个消息在传播路径上没有被篡改过。

假设偷听者丙获得了甲的公钥 N 和 e 以及乙的加密消息 c，但他无法直接获得甲的密钥 d。要获得 d，最简单的方法是从 c 算出 N，然后将 N 分解为 p 和 q，这样就可以计算$(p-1)\times(q-1)$并从而由 e 推算出 d。但至今为止还没有人找到一个多项式的计算方法来分解一个大的整数的因子。

RSA 算法的安全性基于数论中大数分解质因子的困难性。从一个公开密钥和密文中恢

复出明文的难度等价于分解两个大素数之积。因子分解越困难，密码就越难以破译，加密强度就越高，所以 RSA 需采用足够大的整数密钥。统计数据表明，在重要应用中，使用512 位的密钥已不安全，需要采用 1 024 位密钥。

2. DH 算法

DH 算法是最早的公钥算法，是 W.Diffie 和 M.Hellman 提出的。其实质是一个通信双方进行密钥协定的协议：两个实体中的任何一个使用自己的私钥和另一实体的公钥，得到一个对称密钥，这一对称密钥其他实体都计算不出来。

也即允许两名用户在公开媒体上交换信息以生成“一致”的、可以共享的密钥。由甲方产出一对密钥(公钥、私钥)，乙方依照甲方公钥产生乙方密钥对(公钥、私钥)。以此为基线，作为数据传输保密基础，同时双方使用同一种对称加密算法构建本地密钥对数据加密。这样，在互通了本地密钥算法后，甲乙双方公开自己的公钥，使用对方的公钥和刚才产生的私钥加密数据，同时可以使用对方的公钥和自己的私钥对数据解密。该算法源于中国的同余定理。

DH 算法的安全性基于有限域上计算离散对数的困难性。离散对数的研究现状表明：所使用的 DH 密钥至少需要 1 024 位，才能保证有足够的中、长期安全。

3. ECC 算法

ECC 算法(Elliptic Curve Cryptography)是基于椭圆曲线数学的一种公钥密码的方法。椭圆曲线在密码学中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出的。ECC 实际上代表着一类非对称加密方法，它的许多形式可能有稍微的不同，但所有的方法都依赖于解决椭圆曲线离散对数问题的困难性。它可以与 DH 等算法联合应用，组成 ECDH 等算法。

ECC 算法安全性的基础是在椭圆曲线点集上计算离散对数的困难性。这一安全性基础的改变导致了复杂的实现和处理过程，但却使得在保持安全性不变的情况下，所使用的密钥长度大为减小。ECC 算法的主要优势正是在某些情况下它比其他的方法使用更小的密钥，比如 RSA 提供相当的或更高等级的安全。ECC 的另一个优势是可以定义群之间的双线性映射，基于 Weil 对或是 Tate 对；双线性映射已经在密码学中进行大量的应用，例如基于身份的加密。不过 ECC 算法的一个缺点是加密和解密操作的实现比其他机制花费的时间长。

椭圆曲线点集上计算离散对数的研究现状表明：所使用的密钥至少需要 192 位，才能保证有足够的中、长期安全。

9.2.3 混合密钥加密技术

公开密钥加密技术较对称密钥加密技术处理速度慢，运行时占用资源多，因此通常把这两者结合起来实现最佳性能，即用公开密钥技术在通信双方之间传送对称密钥，而用对称密钥来对实际传输的数据加密、解密。这就是所谓的混合密钥加密技术。例如，A 向 B 采用混合加密技术发送保密信息，步骤如下。

(1) A 生成一个随机的对称密钥，又称会话密钥。

(2) A 用会话密钥加密明文。

(3) A 用 B 的公钥加密会话密钥。

(4) A 将密文及加密后的会话密钥传递给 B。

(5) B 使用自己的私钥解密会话密钥。

(6) B 使用会话密钥解密密文，得到明文。

使用混合加密技术，用户可以在每次发送保密信息时都使用不同的会话密钥，从而增加了密码破译的难度。即使某次会话密钥被破译了，也只会泄露该次会话信息，不会影响其他密文的传送。

9.3 数字证书技术

公开密钥体制通过使用公钥和私钥这一密钥对使得数字签名和其他一些密钥管理服务变得容易起来，从而提供了身份认证、数据完整性、数据保密性、不可否认性。然而，没有完整性保护措施就分发公钥会削弱这些安全服务，因此必须提供一种机制来保证公钥以及与公钥相关的其他信息不被偷偷篡改，并且还需要一种把公钥和它的声称所有者绑定的机制。本节的目的就是解释如何利用数字证书及其相关技术来提供上述机制。

9.3.1 消息摘要

在网上支付过程中经常需要验证消息的完整性，消息摘要函数(Message Digest)就提供了这一服务。消息摘要又称为数字摘要(Digital Digest)。它是一个唯一对应一个消息或文本的固定长度的值，它由一个单向 Hash 加密函数对消息进行作用而产生。如果消息在途中改变了，则接收者通过对收到消息的新产生的摘要与原摘要比较，就可知道消息是否被改变了。因此消息摘要保证了消息的完整性。

消息摘要是一种散列(Hash)变换，能对不同长度的输入信息产生固定长度的输出，即一个单独的 128～256 位的大数。这个大数称为原消息的“消息摘要”或“散列”。采用单向哈希(Hash)函数将需加密的明文“摘要”成一串固定长度的密文，该密文亦称为数字指纹(Finger Print)。不同的明文摘要成密文，其结果总是不同的，而相同的明文其摘要必定一致。

一个安全的散列函数 H 具有以下属性。

(1) H 能够应用到大小不一的数据上。

(2) H 对任何输入报文数据生成固定长度的输出。

(3) 对于任意给定的 x，$H(x)$的计算相对简单。

(4) 对于任意给定的 h，要发现满足 $H(x)=h$ 的 x 在计算上是不可行的。

(5) 要发现满足 $H(x)=H(y)$的(x, y)在计算上是不可行的。

消息摘要函数的抗冲突性使得如果一段明文稍有变化，哪怕只更改该段落的一个字母，通过哈希算法作用后都将产生不同的值。而 Hash 算法的单向性使得要找到哈希值相同的两个不同的输入消息，在计算上是不可能的。所以数据的哈希值，即消息摘要，可以检验数据的完整性。

哈希函数的这种对不同的输入能够生成不同的值的特性使得无法找到两个具有相同哈希值的输入。因此，如果两个文档经哈希转换后成为相同的值，就可以肯定它们是同一文档。所以，当希望有效地比较两个数据块时，就可以比较它们的哈希值。例如，可以通过比较数据发送前和发送后的哈希值来验证该数据在传递时是否修改。

由于消息摘要函数比对称加密算法的速度还快，因此有着广泛的应用。消息摘要函数是数字签名和消息识别码(MAC)的基础。构造消息摘要函数主要包括以下常用方法。

(1) MD5(Message Digest Algorithm 5) 算法。MD5 是由 R.Rivest 开发，经 MD2、MD3 和 MD4 发展而来，在 RFC 1321 中有详尽描述。MD5 按 512 位数据块为单位来处理输入，产生 128 位的消息摘要。MD5 广泛用于各种软件的密码认证和序列号的识别。如在 UNIX 系统中用户的密码是以 MD5 经 Hash 运算后存储在文件系统中的。当用户登录的时候，系统把用户输入的密码进行 MD5 运算，然后再去和保存在文件系统中的 MD5 值进行比较，进而确定输入的密码是否正确。通过这样的步骤，系统在并不知道用户密码的明码的情况下就可以确定用户登录系统的合法性，避免用户密码被系统管理员获知。

(2) SHA(Secure Hash Algorithm) 算法。SHA 是由 NIST 开发，并在 1993 年作为信息处理标准公布。SHA 与 MD5 的设计原理相似，同样也按 512 位数据块为单位来处理输入。SHA 对长度不超过 264 位的二进制消息产生 160 位的消息摘要输出，具有比 MD5 更强的安全性。SHA 已成为公认的最安全的散列算法之一，并被广泛使用。

9.3.2 数字签名

数字签名(Digital Signature)就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。

数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。数字签名主要的功能是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。在数字签名应用中，发送者的公钥可以很方便地得到，但他的私钥则需要严格保密。

数字签名的应用过程是将信息的摘要或其他与数据内容有关的变量用发送者的私钥加密，完成对数据的合法“签名”，然后将签名与原文一起传送给接收者。数据接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用 Hash 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比，以确认签名的合法性。这样通过对数据签名的验证，就可以检验签名前的信息内容在传输过程或分发过程中是否已被篡改并且可以确认发送者的身份。

数字签名技术是结合消息摘要函数和公钥加密算法的典型应用，主要应用在数字证书和交易通信过程中。

举例说明，若 A 向 B 发送消息，其创建数字签名的过程如下。

(1) 为保证签名的速度，A 先将原文进行单向 Hash 运算生成定长的消息摘要 A，如图 9.4 所示。

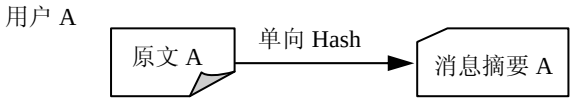


图 9.4　消息摘要的生成

(2) 利用自己的私钥加密消息摘要得到数字签名 A，并将数字签名附在原消息后面，如图 9.5 所示。

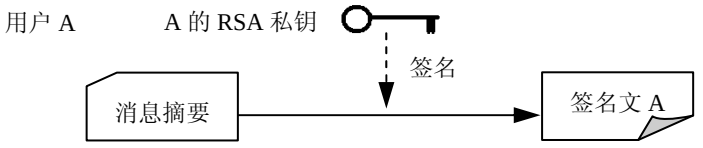


图 9.5　数字签名的生成

(3) 通信时用户 A 将自己的原文和签名文一起送给通信对方即用户 B，如图 9.6 所示。

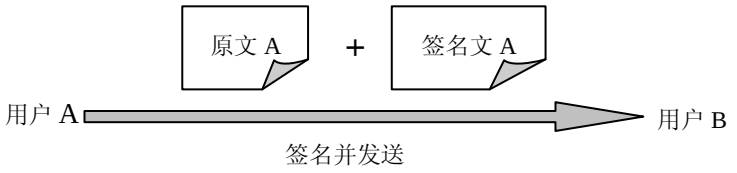


图 9.6　发送签名文

B 接收到消息，对数字签名进行验证的过程为：

由于用户 B 在检验用户 A 的身份即数字证书时保存了用户 A 的 RSA 公钥，所以此时就可以用用户 A 的 RSA 公钥来验证通信得到的签名文。整个验证过程如图 9.7 所示。

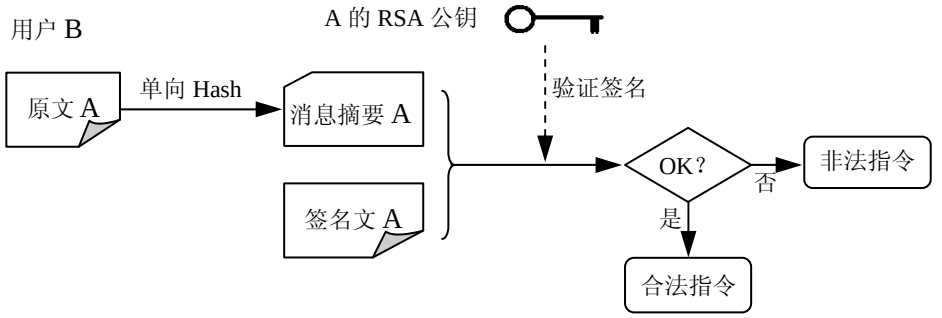


图 9.7　数字签名的验证

(1) 将消息中的原消息与数字签名分离出来。

(2) 使用 A 的公钥解密数字签名得到摘要。

(3) 利用散列函数重新计算原消息的摘要。

(4) 比较解密后获得的哈希摘要与重新计算产生的哈希摘要，若相等则说明消息在传输过程中没有被篡改，否则消息不可靠。

由上述数字签名及其验证的过程不难看出，该技术带来了以下 3 个方面的安全性。

(1) 信息的完整性：由消息摘要函数特性可知，若信息在传输过程中遭到篡改或破坏，B 重新计算的摘要必不同于用 A 的公钥解密出的摘要，则 B 可知该信息非 A 最初发送的信息。

(2) 信源确认：由于公钥与私钥存在一一对应关系。B 能用 A 的公钥解密出加密的摘要，且其值与重新计算出的摘要一致，则该消息必然是 A 发出的。

(3) 不可否认性：由于只有 A 持有自己的私钥，其他人不可能假冒身份，故 A 无法否认他发送过该消息。

9.3.3 数字时间戳

在支付活动中，时间和签名一样是十分重要的信息。在网上支付中，同样也需要对支付的日期和时间信息采取安全措施，参与支付各方不可抵赖。这需要在经过数字签名的支付信息上打上一个可信赖的时间戳，从而解决一系列的实际和法律问题。由于用户桌面时间很容易改变，由该时间产生的时间戳不可信赖，因此数字时间戳服务(DTS)通常是由专门的机构提供的网上安全服务项目。

数字时间戳(Time-Stamp)是一个经加密后形成的凭证文档，它包括以下 3 个部分。

(1) 需加时间戳的文件的摘要(Digest)。

(2) DTS 收到文件的日期和时间。

(3) DTS 的数字签名。

数字时间戳的使用过程如图 9.8 所示。需要数字时间戳的用户首先将文件用 Hash 算法加密得到摘要，然后将摘要发送到提供数字时间戳服务的专门机构，DTS 机构对原摘要加上收到文件摘要的时间信息后，用自己的私钥加密(数字签名)再发还给原用户，获得数字时间戳的用户就可以将它发送给自己的商业伙伴以证明信息的发送时间。注意，书面签署文件的时间是由签署人自己写上的，而数字时间戳则不然，它是由认证单位 DTS 来加的，以 DTS 收到文件的时间为依据。

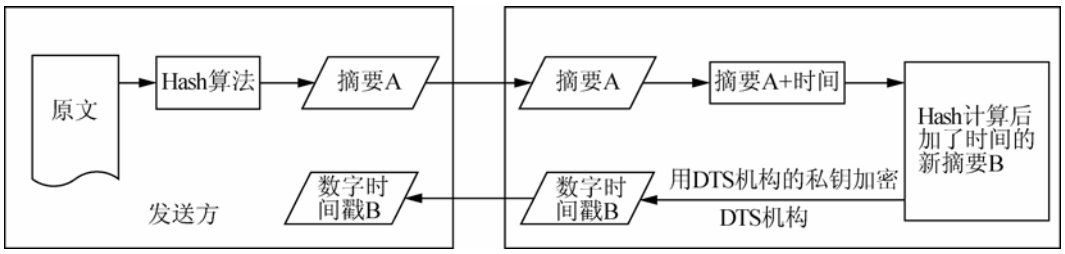


图 9.8 数字时间戳的生成

9.3.4 数字证书

不断发展的互联网技术使得顾客能极其方便轻松地在网上购物，但同时也增加了对某些敏感或有价值的数据被滥用的风险。为保证互联网上电子交易及支付的安全性、机密性，防范交易及支付过程中的欺诈行为，必须在网上建立一种信任机制。这就要求参加电子商务的买方和卖方都必须拥有合法的身份，并且在网上能够有效无误地被验证。

数字证书正是各类实体(持卡人/个人、商户/企业、网关/银行等)在网上进行信息交流及

商务活动的身份证明，在网上支付的各个环节，支付的各方都需验证对方证书的有效性，从而解决相互间的信任问题。在网上支付活动中，数字证书大多是由权威机构——CA(证书授权，Certificate Authority)中心发行的，能提供在 Internet 上进行身份验证的一种权威性电子文档。

作为身份验证的数字证书必须具有唯一性和可靠性。为了达到这一目的，需要采用很多安全技术来实现。通常，数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所有的私有密钥(私钥)，用它进行解密和签名；同时设定一把公共密钥(公钥)并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。公开密钥技术解决了密钥发布的管理问题，用户可以公开其公开密钥，而保留其私有密钥。

简单地说，证书的构成就是一个公钥，再加上公钥所有者的标识，以及被信任的第三方对上述信息的数字签名。公证方的数字签名保证了公钥及其所有者的对应关系，同时也保证了证书中的公钥信息不会被篡改。

数字证书由独立的证书发行机构发布。数字证书各不相同，每种证书可提供不同级别的可信度。从证书的用途来看，数字证书可分为签名证书和加密证书。签名证书主要用于对用户信息进行签名，以保证信息的不可否认性；加密证书主要用于对用户传送信息进行加密，以保证信息的真实性和完整性。

从数字证书遵循的标准和格式来看，存在很多不同种类的证书类型。它们包括：X.509 公钥证书、简单 PKI(Simple Public Key Infrastructure)证书、PGP 证书、属性(Attribute)证书等。这些证书具有各自不同的格式。并且，一种类型的证书可被定义为好几种不同的版本，每一种版本也可能以好几种不同的方式来具体实现。例如，X.509 证书就有 3 种版本。其中版本 3 的公钥证书包括好几种可选的不同扩展，可以用不同的应用方式来具体实现。

在所有格式的证书中，X.509 证书应用范围最广。在许多网络安全应用，如 VPN、S/MIME(Secure/Multipurpose Internet Mail Extension)中，都使用了 X.509 格式的证书，(在本文中，数字证书或证书仅仅是指 X.509 公钥证书。)

下面以 X.509 公钥证书为例，叙述数字证书的结构。

如图 9.9 所示，证书内容一般由以下几部分组成。

(1) 申请者的信息。用来刻画证书申请者的基本信息，其中包括证书拥有者的可识别名；证书所有人的公开密钥和算法识别符，包括公钥算法、公钥的位字符串表示；证书拥有者的唯一识别符。

(2) 证书信息。用来描述证书的一般属性，包括证书的版本信息，不同版本的证书格式不同；证书序列号指由证书颁发者分配的本证书的唯一标识符；证书的有效期限一般采用 UTC 时间格式，它的计时范围为 1950～2049；证书扩展信息是构建证书的可选的标准和专用扩展，包括证书策略、策略映射、密钥标识符、主体及颁发者的别名和主体目录属性等。

(3) 证书颁发者的信息。用来描述数字证书颁发者的签名和用来生成数字签名的签名算法。任何人收到证书后都能使用签名算法来验证证书是否是由颁发者的签名密钥签发的。

其中包括颁发者的标识信息，颁发者唯一标识符；颁发者签名算法及相关参数。

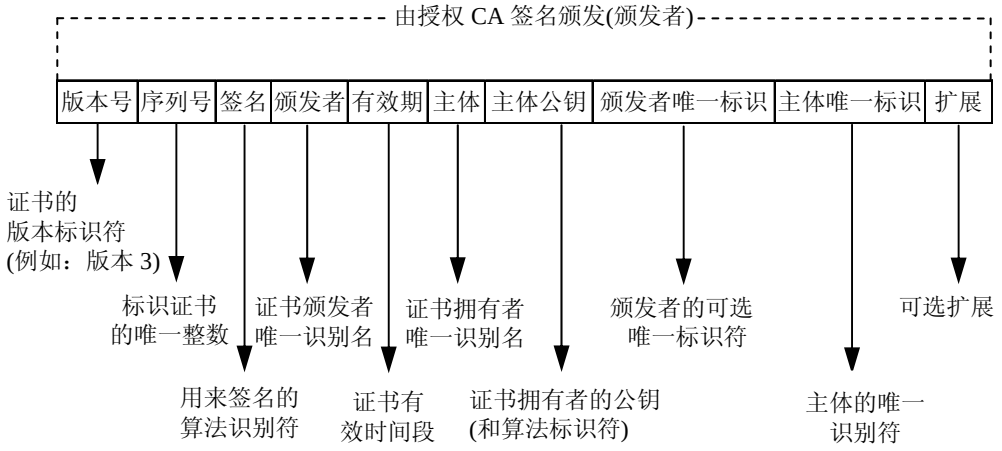


图 9.9　数字证书的结构

从数字证书的应用角度分类，数字证书可以分为以下几种。

(1) 服务器证书。服务器证书被安装于服务器设备上，用来证明服务器的身份和进行通信加密。服务器证书可以用来防止假冒站点。在服务器上安装服务器证书后，客户端浏览器可以与服务器证书建立 SSL 连接，在 SSL 连接上传输的任何数据都会被加密。同时，浏览器会自动验证服务器证书是否有效，验证所访问的站点是否是假冒站点，服务器证书保护的站点多被用来进行密码登录、订单处理、网上银行交易等。全球知名的服务器证书品牌是 VeriSign，Thawte，GeoTrust 等。

(2) 电子邮件证书。电子邮件证书可以用来证明电子邮件发件人的真实性。它并不证明数字证书上面 CN 一项所标识的证书所有者姓名的真实性，它只证明邮件地址的真实性。收到具有有效电子签名的电子邮件，不但能相信邮件确实由指定邮箱发出，还可以确信该邮件被发出后没有被篡改过。

如果使用接收的邮件证书，还可以向接收方发送加密邮件。该加密邮件可以在非安全网络传输，只有接收方的持有者才可能打开该邮件。

(3) 客户端个人证书。客户端证书主要被用来进行身份验证和电子签名。安全的客户端证书被存储于专用的 Usb Key 中。存储于 Key 中的证书不能被导出或复制，且 Key 使用时需要输入 Key 的保护密码。使用该证书需要物理上获得其存储介质 Usb Key，且需要知道 Key 的保护密码，这也被称为双因子认证。这种认证手段是目前在 Internet 最安全的身份认证手段之一。Key 的形式有多种，如指纹、口令卡等。

数字证书颁发过程一般为：用户首先产生自己的密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户发送而来，然后，认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。

通过数字证书以及对称和非对称密码体制等密码技术的运用，建立起一套严密的认证

系统，从而保证信息除发送方和接收方外不被其他人窃取；信息在传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己发送出的信息不能抵赖。这样，在网上的电子交易中，如果双方出示了各自的数字凭证，并用它来进行交易操作，就可以不用担心受骗上当了。

9.4 认 证 技 术

认证技术是网上支付安全的一个重要保障，也是信息安全理论与技术的一个重要内容。

常用的认证技术主要涉及身份认证、报文认证、服务器认证等方面的内容。

从概念上讲，作为一种证实信息交换过程合法有效的手段，认证主要包括如下几个方面的内容。

(1) 实体 A 与实体 B 在进行信息交换时，A 与 B 都必须对对方的身份进行认证，以保证它们所收到的信息都是由确认的实体发送过来的。

(2) 设实体 A 经过通信信道向实体 B 发送一段信息，那么作为收方的 B 必须知道它所收到的信息在离开 A 后是否被修改过，换句话说，B 必须证实它所收到的信息是真实的。

(3) 信息收方对收到的信息不能进行任意删改，也不能抵赖(否认)它所收到的信息。

(4) 发方不能抵赖它所发送过的信息。如果收、发双方发生争执，第三方必须能进行公正的判决。

(5) 对收到的信息，收方应能检测出是否是过时的信息，或者是某种信息的重播。

9.4.1 身份认证技术

身份认证是信息认证技术中十分重要的内容，它一般涉及两个方面的内容，一个是识别，一个是验证。所谓识别，就是指要明确用户是谁。这就要求对每个合法的用户都要有识别能力。要保证识别的有效性，就需要保证任意两个不同的用户都具有不同的识别符。所谓验证，就是指在用户声称自己的身份后，认证方还要对它所声称的身份进行验证，以防假冒。一般来说，用户身份认证可通过 3 种基本方式或其组织方式来实现。

1. 基于口令的身份认证

传统的认证技术主要采用基于口令的认证方法。系统为每一个合法用户建立一个用户名/口令对。当被认证对象要求访问提供服务的系统或使用某项功能时，提供服务的认证方要求被认证对象提交该对象的用户名和口令。认证方收到口令后，将其与系统中存储的用户口令进行比较，以确认被认证对象是否为合法的访问者。

然而，基于口令的认证方法存在下面几点不足。

(1) 用户每次访问系统时都要以明文方式输入口令，这时很容易泄密。

(2) 口令在传输过程中可能被截获。

(3) 系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件。

(4) 用户在访问多个不同安全级别的系统时，都要求用户提供口令，用户为了记忆的

方便，往往采用相同的口令。而低安全级别系统的口令更容易被攻击者获得，从而用来对高安全级别系统进行攻击。

(5) 只能进行单向认证，即系统可以认证用户，而用户无法对系统进行认证。攻击者可能伪装成系统骗取用户的口令。

对于第(2)点，系统可以对口令进行加密传输。对于第(3)点，系统可以对口令文件进行不可逆加密。尽管如此，攻击者还是可以利用一些工具很容易地将口令和口令文件解密。

使用这种方法进行身份认证简单、方便，但安全性极差，某安全性仅仅基于用户口令的保密性，一旦约定的口令、密码泄露或被截取，任何非授权人都可以冒充。通常用户使用的口令较短且容易猜测，因此这种方案不能抵御口令猜测攻击。

目前在大多数计算机系统中，为了加强口令的安全性，一般都将用户的口令采用单向函数运算存储。在这种情况下，攻击者不可能利用口令的密文形式恢复出明文形式。

2. 基于物理证件的身份认证

基于物理证件的身份认证是一种利用授权用户所拥有的某种东西来进行访问控制的认证方法。物理证件是一种个人持有物，其作用类似于钥匙用于启动信息系统。使用得比较多的是一种嵌有磁条的塑料卡，磁条上记录有用于机器识别的个人信息。这类卡通常和个人识别号(PIN)一起使用，安全性不高。这类卡易于制造，而且磁条上记录的数据也易于转录，因而安全性不高。为了提高卡片的安全性，现在普遍使用 IC 卡来代替传统的磁卡。

IC 卡又成为智能卡，是通过在一块塑料基片中嵌入集成电路而制成的卡片。它的外形与覆盖磁条的磁卡相似。根据卡中所嵌入集成电路的不同，可以将 IC 卡分成存储器卡、逻辑加密卡和 CPU 卡 3 类。

使用 IC 卡进行身份认证，前提条件就是需要保证系统能正确鉴别智能卡本身。目前主要采用加密技术进行智能卡的鉴别。根据所采用的密码体制不同，智能卡的鉴别主要分为两类：对称鉴别体制和非对称鉴别体制。智能卡的对称鉴别体制是智能卡常用的鉴别方法，它采用如 DES 这样的密码算法。在主机(或终端机)执行对智能卡的鉴别时，首先由主机产生一个随机数 R，并发送给智能卡，智能卡收到主机传来的数据 R，并结合卡内存储的密钥 K，进行加密运算 f，并产生出密文 X。然后卡片将 X 送给主机，主机从密钥库中检索出该卡片的密钥 K，利用 K 和 X 进行解密运算 f，得到 $R1$。如果 $R1=R$，则说明智能卡是合法的。同样，如果智能卡需要对主机(或终端机)进行鉴别时，也采用上述方法，只是数据流向相反，由智能卡产生随机数，并且在卡内判断主机的合法性。

3. 基于人体生物学特征的身份认证

基于人体生物学特征的身份认证，主要是指根据指纹、视网膜、面型、声音等人体组织特征的识别，进行身份认证。由于大部分人体组织特征具有信息量大、因人而异、特征稳定甚至终身不变等特点，因此它们也被称为一种不需记忆且随身携带的活口令。但从技术上说，上述几种组织特征都还存在一些缺陷：或者误识率过高，或者使用不便，或者价格昂贵，或者难以防伪。

什么样的生物识别系统比较适合用来进行身份认证呢？首先，不易模仿、特征稳定是第一个要求。例如，声音识别对使用者来讲虽然非常便利，但它很容易因感冒或外在音源

干扰，以致无法辨认。然后，准确性高、易于使用是第二个重要条件。目前出现的生物识别技术主要有指纹识别、脸部识别、眼球虹膜识别等。

9.4.2 报文认证技术

报文认证用于保证通信双方的不可抵赖性和信息的完整性。当通信双方之间建立通信联系后，接收方对收到的信息进行报文认证，即可保证所收到信息的真实性。报文认证可使接收者识别报文的源、内容的真伪，以及报文的时间性。报文认证的内容包括以下 3 部分。

(1) 确认报文是由预定的发送方产生的。

(2) 证实报文的完整性(即证实报文的内容没有被修改过)。

(3) 确认报文的序号和时间是正确的。

报文认证是基于密码技术进行的，通常包括基于对称密码体制的报文认证和基于公钥体制的报文认证。下面就按照密码体制的不同，分类介绍不同的报文认证技术，其中主要讨论报文源和报文内容的鉴别。关于报文的序号和时间性的认证，主要是阻止报文的重放攻击，常采用报文的流水作业号、链接认证符、随机数认证法、时间戳等技术，这里不多做介绍。

1. 基于对称密码体制的报文认证

这是一种简单的报文来源认证方法，通信双方使用共享密钥加/解密传输信息，并借以认证彼此身份。

设通信双方 A 和 B，A、B 共享的密钥 K_{AB}，M 为 A 发送给 B 的报文。为防止报文 M 在公共信道被窃听，A 使用共享密钥 K_{AB} 将 M 加密后再传送，如图 9.10 所示。

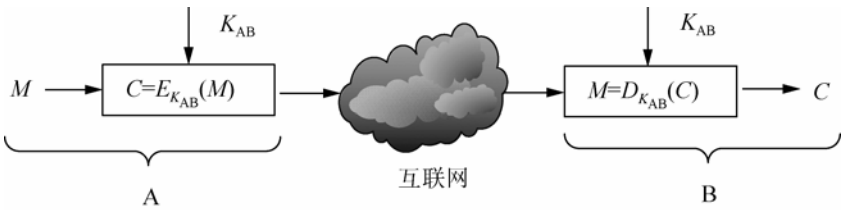


图 9.10 对称密钥报文认证

B 使用 K_{AB} 解密收到的密文 C，成功得到明文。由于 K_{AB} 为 A 和 B 的共享密钥，B 据此可以确定 M 是由 A 所发出的。

但这种基于对称密码体制的报文认证方法却不能提供报文完整性的鉴别。为检验报文的完整性，报文发送方可以在报文中加入一个鉴别码并经加密后发送给接收者检验。接收方使用约定算法对解密后的报文进行运算，将运算得到的鉴别码与收到的鉴别码进行比较。若二者相等，则接收，否则拒绝接收。单向哈希函数提供了一种良好的检验报文完整性的方法，如图 9.11 所示。另外，也可采用报文认证码(MAC)和篡改检测码(MDC)实现完整性鉴别。

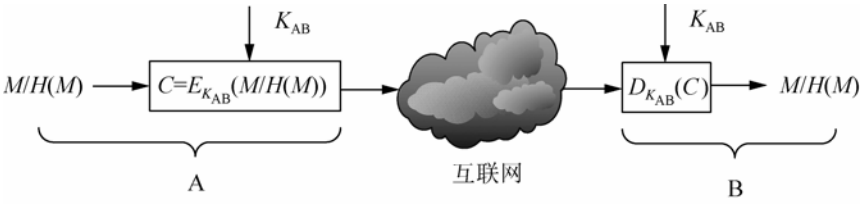


图 9.11　利用哈希函数的对称密钥报文认证

在图 9.11 中，A 先对 M 求哈希值 $H(M)$，然后将 $M/H(M)$使用共享密钥 K_{AB} 加密后传送给 B，B 通过解密并验证附于报文 M 后的哈希值是否正确。

这种认证方法的优点是速度较快，其缺点是通信双方 A 和 B 需要事先约定共享密钥。更为重要的是，若 A 需要与 n 个用户通信，则 A 不仅需要事先约定 $n-1$ 个密钥，并且还应妥善保存这些密钥。在大型网络环境下，这一要求使得密钥分配和密钥管理都十分困难。

2. 基于公钥体制的报文认证

基于公钥体制的报文认证主要利用数字签名技术和单向哈希函数技术实现。设 A 对报文 M 的哈希值 $H(M)$的签名为$\mathrm{SIG}_{S_A}(H(M))$，其中 S_A 为 A 的私钥。A 将 $M/\mathrm{SIG}_{S_A}(H(M))$发送给用户 B，B 通过 A 的公钥 P_A 可确认报文是由 A 所发出的，并且通过计算哈希值还可对报文 M 的完整性进行鉴别。在报文需要保密的情况下，A 可以使用 B 的公开密钥 K_{P_B} 对整个报文进行加密，然后 B 可以使用自己的秘密密钥 K_{S_B} 进行解密，如图 9.12 所示。

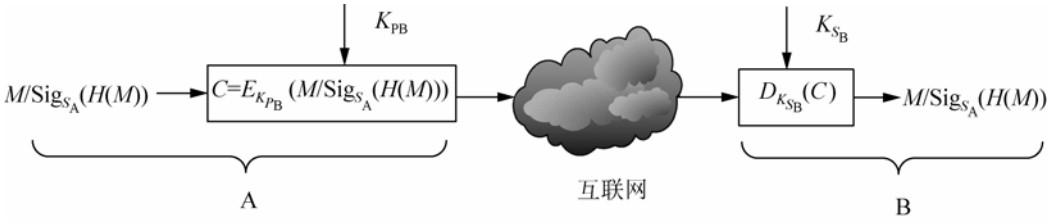


图 9.12　公开密钥报文认证

在公钥体制下，为检验报文的完整性，除利用哈希函数形成数字摘要的技术外，也可以采用传统的加入鉴别码的方法，即报文发送者在报文中加入一个报文认证码(MAC)或篡改检测码(MDC)，并经接收者的公开密钥加密后发送给接收者检验。接收者利用自己的秘密密钥进行解密，并经约定的算法对解密后的报文进行运算，将得到的鉴别码与收到的鉴别码进行比较，若二者相等，则可证实报文内容的真实性，否则拒绝接收。

9.4.3　CA 认证

在网上进行商务活动时，无论是数字证书的发放还是数字时间戳服务，都需要有一个具有权威性和公正性的第三方来完成。这种权威性和公正性的第三方就是证书授权(Certification Authority，CA)中心，又称认证中心。

认证中心作为受信任的第三方，需要承担网上安全电子交易的认证服务，主要负责产生、分配并管理用户的数字证书。它通过自身的注册审核体系，核实进行证书申请的用户身份和各项相关信息，使网上交易用户属性的客观真实性与证书的真实性一致。CA 中心对

网上交易活动中的数据加密、数据签名、数据完整性以及身份鉴别所需的密钥和认证实施统一的集中化管理，支持网上交易的参与者在网络环境下建立和维护平等的信任关系。CA中心为网上交易各方的信息安全提供有效的、可靠的保护机制。这些机制提供机密性、身份验证特性、不可否认性等。

认证中心作为一个权威、公正、可信的第三方机构，它的建设是电子商务最重要的基础建设之一，也是电子商务大规模发展的根本保证。最早的 CA 认证中心采用的就是由SETC0 公司建立的、以 SET 协议为基础的 SET CA 体系，这种体系只能服务于 B2C 电子商务模式中的卡支付应用。由于 B2B 电子商务模式的发展，要求 CA 的支付接口能够兼容支持 B2B 和 B2C 两种模式，即同时支持网上购物、网上银行、网上交易与供应链管理等职能，这样就产生了以通用公钥基础设施(PKI)为技术基础的 non-SET CA 体系，即 PKI 安全体系。

9.5 PKI 安全体系

本节从 PKI 的概念入手，分析 PKI 提供的核心服务、PKI 的基本职能以及必要的构成组件；讨论 PKI 系统中的实体模型，比较各种 PKI 系统中常用信任结构的特点和适用范围，并给出 PKI 的相关安全协议以及实现标准。

9.5.1 PKI 的定义

PKI(Public Key Infrastructure，公钥基础设施)是一个利用公钥密码技术在开放的 Internet 网络环境中提供数据加密以及数据签名服务的统一的技术框架。它由公开密钥密码技术、数字证书、证书权威机构(CA)和系统安全策略等基本部分组成，是一种验证持有密钥的用户身份的综合系统。从广义上讲，所有提供公钥加密和数字签名服务的系统，都可叫做 PKI 系统。

PKI 系统的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性、不可否认性。

PKI 基础设施是目前比较成熟、完善的 Internet 网络安全解决方案。它作为安全基础设施，能为不同的用户按不同安全需求提供多种安全服务。这些服务主要包括认证、数据完整性、数据保密性、不可否认性、公正及时间戳服务等。

9.5.2 PKI 的构成组件

PKI 是利用公钥技术实现电子商务安全的一种体系。它由公开密钥密码技术、数字证书、认证机构(CA)和关于公开密钥的安全策略等基本成分共同组成。从一般意义上讲，PKI 包含了安全认证系统和具体的应用系统。

一个典型、完整、有效的 PKI 应用系统应具有以下部分。

1. 认证机构

认证机构(Certificate Authority，CA)是 PKI 的核心，是数字证书的申请注册、签发和管理机构，通常称为认证中心。CA 负责管理 PKI 结构下的所有用户(包括各种应用程序)的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份。

2. 数字证书

数字证书是由具备权威性、可信任性和公正性的第三方机构签发的网上实体身份的证明。有时又称电子证书，通常符合 X.509 标准。

3. 证书库

证书库与网上“白页”类似，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。构造证书库的最佳方法是采用支持 LDAP 协议的目录系统，用户或相关的应用通过 LDAP 来访问证书库。系统必须确保证书库的完整性，防止伪造、篡改证书。

4. 密钥备份及恢复系统

若用户丢失了私钥，则密文数据将无法解密，造成数据丢失。为避免这种情况的出现，PKI 应该提供备份与恢复密钥的机制。密钥的备份与恢复应该由可信的机构来完成，一般由 CA 充当该角色。

5. 证书作废处理系统

证书作废处理系统是 PKI 的一个重要组件。同日常生活中的各种证件一样，证书在 CA 为其签署的有效期以内也可能需要作废。作废证书一般通过将证书列入作废证书表(CRL)来完成。通常，系统中由 CA 负责创建、更新及维护 CRL。

6. PKI 应用接口系统

PKI 应用接口系统主要功能是为所有应用对证书合法性验证、密钥备份与恢复、证书作废处理、交叉证书验证提供可信、透明、统一的支持。良好的应用接口系统，使得各种应用能够方便地使用加密、数字签名等安全服务并以安全、一致、可信的方式与 PKI 交互。通常应用接口系统应该是跨平台的。

完整的 PKI 还包括认证政策的制定(包括遵循的技术标准、各 CA 之间的上下级或同级关系、安全策略、安全程度、服务对象、管理原则和框架等)、认证规则、运作制度的制定、所涉及的各方法律关系内容以及技术的实现。

9.5.3 PKI 的实体模型

PKI 的标准之一 RFC 2510 定义的 PKI 实体模型如图 9.13 所示。从中可以看出 PKI 系统主要由 PKI 用户、PKI 管理实体、PKI 的证书及 CRL 库 3 部分构成。而 PKI 管理实体中的核心是 CA。

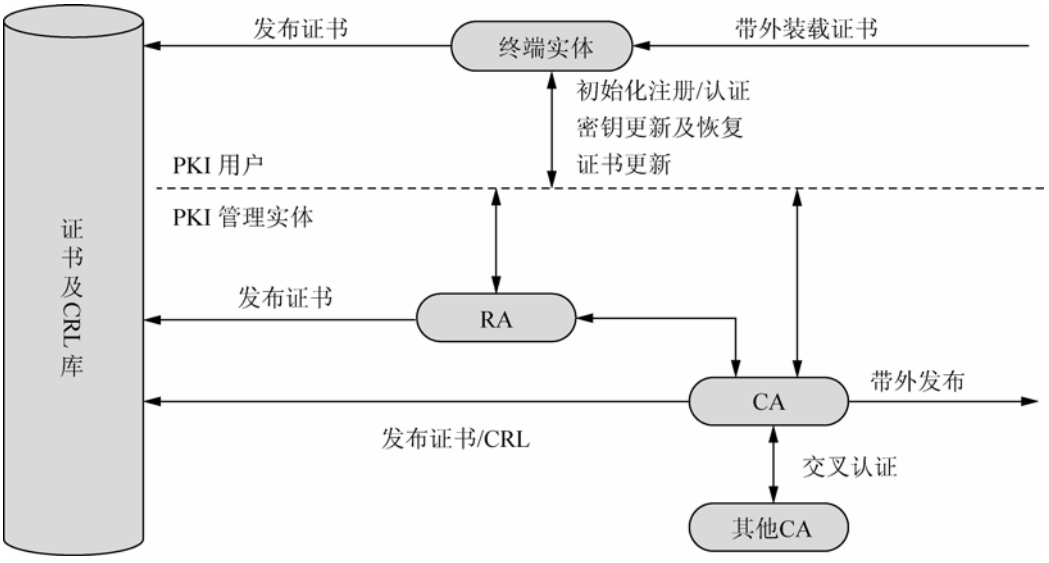


图 9.13　PKI 的实体模型

其中，终端实体是指 PKI 证书的用户和证书主体的终端用户系统。RA 是 CA 委派的承担某些管理功能的可选系统，通常称为注册机构。

9.5.4　PKI 的信任结构

PKI 的信任结构刻画 CA、证书主体和证书用户之间的信任关系，它是构成 PKI 结构和运作整体所必需的部分。PKI 信任结构的正确选择关系到整个 PKI 的安全。通常使用以下 4 种信任结构。

1. 认证机构的严格层次结构

这是 CA 层次结构中的常见模型。它像一棵倒转的树，根 CA 代表树根，它对整个 PKI 系统的实体都有意义。根 CA 下面的树枝状 CA 就代表根 CA 的子 CA，最下面的叶子节点代表终端实体。不同子 CA 颁发的证书之间不一定相互信任，但它们都信任同一个根 CA。这些 CA 都认证零个或多个直接在它下面的 CA。倒数第二层的 CA 认证终端实体。

2. 分布式信任结构

这种结构的区别在于有多个根 CA，但每个 CA 体系遵循严格层次结构。

3. 基于 Web 信任结构

在这种结构中，浏览器厂商起到根 CA 的作用，他们将一些 CA 的公钥预先装在浏览器上，如 IE、Netscape。这些 CA 就成为浏览器厂商的子 CA，其中有著名的全球最大的 CA 公司 Versign。

在这种用户中心信任结构中，每个用户都对决定信赖哪个证书和拒绝哪个证书直接完全地负责。

4. 交叉认证

交叉认证就是实现多个 PKI 域之间的互操作。交叉认证实现的方法有多种：一种方法是桥接 CA，即用一个第三方 CA 作为桥，将多个 CA 连接起来，成为一个可信任的统一体；另一种方法是多个 CA 的根 CA(RCA)互相签发根证书，这样当不同 PKI 域中的终端用户沿着不同的认证链检验认证到根时，就能达到互相信任的目的。

目前，国际上通常采用的是基于 Web 信任结构模型。在国内，还是以单一认证机构的严格层次模型为主。

本 章 小 结

网上交易主要是在网络的虚拟环境上进行的交易，利用电子商务的各种手段，达成从买到卖的虚拟交易过程。但是对于大部分人而言，可能都尚存一种顾虑。尤其是在国内，网上支付更是被很多人敬而远之，因为毕竟不是面对面交易。如何解决这些问题就成了困扰我国电子商务健康发展的障碍。

随着电子支付的蓬勃发展，网上安全支付越来越引起人们的重视。网上支付活动中的安全技术主要指密码技术和交易的安全机制。密码技术有对称密码技术、公钥密码技术、数字签名技术、Hash 函数、公钥认证技术、数字时间戳等。在一个加密系统中，信息使用加密密钥加密后，接收方使用解密密钥对密文解密得到原文。数字签名用来保证信息传输过程中信息的完整和提供信息发送者的身份认证。

认证技术分实体认证和信息认证。实体认证是对参与通信实体的身份认证，信息认证是指对信息体进行认证，以决定该信息的合法性。常用的认证技术有身份认证技术、报文认证技术、服务器认证技术等。CA 认证中心具有权威性、可信赖性及公正性，负责产生、分配和管理所有网上实体所需的数字证书，是安全网上支付的核心环节。

关键术语

对称密钥体制；公开密钥体制；数字签名；数字证书；身份认证技术；服务器认证技术

习　　题

一、选择题

1．DES 是(　　)。

A．Data Encryption Standard　　B．Data End System

C．Data Encryption System　　D．Data End Stardard

2．在采用 RSA 公开密钥加密系统中，若 A 想给 B 发送一封邮件，并且想让 B 知道邮

件是 A 发出的，则 A 应该选用的加密密钥是(　　)。

A．A 的公钥　　B．B 的公钥　　C．A 的私钥　　D．B 的私钥

3．非对称加密将密钥被分解为一对密钥，即(　　)。

A．一把公开的加密密钥和一把公开的解密密钥

B．一把秘密的加密密钥和一把公开的解密密钥

C．一把公开的加密密钥和一把秘密的解密密钥

D．一把公开密钥或加密密钥和一把专用密钥或解密密钥

4．加密技术是电子商务采取的主要安全措施之一，贸易方可根据需要在信息交换的过程中使用。所谓加密技术指的是(　　)。

A．将数据进行编码，使它成为一段数字字符

B．将数据进行编码，使它成为一种不可理解的形式

C．将数据进行编码，使它成为一段字母字符

D．将数据进行编码，使它成为一段看不见的字母、数字混合字符

5．密钥的长度是指密钥的位数，一般来说(　　)。

A．密钥位数越长，被破译的可能就越小

B．密钥位数越短，被破译的可能就越小

C．密钥位数越长，被破译的可能就越大

D．以上说法都正确

6．认证中心是检验公开密钥是否真实的第三方，它是一个权威机构，用来(　　)。

A．专门检验手续是否合法　　B．专门验证交易双方是否合法

C．专门检验商品质量　　D．专门验证交易双方的身份

7．SET 协议是实现在开放的 Internet 网络上使用付款卡(信用卡、借记卡和取款卡等)支付的安全事务处理协议。SET 协议的目的是为了(　　)。

A．安全地在网上使用现金支付

B．安全地在网上传递交易信息

C．安全地在网上使用订单进行交易

D．安全地在网上使用付款卡进行交易

8．数字签名用来保证信息传输过程中信息的完整和提供信息发送者的身份认证，数字签名采用的主要技术是(　　)。

A．对称密钥算法　　B．数据加密标准法

C．公开密钥算法　　D．以上说法都正确

二、简答题

1．简述网上支付可能存在的安全问题。

2．什么是对称密钥体制？对称密钥体制与公开密钥体制有何区别？

3．举例说明常用的公开密钥算法及其运用原理。

4．什么是数字证书？简述数字证书的组成部分。

5．简述数字签名的概念及其作用。

6．保障网上支付安全的技术有哪些？

7．什么是 CA 认证中心？简述其功能。
8．简述混合密钥加密技术的原理。
9．简述数字时间戳及其应用场合。
10．简述 RSA 算法的基本思想。
11．简述网上支付的安全需求所包括的内容。

案例分析

NPS 支付网关安全案例

在现代电子商务中，网上购物已成为时尚。深圳市全动科技有限公司开发的网上支付系统 NPS(Network Payment System)与全国各地多家银行(包括 VISA、Master、JCB 等)签订了网上支付合作协议，满足消费者在商城上购物时方便地选择银行进行支付，给消费者或商家等带来方便。

在网上交易过程中，消费者在商家的网站上挑选商品，放入购物车，然后进入结账页面，商户 Web 系统将要求用户输入送货地址、联系电话等信息。然后，商家 Web 系统根据购物车内容生成相应订单，订单一般包括：订单号、交易日期、货品数量和单价及总计价、送货地址、联系电话等，然后将订单通过加密发送到 NPS 支付通道，并选择所需的银行进行网上交易。

NPS 支付网关接收到从商家递交的订单支付请求，将订单号、商户名称、订单总金额等交易信息显示给消费者，消费者确认订单信息后，选择一家银行进行支付，NPS 将导航消费者到相应的银行网上支付页面，消费者在银行的网上支付页面使用银行卡进行支付。当消费者输入银行卡号密码后，银行 Web 系统发出支付命令，将相关信息返回 NPS。NPS 处理银行返回的信息后，再根据商家的需求进行实时的反馈，即将客户支付订单的交易结果反馈给商家，并通过页面返回给消费者。NPS 支付模型如图 9.14 所示。

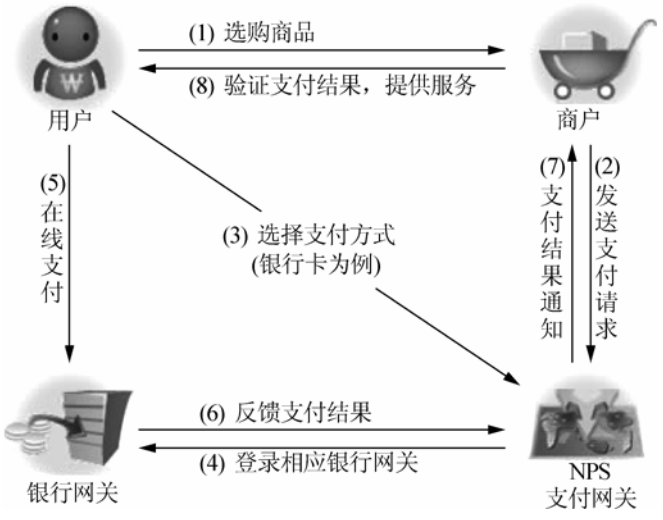


图 9.14　NPS 支付模型

消费者从商家网站上向 NPS 提交支付订单、发起交易时，采用了 128 位的 SSL(Secure Socket Layer)安全加密，SSL 是一种被广泛使用的 Internet 传输加密标准，客户端的浏览器发送网页请求时使用 HTTPS 协议，传输数据保证了信息安全。

NPS 支付通道服务器安装了服务器证书，增加了客户对 NPS 网站的信任感。当消费者在商城提交订单到 NPS 进行网上交易时，些时出现一个安全的提示，只要单击“确定”或“是”按钮，即可以对数据

进行加密。

NPS 接收到商家提交过来的支付请求后，验证商家的数字签名，校验加密数据；生成支付反馈结果信息时也采用数字签名和高强度加密算法进行数据加密，确保数据的安全。

订单支付成功实时反馈给商家，根据商家的需求，实时更新商家的数据库，并发 E-mail 通知商家，保证了支付结果反馈的准确性。

NPS 支付系统采用双机热备和异地灾备技术，保证了系统的运营平台的稳定性和永不停顿。

NPS 系统采用 Java 技术实现系统平台，系统运行稳定、安全、高效。

资料来源：深圳市全动科技有限公司网站(www.nps.cn)。

问题：研究上面的案例，讨论 NPS 支付网关的安全性是否足够。如果构建一个集团公司的电子商务部门(如网上销售系统)，有哪些可行的支付手段？如何在公司的网上销售系统中集成“NPS 支付网关”的支付方式，并保证交易的安全性？