Chapter
1

项目一

密码技术的应用

项目要点

- 网络安全
- 密码技术
- 利用密码技术进行 OpenSSH 安全认证

引 言

本项目主要介绍与密码算法相关的一些知识，包括基本概念和简单的实现方法，帮助读者了解几种常用的加密算法和技术：对称密码算法、公钥密码算法、数字签名技术、密钥管理等，掌握涉及密码系统的基本概念和原理，能够运用基本原理对实际问题进行分析。

任务：利用密码技术进行 OpenSSH 安全认证

任务描述

小张是某网络公司的业务人员，为了保证公司的客户资料等机密文件的安全性，小张决定进行加密设置。

任务分析

在计算机网络中，加密的方法有很多。其中 OpenSSH 技术具有安全性高、操作简单方便的特点，因此，小张决定通过实现 OpenSSH 安全认证来完成这项任务。

准备知识

1. 网络安全的概念

（1）概述

以 Internet 为代表的全球性信息化浪潮所带来的影响日益深刻，信息网络技术的应用日益普及，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型的、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。

知识链接

伴随网络的普及，安全日益成为影响网络效能的重要因素，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，也对安全提出了更高的要求，这主要表现在以下两个方面。

①开放性的网络，导致网络的技术是全开放的，任何组织和个人都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如，任何具有不良企图的黑客可以对物理传输线路实施攻击，也可以对网络通信协议实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。网络的国际化还意味着网络的攻击不仅仅来自本地网络用户，它可以来自 Internet 上的任何一台主机，也就是说，网络安全所面临的是一个国际化的挑战。

②自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而不受

任何约束。

开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革，使得人们能够利用 Internet 提高办事效率和市场反应能力，从而更具竞争力，同时人们又要面对网络开放所带来的数据安全的新挑战。如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必须考虑的事情之一。

1）网络安全的概念

网络安全包括 5 个要素：机密性、完整性、可用性、可控性和可审查性。机密性指确保信息不暴露给未授权的实体。完整性则意味着只有得到授权的实体才能修改数据，并且能够判别出数据是否已被篡改。可用性说明得到授权的实体在需要时可访问数据。可控性表示可以控制授权范围内的信息流向及行为方式。可审查性指对出现的网络安全问题提供调查的依据和手段。

网络安全的定义从狭义的保护角度来看，是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害，从广义来说，凡是涉及计算机网络上信息的机密性、完整性、可用性、可控性、可审查性的相关技术和理论都是计算机网络安全的研究领域。

2）网络安全的现状

现在全球普遍存在缺乏网络安全意识的状况。人们在组建一个网络的时候，并没有意识到网络安全的重要性。这导致大多数网络存在着先天性的安全漏洞和安全威胁。

国际上也存在着信息安全管理规范和标准不统一的问题。美国是西方国家中对信息安全着力较多的国家之一，同样存在着规范和标准跟不上技术进步发展的问题。西欧国家则另有一套信息安全标准，虽然在原理和结构上同美国有相同的部分，但是不同的部分也相当多。

知识链接

在信息安全的发展过程中，企业和政府的要求有一致的地方，也有不一致的地方。企业更注重于信息和网络安全的可靠性，政府更注重信息和网络安全的可管理性和可控制性。由美国政府组织的 KRS 系统，就是由于企业不欢迎而无法推广。在发展中国家，对信息安全的投入还满足不了信息安全的需求。

但不可忽视的现象是信息和安全的技术仍然在发展过程中。

同样在国内，网络安全产品的“假、大、空”现象在一定程度上普遍存在，防火墙变成了网络安全的全部。产生这种情况的原因是重技术、轻管理，以及网络安全知

识的普及程度不够所导致的。

（2）网络安全所面临的威胁

使用 TCP/IP 协议的网络所提供的网络服务都包含许多不安全的因素，存在着许多漏洞。同时，网络的普及使信息共享达到了一个新的层次，信息被暴露的机会大大增多。特别是 Internet 网络就是一个不设防的开放大系统。另外，数据处理的可访问性和资源共享的目的性之间是一对矛盾，这些都给网络带来了威胁。

1）网络中存在的威胁

目前网络中存在的威胁主要表现在以下几个方面。

①非授权访问。

没有预先经过同意就使用网络或计算机资源的情况被看作是非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。非授权访问主要包括以下几种形式：假冒，身份攻击，非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。

②泄漏或丢失信息。

泄漏或丢失信息指敏感数据被有意泄漏出去或丢失，通常包括信息在传输中丢失或泄漏（如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，得到用户密码、账号等重要信息），信息在存储介质中丢失或泄漏，敏感信息被隐蔽隧道窃取等。

③破坏数据完整性。

指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用等。

④拒绝服务攻击。

通过不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序响应来减慢甚至使网络服务瘫痪，影响正常用户的使用，导致合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务等。

⑤利用网络传播病毒。

通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

2）主机网络安全

由于主机安全和网络安全的技术手段难以有机地结合，因此容易被入侵者各个击破。并且由于它们在保护计算机和信息的安全上各自为政，因此很难解决系统安全性和使用方便性之间的矛盾。举一个简单的例子，从严密保护主机安全的角度来说应该禁止用户的远程登录，但是这给用户的使用将带来极大的不便，对 Internet 上绝大多

数 UNIX 主机来说是不可以接受的。而一旦允许用户远程登录，却无法区分用户的远程登录是合法的还是非法的，也就控制不了非法用户的入侵，并且系统一旦被入侵，入侵者就拥有合法用户的全部权力，危害极大。

知识链接

对于防火墙系统来说也有同样的问题，防火墙可以禁止外部主机对于内部主机的访问（安全但不方便），但是一旦允许用户经防火墙授权认证后进入内部主机，就无法控制其在内部主机上的行为（方便但不安全）。

为了解决这些问题，一种结合主机安全和网络安全的边缘安全技术开始兴起，这就是主机网络安全技术。主机网络安全技术是一种主动防御的安全技术，它结合网络访问的网络特性和操作系统特性来设置安全策略，用户可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行，以使同一用户在不同场所拥有不同的权限，从而保证合法用户的权限不被非法侵占。

知识链接

主机网络安全技术考虑的元素有 IP 地址、端口号、协议、MAC 地址等网络特性和用户、资源权限以及访问时间等操作系统特性，并通过对这些特性的综合考虑，来达到用户网络访问的细粒度控制。

与网络安全采用安全防火墙、安全路由器等在被保护主机之外的技术手段不同，主机网络安全所采用的技术手段通常在被保护的主机内实现，并且一般为软件形式。因为只有在被保护主机之上运行的软件，才能同时获得外部访问的网络特性以及所访问资源的操作系统特性。在当前广泛使用的计算机安全产品中，已经有一些软件在主机网络安全技术方面做了一些探索。

这类产品中，应用最为广泛的当属 Wietse Venema 开发的共享软件 TCP Wrapper。TCP Wrapper 是一种对进入的网络服务请求进行监视与过滤的工具，它可以截获 Systat、Finger、 FTP、Telnet、Rlogin、RSH、Exec、TFTP、Talk 等网络服务请求，并根据系统管理员设置的服务访问策略来禁止或允许服务请求。一般情况下，其策略主要考虑的是外部主机的域名（或 IP 地址）和请求的服务类型。通过扩充，还可以将请求访问的用户名和访问时间包括进来，即可以制定“在某时间允许 / 禁止某用户从外部某主机对某服务的访问”这样的策略。

另外，现在一些操作系统厂商已经或即将在操作系统中提供主机网络安全产品，

如 IBM 公司在 AIX4.3.1 中引入了强制访问控制、控制访问的多级目录管理，并可内置 Check Point 公司的 Firewall-1/VPN-14.0；SUN 公司即将发布的 Solaris 中也将引入公共密钥结构 (PKI）、基于 IP Security 的虚拟私有网络 (VPN）和内置的防火墙。

知识链接

上述这些措施都将极大地改善主机的网络安全状况。不过它们都是侧重于从访问的网络特性方面考虑，对于访问的操作系统特性考虑不够，因此对于冒充合法用户之类的攻击缺乏有效的办法。

3）主机网络安全系统体系结构

主机网络安全系统是为了解决主机安全性与访问方便性之间的矛盾，将用户访问时表现的网络特性和操作系统特性综合起来考虑，因此，这样的系统必须建立在被保护的主机上，并且贯穿于网络体系结构中的应用层、传输层、网络层之中。在不同的层次中，可以实现不同的安全策略，具体内容如下。

①应用层：是网络访问的网络特性和操作系统特性的最佳结合点。通过对主机所提供服务的应用协议的分析，可以知道网络访问的行为，并根据用户设置的策略判断在当前环境下是否允许该行为；另外，还要附加更严格的身份认证。

②传输层：是实现加密传输的首选层。对于使用了相同安全系统的主机之间的通信，可以实现透明的加密传输，而对于没有加密措施的通用客户软件之间的通信，仍可以使用不加密方式，并且加密与否对于用户来说是透明的。

③网络层：是实现访问控制的首选层。通过对 IP 地址、协议、端口号的识别，能方便地实现包过滤功能。

当然，更复杂的设计可以在更多的层实现更多的安全功能，下面就前面的设想提出一个可行的主机网络安全系统的结构模型，如图 1-1 所示。

在图 1-1 的结构模型中，安全检查承担了防火墙的任务，它对进出的数据包按照系统设置的安全规则进行过滤，另外，在该模块中还可以实现加密 / 解密。对用户的访问进行细粒度控制是主机网络安全系统最为重要的特点，它包括两个方面：内部资源访问控制和外部资源访问控制。

内部资源访问控制主要是对网络用户 (不管是合法用户还是入侵者) 的权限进行控制，对用户的权限进行细致的分类控制、跟踪并及时阻止非法行为，防止用户利用系统的安全漏洞进行攻击。内部资源访问控制根据系统资源控制文件 (全局作用) 和用户资源控制文件 (局部作用) 来控制用户的行为。例如，系统资源控制文件可以设置“如果网络用户获取到 ROOT 权限 (不管是使用系统命令获得还是利用系统漏洞取

得），则切断其连接”这样的规则，从而阻止入侵者获得超级权限后严重威胁系统安全。又如，用户资源控制文件可以设置“在某某时间某某地点（如日常工作场所）可以远程登录，其他情况下禁止远程登录”，这样的规则使用户既有系统之外的方便性又保证了系统的安全性。

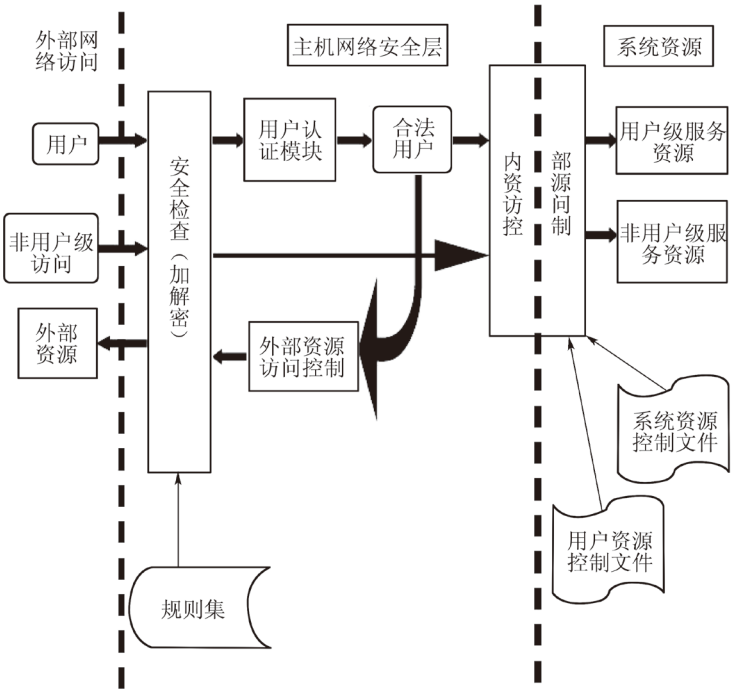

图 1-1 主机网络安全系统结构模型

知识链接

外部资源访问控制是控制用户对系统之外网络资源的访问，如阻止网络用户通过本主机远程登录外部主机，即不允许将本地主机当作跳板（这是黑客最常见的行为）。

（3）协议安全分析

计算机网络的运行机制基于网络协议，不同结点之间的信息交换按照事先约定的固定机制通过协议数据单元来完成。目前，TCP/IP 协议在 Internet 上一统天下。正是由于它的广泛使用性，使得 TCP/IP 的任何安全漏洞都会产生巨大的影响。TCP/IP 协议在设计初期并没有考虑到安全性问题，而是注重异构网的互联，而且用户和网络管理员没有足够的精力专注于网络安全控制，再加上操作系统越来越复杂，开发人员不

可能测试出所有的安全漏洞，连接到网络上的计算机系统就可能受到外界的恶意攻击和窃取。

1）物理层安全

物理层安全威胁主要指网络周边环境和物理特性引起的网络设备和线路的不可用而造成的网络系统的不可用，如设备老化、设备被盗、意外故障、设备损毁等。由于以太局域网中采用广播方式，因此，在某个广播域中利用嗅探器可以在设定的侦听端口侦听到所有的信息包，并且对信息包进行分析，那么本广播域的信息传递都会暴露无遗，所以需将两个网络从物理上隔断，同时保证在逻辑上两个网络能够连通。

2）网络层安全

网络层的安全威胁主要有两类：IP 欺骗和 ICMP 攻击。

IP 欺骗技术的一种实现方法是把源 IP 地址改成一个错误的 IP 地址，而接收主机不能判断源 IP 地址的正确性，由此形成欺骗。另外一种方法是利用源路由 IP 数据包，让它仅仅被用于一个特殊的路径中传输，这种数据包被用于攻击防火墙。

ICMP(Internet 控制信息协议）在 IP 层检查错误和其他条件。ICMP 信息对于判断网络状况非常有用，例如，当 Ping 一台主机想看它是否运行时，就产生了一条 ICMP 信息。

知识链接

远程主机将用它自己的 ICMP 信息对 Ping 请求做出回应，这种过程在网络中普遍存在。然而，ICMP 信息能够被用于攻击远程网络或主机，利用 ICMP 来消耗带宽从而有效地摧毁站点。

3）传输层安全

具体的传输层安全措施要取决于具体的协议。TLS(传输层安全）协议在 TCP 的顶部提供了如身份验证、完整性检验以及机密性保证这样的安全服务。TLS 需要为一个连接维持相应的场景，它是基于可靠的传输协议 TCP 的。由于安全机制与特定的传输协议有关，所以像密钥管理这样的安全服务可为每种传输协议重复使用。

在 Internet 中提供安全服务的一个最初想法便是强化它的 IPC(广义的进程间通信）界面，具体做法包括双端实体的认证，数据加密密钥的交换等。Netscape 通信公司遵循了这个思路，制定了建立在可靠的传输服务基础上的安全套接层协议 (SSL）。SSL 版本 3(SSL v3）主要包含以下两个协议：SSL 记录协议和 SSL 握手协议。

4）应用层安全

现在，应用层安全已经被分解成网络层、操作系统、数据库的安全，由于应用系

统复杂多样，不存在一种安全技术能够完全解决一些特殊应用系统的安全问题。但对一些通用的应用程序，如 Web Server 程序、FTP 服务程序、E-mail 服务程序、浏览器、MS Office 办公软件等，可以通过互联网扫描服务和系统扫描服务检查应用程序自身的安全漏洞和由于配置不当造成的安全漏洞，在最大程度上避免安全隐患。

（4）网络安全标准

针对日益严峻的网络安全形势，许多国家和标准化组织纷纷出台了相关的安全标准，我们国家也制定了相应的安全标准，这些标准既有很多相同的部分，也有各自的特点。其中以美国国防部制定的可信计算机安全标准（TCSEC）应用最为广泛。

1）国外网络安全标准与政策现状

国际性的标准化组织主要有国际标准化组织（ISO）、国际电器技术委员会（IEC）及国际电信联盟（ITU）所属的电信标准化组织（ITU-TS）。ISO 是总体标准化组织，而 IEC 在电工与电子技术领域里相当于 ISO 的位置。1987 年，ISO 的 TC97 和 IEC 的 TCs47B/83 合并成为 ISO/IEU 联合技术委员会（JTC1）。ITU-TS 是联合缔约组织。

知识链接

这些组织在安全需求服务分析指导、安全技术研制开发、安全评估标准等方面制定了一些标准草案，但尚未正式执行。另外还有众多的标准化组织也制定了不少安全标准，如 IETF 就有 9 个功能组：认证防火墙测试组 (AFT)、公共认证技术组 (CAT)、域名安全组 (DNSSEC)、IP 安全协议组 (IPSEC)、一次性密码认证组 (OTP)、公开密钥结构组 (PKIX)、安全界面组 (SECSH)、简单公开密钥结构组 (SPKI)、传输层安全组 (TLS) 和 Web 安全组 (WTS) 等。

①美国 TCSEC(桔皮书)。

该标准是美国国防部制定的。它将安全分为 4 个方面：安全政策、可说明性、安全保障和文档。这 4 个方面又分为 7 个安全级别，从低到高依次为 D1、C1、C2、B1、B2、B3 和 A1 级。

②欧洲 ITSEC。

ITSEC 与 TCSEC 不同，它并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。ITSEC 定义了从 E0 级 (不满足品质) 到 E6 级 (形式化验证) 的 7 个安全等级，对于每个系统，安全功能可分别定义。ITSEC 预定义了 10 种功能，其中前 5 种与桔皮书中的 C1 ~ B3 级非常相似。

③加拿大 CTCPEC。

该标准将安全需求分为 4 个层次：机密性、完整性、可靠性和可说明性。

④美国联邦准则（FC）。

该标准参照了 CTCPEC 及 TCSEC，其目的是提供 TCSEC 的升级版本，同时保护已有投资。FC 是一个过渡标准，后来结合 ITSEC 发展为联合通用准则。

⑤联合通用准则（CC）。

CC 的目的是把已有的安全准则结合成一个统一的标准。该项计划从 1993 年开始执行，1996 年推出第一版，但目前仍未付诸实施。CC 结合了 FC 及 ITSEC 的主要特征，它强调将安全的功能与保障分离，并将功能需求分为 9 类 63 族，将保障分为 7 类 29 族。

⑥ ISO 安全体系结构标准。

在安全体系结构方面，ISO 制定了国际标准 ISO7498-1-1989《信息处理系统—开放系统互连—基本模型—第 2 部分：安全体系结构》。该标准为开放系统标准建立了一个框架。其任务是提供安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

知识链接

近 20 年来，人们一直在努力发展安全标准，并将安全功能与安全保障分离，制定了复杂而详细的条款。但真正实用、在实践中相对易于掌握的还是 TCSEC 及其改进版本。在现实中，安全技术人员也一直将 TCSEC 的 7 级安全划分当作默认标准。

2）ISO7498-2 安全标准。

ISO7498 从体系结构的角度描述了 ISO 基本参考模型之间的安全通信必须提供的安全服务及安全机制，并说明了安全服务及其相应机制在安全体系结构中的关系，从而建立了开放互连系统的安全体系结构框架。

ISO7498-2 提供了以下 5 种可选择的安全服务。

①身份认证。

身份认证是访问控制的基础。身份认证必须做到准确无误地将对方辨别出来，同时还应该提供双向的认证，即互相证明自己的身份。网络环境下的身份认证更加复杂，主要是要考虑到验证身份的双方一般都是通过网络交互而非直接交互，像指纹认证等手段就无法应用。同时大量的黑客随时都可能尝试向网络渗透，截获合法用户密码冒名顶替，因此必须利用高强度的密码技术来进行身份认证，比较著名的有 KERTESOS、PGP 等方法。

②访问控制。

访问控制是控制不同用户对信息资源的访问权限，对访问控制的要求主要有以下

几方面。

- 一致性，也就是对信息资源的控制没有二义性，各种定义之间不冲突。
- 统一性，对所有信息资源进行集中管理，安全政策统一贯彻。
- 审计功能，对所有授权有记录并可以核查。
- 尽可能地提供细粒度的控制。目前很多系统的访问控制实际上还是基于 UNIX 文件系统的模式，不能很好地满足安全需求。

③数据加密。

数据加密是大家所熟知的保证安全通信的手段。由于计算机技术的发展，传统通信加密算法被不断破译，促使更高强度的加密算法问世。目前加密技术主要有两大类：一类是基于对称密钥加密的算法，也称私钥算法；另一类是基于非对称密钥的加密算法，也称公钥算法。这两种加密算法都已经达到一个很高的强度。

拓展提高

具体到加密手段，一般分软件加密和硬件加密两种，软件加密成本低而且实用灵活，更换也方便；硬件加密效率高，本身安全性高。用户可以根据不同需要采用不同的方法。密钥管理包括密钥产生、分发、更换等，是数据保密的重要一环。目前如何实现密钥完全自动管理还有待于进一步研究。

④数据完整性。

数据完整性是指信息在存储、传输和使用中不被篡改和泄密。显然，金融信息网络传输的信息对传输、存储和使用的完整性要求很高，需采用相应的安全措施来保障数据的传输安全，以防被篡改或泄密。

⑤防止抵赖。

接收方要对方保证自己收到的信息是发送方发出的信息而不是被中间人冒名、篡改过的信息。发送方要求对方不能否认已经收到的信息。对金融电子化系统来说，电子签名的主要目的就是防止抵赖，给仲裁提供证据。

3）BS7799(ISO17799：2000）标准

ISO17799 于 2000 年 12 月出版，它适用于所有的组织，目前已成为强制性的安全标准。ISO17799 是一个详细的安全标准，包括安全内容的所有准则，具体由 10 个独立的部分组成，其中每一部分都覆盖不同的主题和区域。

①信息安全方针。

为信息安全提供管理方向和支持。

②组织安全。

建立组织内的信息安全管理体系，以便实施安全管理。

③财产分类和控制。

维护组织资产的适当保护系统。

④人员安全。

减少误操作、入侵、盗用等人为造成的风险。

⑤物理和环境安全。

防止电子商务和信息的未经许可的介入、损伤和干扰。

⑥计算机通信和操作管理。

保证通信和操作设备的正确使用和安全维护。

⑦访问控制。

控制对信息的访问。

⑧系统开发与维护。

保证在信息系统中建立安全设置。

⑨商务持续性管理。

防止商务活动中断及保护关键商务过程不受重大失误或灾难事故的影响。

⑩符合性。

避免任何违反法令、法规、合同约定及其他安全要求的行为。

4）国内安全标准、政策制定和实施情况

①身份认证。

身份认证主要是通过标识和鉴别用户的身份，防止攻击者假冒合法用户获取访问权限。就金融信息网络而言，主要考虑用户、主机和节点的身份认证。

②访问控制。

访问控制根据主体和客体之间的访问授权关系，对访问过程做出限制，可分为自主访问控制和强制访问控制。自主访问控制主要基于主体的活动，实施用户权限管理、访问属性（读、写及执行）管理等。

拓展提高

强制访问控制则强调对每一主、客体进行密级划分，并采用敏感标识来标识主、客体的密级。就金融信息网络安全要求而言，应采用自主访问控制策略。

③数据完整性。

数据完整性是指信息在存储、传输和使用中不被篡改和泄密。显然，金融信息网络传输的信息对传输、存储和使用的完整性要求很高，需采用相应的安全措施来保障数据的传输安全，以防篡改和泄密。

④安全审计。

审计是通过对网络上发生的各种访问情况记录日志，并对日志进行统计分析，从而对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。在存储和使用安全建设中，审计的主要对象为用户、主机和节点，主要内容为访问的主体、客体时间和成败情况等。

⑤隐蔽信道分析。

隐蔽信道是指以危害网络安全策略的方式传输信息的通信信道。隐蔽信道是网络遭受攻击的主要原因之一。目前主要采用安全监控和安全漏洞检测来加强对隐蔽信道的防范，在必要的网络接口安装安全监控系统，同时定期对网络进行安全扫描和检测。

（5）网络安全组件

网络的整体安全是由安全的操作系统、应用系统、防火墙、网络监控、安全扫描、信息审计、通信加密、灾难恢复、网络反病毒等多个安全组件共同组成的，每一个单独的组件只能完成其中部分功能，而不能完成全部功能。

1）防火墙

防火墙是指在两个网络之间加强访问控制的一整套装置，是软件和硬件的组合体，通常被比喻为网络安全的大门，用来鉴别什么样的数据包可以进出企业内部网。防火墙在内部网（可信任的）和外部网（不可信任的）之间构造一个保护层。

拓展提高

防火墙可以阻止基于 IP 包头的攻击和非信任地址的访问，但无法阻止基于数据内容的黑客攻击和病毒入侵，同时也无法控制内部网络之间的攻击行为。

2）扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以自动发现系统的安全缺陷。扫描器可以分为主机扫描器和网络扫描器。但是，扫描器无法发现正在进行的入侵行为，而且它也可以被攻击者加以利用。

3）防毒软件

防毒软件可以实时检测、清除各种已知病毒，具有一定的对未知病毒的预测能力，利用代码分析等手段能够检查出最新病毒。在应对网络入侵方面，它可以查杀特洛伊木马和蠕虫等病毒程序，但不能有效阻止基于网络的攻击行为。

4）安全审计系统

安全审计系统对网络行为和主机操作提供全面翔实的记录，其目的是测试安全策略是否完善，证实安全策略的一致性，方便用户分析与审查事故原因，协助对攻击的分析，收集证据以用于起诉攻击者。

前 4 种安全组件对正在进行的外部入侵和网络内部攻击缺乏检测和实时响应功能。

而所有这些缺点在 IDS 上得到了圆满的解决。

5）IDS

由于防火墙所暴露出来的不足和弱点，引发了人们对 IDS（入侵检测系统）技术的研究和开发。它被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

① IDS 的主要功能。

- 监控、分析用户和系统的活动。
- 核查系统配置和漏洞。
- 评估关键系统和数据文件的完整性。
- 识别攻击的活动模式，并向网管人员报警。
- 对异常活动的统计分析。
- 操作系统审计跟踪管理，识别违反政策的用户活动。
- 评估重要系统和数据文件的完整性。

② IDS 可分为主机型和网络型两种。

主机型入侵检测系统（Host Intrusion Detection System，HIDS）主要用于保护运行关键应用的服务器，它通过监视与分析主机的审计记录和日志文件来检测入侵。

HIDS 的优点如下：

- 确定攻击是否成功。
- 监控粒度更细。
- 配置灵活。
- 可用于加密和交换的环境。
- 对网络流量不敏感。
- 不需要额外的硬件。

HIDS 的缺点如下：

- 占用主机资源，在服务器上产生额外负载。
- 缺乏平台支持，可移植性差。

拓展提高

网络入侵检测系统（Network Intrusion Detection System，NIDS）主要用于实时监控网络关键路径信息，它通过侦听网络上的所有分组来采集数据，分析可疑现象。NIDS 通常利用一个运行在混杂模式下的网络适配器来实时监视并分析通过网络的所有通信业务。

NIDS 的优点如下：

- 监测速度快。

- 隐蔽性好。
- 视野更宽。
- 较少的监测器。
- 攻击者不易转移证据。
- 操作系统无关性。
- 可以配置在专用机器上，不占用额外资源。

NIDS 的缺点如下：

- 只能监视本网段的活动，精确度不高。
- 在交换环境下难以配置。
- 防入侵欺骗的能力较差。
- 难以定位入侵者。

综观上述网络安全组件的特点，我们可以得出这样一个结论：由于每个网络安全组件自身的限制，不可能把入侵检测和防护做到一应俱全。所以不能指望通过使用某一种网络安全产品实现绝对的安全。只有根据具体的网络环境，有机整合这些网络安全组件才能最大限度地满足用户的安全需求。

（6）安全策略的制定与实施

安全的基石是社会法律、法规，即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。各网络使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

1）安全工作目的

安全工作的目的就是在法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，达到以下目的：

①使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。

②使用授权机制，实现对用户的权限控制，同时结合内容审计机制，实现对网络资源及信息的可控性。

③使用加密机制，确保信息不暴露给未授权的实体或进程，从而实现信息的保密性。

④使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，从而确保信息的完整性。

⑤使用审计、监控、防抵赖等安全机制，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

2）安全策略

安全策略是指在某个特定的环境中，为达到一定级别的安全保护需求所必须遵守的诸多规则和条例。安全策略包括 3 个重要组成部分：安全立法、安全管理、安全技术。

拓展提高

安全立法是第一层，有关网络安全的法律法规可以分为社会规范和技术规范；安全管理是第二层，主要指一般的行政管理措施；安全技术是第三层，它是网络安全的物质技术基础。

3）安全策略的实施

①重要的商务信息和软件的备份应当存储在受保护、受限制访问且距离资料地点足够远的地方，这样备份数据就能逃脱本地的灾害。因此需要将关键的生产数据安全地存储在相应的位置。

这一策略要求将最新的备份介质存放在距离资料地较远的地方。同样，规定只有被授权的人才有权限访问存放在远程的备份文件。在某些情况下，为了确保只有被授权的人可以访问备份文件中的信息，需要对备份文件进行加密。

②需要给网络环境中系统软件打上最新的补丁。各公司的联网系统应当具备一套可供全体员工使用的方法，以方便定期检查最新的系统软件补丁、漏洞修复程序和升级版本。当需要时，此方法必须能够为连接 Internet 和其他公用网络的计算机迅速安装这些新的补丁、漏洞修复程序和升级版本。

此策略的目的是确保系统管理员和其他用户快速更新、升级连接 Internet 等公用网的计算机的系统软件。如果系统软件更新不及时，入侵者可能运行漏洞识别软件判断系统是否存在已知漏洞。这意味着恐怖分子、黑客、工业间谍和其他图谋不轨的人可以利用计算机识别可以进行破坏的系统。

拓展提高

如果与网络连接的系统没有安装带有安全性漏洞的修复程序、安全补丁和更新的软件，短时间内这些系统的漏洞就会被识别并被渗透。在未来几年，借助一些分布在系统中的自动执行软件，这一方法的执行将逐渐不需要人工干预。

③安装入侵检测系统并实施监视。为了让企业能快速响应攻击，所有与 Internet 连接的、设置多用户的计算机必须运行一套信息安全部门认可的入侵检测系统。

入侵检测系统不同于漏洞识别系统，前者在防御措施遭受破坏时向工作人员发出警报，后者是告诉工作人员有哪些漏洞需要修复以支撑防御系统。通常入侵检测系统会通过一个网络管理系统或其他通知手段实时向负责人员报警并采取应对措施。例如，计算机紧急响应小组 (CERT) 的成员可根据入侵检测系统的 BP 机报警采取行

动。这一策略的目的是确保内部网络外围设备上的所有系统都具备适当的入侵检测系统。

④启动最小级别的系统事件日志。计算机系统在处理一些敏感、有价值或关键的信息时必须可靠地记录下重要的、与安全有关的事件。与安全有关的事件包括：企业猜测密码、使用未经授权的权限、修改应用软件以及系统软件。

此策略可为所有生产系统采用，而不只是那些需要处理敏感的价值高的或关键信息的系统。不管怎样，企业实施此策略可确保此类日志被记录下来，并在一段时期内保存在一个安全的地方。在许多情况下会运用哈希算法或数字签名来判断系统日志记录之后是否被改变过。

2. 密码技术

（1）对称密码体制

密码技术是信息交换安全的基础，通过数据加密、消息摘要、数字签名及密钥交换等技术实现了数据机密性、数据完整性、不可否认性和用户身份真实性等安全机制，从而保证了网络环境中信息传输和交换的安全。密码技术大致可以分为 3 类：对称密钥算法、非对称密钥算法和单向散列函数。

单向散列函数的特点是加密数据时不需要密钥，并且经加密的数据无法解密还原，只有使用同样的单向加密算法对同样的数据进行加密，才能得到相同的结果。单向散列函数主要用于提供信息交换时的完整性，以验证数据在传输过程中是否被篡改。由于单向散列函数计算量大，通常只适合于加密短数据，如计算机系统中的密码、数据检验和等。现行的单向加密算法有 MD5、MD2 和 SHA 等算法。

拓展提高

在对称密码（也称单钥密码）算法中，使用单一密钥来加密和解密数据，典型的对称密钥算法是 DES、IDEA 和 RC 等算法。这种密码算法的特点是计算量小、加密效率高，但在分布式系统中应用时则存在着密钥交换和管理问题。

1）对称加密体制的概念

对称密码算法是指加密和解密数据使用同一个密钥，即加密和解密的密钥是对称的，这种密码系统也称为单密钥密码系统。图 1-2 表示了对称密钥算法的基本原理。

原始数据（即明文）经过对称加密算法处理后，变成了不可读的密文（即乱码）。如果想解读原文，则需要使用同样的密码算法和密钥来解密，即信息的加密和解密使用同样的算法和密钥。

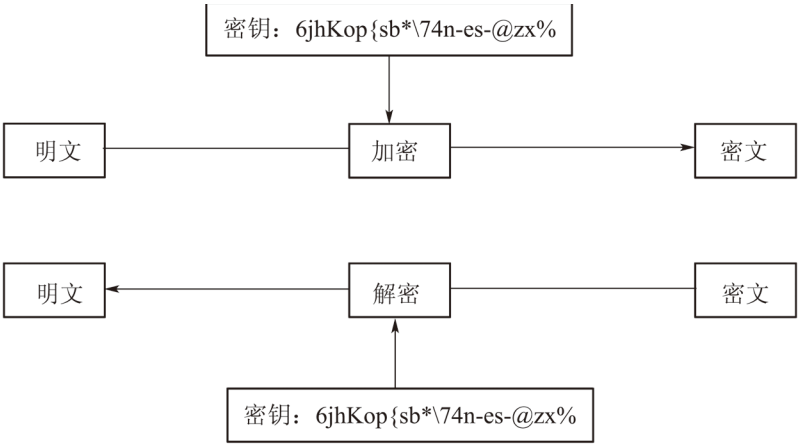

图 1-2　对称密码算法的基本原理

拓展提高

对称密码算法的优点是计算量小、加密速度快，缺点是加密和解密使用同一个密钥，容易产生发送者或接收者单方面密钥泄露问题，并且在网络环境下应用时必须使用另外的安全信道来传输密钥，否则容易被第三方截获，造成信息失密。

在数据加密系统中，使用最多的对称密码算法是 DES 及 3DES。在个别系统中也有使用 IDEA、RC 以及其他算法的，接下来具体介绍 DES 算法。

2）DES 算法

DES 算法最初是由 IBM 公司在 1970 年左右开发，1977 年被美国选为国家标准。以前，美国政府每隔几年就对 DES 算法重新做一次证明，但 1988 年，美国政府宣布不再证明 DES 了。对于 DES 一直有许多争论，最大的问题是它可能有一个未知的弱点，或者是只为 NSA(美国国家安全局) 所掌握的弱点。原来 DES 建议的密钥长度为 64 位，但在被批准成为标准前减少为 56 位，于是有人认为减少密钥长度使得美国政府可以使用 NSA 功能强大的计算机系统破译密码。现在，56 位密钥空间的 DES 算法已经被认为是经不起攻击的了。

图 1-3 描述了 DES 算法的工作原理。基本上，DES 算法所做的就是 16 次的迭代，把各块明文交织起来并与从密钥中获得的值混合，下面以 56 位的 DES 算法为例，简要介绍 DES 算法的整个工作流程。

- 在图 1-2 的左边，64 位的明文被修改 (排列) 以改变位的次序。
- 把明文分成两个 32 位的块。
- 在图中的密码一侧，原始密钥被分成两半。
- 密钥的每一半向左循环移位，然后重新合并、排列，并扩展到 48 位，分开的

密钥仍然保存起来供以后的迭代使用。

- 在图中的明文一边，右侧 32 位块被扩展到 48 位，以便与 48 位的密钥进行异或 (XOR) 操作，在这一步后还要进行另外一次排列。
- 把第 3 步和第 5 步的结果 (明文与密钥) 进行 XOR 操作。
- 使用置换函数把第 6 步的结果置换成 32 位。
- 把第 2 步创建的 64 位值的左边一半与第 7 步的结果进行 XOR 操作。
- 把第 8 步的结果和第 2 步创建的块的右半部分共同组成一个新块，前者在右边，后者在左边。
- 从第 4 步开始重复这个过程，迭代 15 次。
- 完成最后一次迭代后，对这个 64 位块进行一次翻转，得到一个 64 位的密文。
- 对原始明文中的下一个 64 位块重复整个过程，直到把原始消息加密完毕。

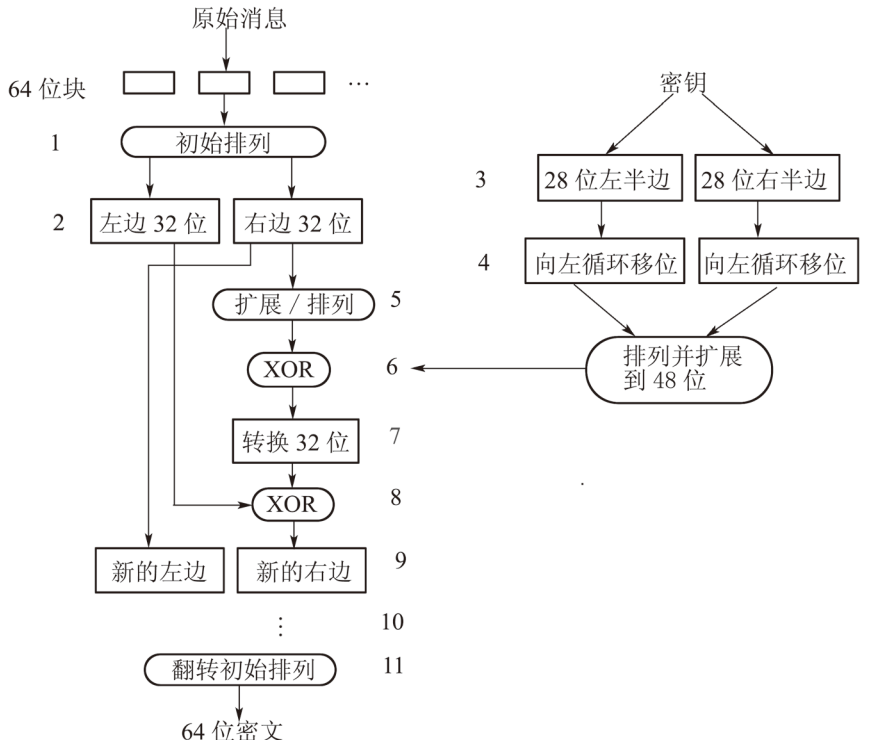

图 1-3 DES 算法的工作流程

3) DES 算法实现

根据以上对算法的描述，下面给出 DES 算法的具体实现过程。

①变换密钥，取得 64 位的密钥，其中第 8 位作为奇偶校验位。

②舍弃 64 位密钥中的奇偶校验位，根据以下数组 1-1(PC-1) 进行密钥变换，得到 56 位的密钥，在变换中，奇偶校验位可以被舍弃。

数组 1–1 变换选择 (PC–1)

57 49 41 33 25 17 9
1 58 50 42 34 26 18
10 2 59 51 43 35 27
19 11 3 60 52 44 36
63 55 47 39 31 23 15
7 62 54 46 38 30 22
14 6 61 53 45 37 29
21 13 5 28 20 12 4

③将变换后的密钥分为两个部分，开始的 28 位称为 C[0]，最后的 28 位称为 D[0]。

④生成 16 个子密钥，初始 I=1。

⑤同时将 C[I]、D[I] 左移 1 位或 2 位，根据 I 值决定左移的位数。

I：1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

左移位数：1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1

⑥将 C[I]D[I] 作为一个整体按以下数组 1–2(PC–2) 变换，得到 48 位的 K[I]。

数组 1–2 变换选择 2 (PC–2)

14 17 11 24 1 5
3 28 15 6 21 10
23 19 12 4 26 8
16 7 27 20 13 2
41 52 31 37 47 55
30 40 51 45 33 48
44 49 39 56 34 53
46 42 50 36 29 32

⑦从⑤处循环执行，直到 K[16] 被计算完成。

⑧处理 64 位的数据。

a. 取得 64 位的数据，如果数据长度不足 64 位，应该将其扩展为 64 位 (例如补零)。

b. 将 64 位数据按以下数组 1–3 变换 (IP)。

数组 1–3 初始变换 (IP)

58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6

64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7

⑨将变换后的数据分为两部分，开始的 32 位称为 L[0]，最后的 32 位称为 R[0]。

⑩用 16 个子密钥加密数据，初始 I=1。

a. 将 32 位的 R[I−1] 按数组 1−4 扩展为 48 位的 E[I−1]。

数组 1−4 扩展 (E)

32 1 2 3 4 5
4 5 6 7 8 9
8 9 10 11 12 13
12 13 14 15 16 17
16 17 18 19 20 21
20 21 22 23 24 25
24 25 26 27 28 29
28 29 30 31 32 1

b. 异或 E[I−1] 和 K[I]，即 E[I−1] XOR K[I]。

c. 将异或后的结果分为 8 个 6 位长的部分，第 1 位到第 6 位称为 B[1]，第 7 位到第 12 位称为 B[2]，依此类推，第 43 位到第 48 位称为 B[8]。

d. 按 S 表变换所有的 B[J]，初始 J=1。所有在 S 表的值都被当作 4 位长度处理。

ⓐ将 B[J] 的第 1 位和第 6 位组合为一个 2 位长度的变量 M，M 作为在 S[J] 中的行号。

ⓑ将 B[J] 的第 2 位到第 5 位组合，作为一个 4 位长度的变量 N，N 作为在 S[J] 中的列号。

ⓒ用 S[J][M][N] 来取代 B[J]。

数组 1−5 替换盒 1 (S[1])

14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8
4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

S[2]

15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10
3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5

0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15
13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9

S[3]

10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8
13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1
13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7
1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12

S[4]

7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9
10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

S[5]

2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9
14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6
4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14
11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3

S[6]

12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11
10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8
9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

S[7]

4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1
13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6
1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2
6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12

S[8]

13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7
1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2
7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8
2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11

ⓓ从ⓐ处循环执行，直到 B[8] 被替代完成。

ⓔ将 B[1] 到 B[8] 组合，按以下数组 1–6(P) 变换，得到 P。

数组 1–6 变换 P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

e. 异或 P 和 L[I−1]，并把结果放在 R[I]，即 R[I]=PXOR L[I−1]。

f. L[I]=R[I−1]。

g. 从 a. 处开始循环执行，直到 K[16] 被变换完成。

组合变换后的 R[16]L[16](注意：R 作为开始的 32 位)，按以下数组 1–7(IP–1) 变换得到最后的结果。

数组 1–7 最后变换 (IP–1)

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

以上就是对 DES 算法的描述。

（2）公钥密码体制

在非对称密钥算法中，使用两个密钥 (即公钥和私钥) 分别加密和解密数据，特别适合网络安全基础教程与实训在分布式系统中应用。当两个用户进行加密通讯时，发送方使用接收方的公钥加密所发送的数据；接收方则使用自己的私钥解密所接收的数据。由于私钥不在网上传送，比较容易解决密钥管理问题，消除了在网上交换密钥所带来的安全隐患。典型的非对称密钥算法是 RSA 算法。非对称密钥算法的缺点是计算量大、速度慢，不适合加密长数据。

1）公钥密码体制的概念

非对称密钥算法是指加密和解密数据使用两个不同的密钥，即加密和解密的密钥是不对称的，这种密码系统也称为公钥密码系统 (PKC，Pubilic Key Cryptosystem）。公钥密码学的概念首先是由 Diffie 和 Hellman 两个人在 1976 年发表的一篇名为《密码学的新方向》的著名论文中提出的，并引起很大的轰动。该论文曾获得 IEEE 信息论学会的最佳论文奖。

拓展提高

与对称密钥算法不同的是，非对称密钥算法将随机产生两个密钥：一个用于加密明文，其密钥是公开的，称为公钥；另外一个用来解密密文，其密钥是秘密的，称为私钥。

图 1-4 所示为非对称密码算法的基本原理。

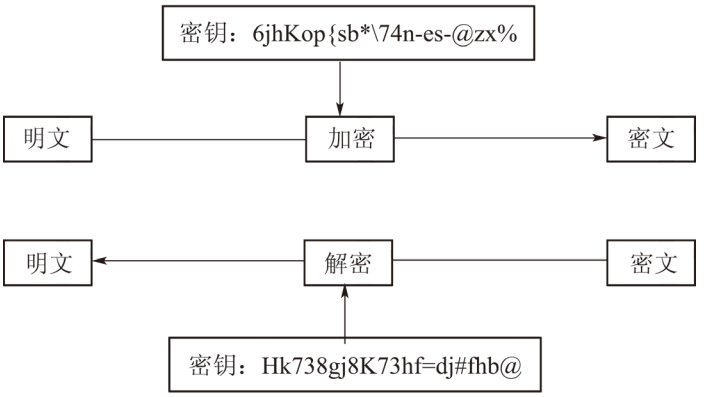

图 1-4　非对称（公钥）密码算法基本原理

如果两个人使用非对称密钥算法传输机密信息，则发送者首先要获得接收者的公钥，并使用接收者的公钥加密原文，然后将密文传输给接收者。接收者使用自己的私钥才能解密密文。由于加密密钥是公开的，不需要建立额外的安全信道来分发密钥，而解密密钥是由用户自己保管的，与对方无关，从而避免了在对称密码系统中容易产生的任何一方单方面密钥泄露问题，以及分发密钥时的不安全因素和额外的开销。非对称密钥算法的特点是安全性高、密钥易于管理，缺点是计算量大、加密和解密速度慢。因此，非对称密钥算法比较适合于加密短信息。在实际应用中，通常采用由非对称密钥算法和对称密钥算法构成混合密码系统，发挥各自的优势。使用对称密钥算法来加密数据，加密速度快；使用非对称密钥算法来加密对称密码算法的密钥，形成高安全性的密钥分发信道，同时还可以用来实现数字签名和身份验证机制。

非对称密钥算法除了用于加密数据外，还可以用于数字签名。数字签名主要提供信息交换时的不可否认性，公钥和私钥的使用方式与数据加密恰好相反。当两个用户

进行通信时，发送方首先使用自己的私钥来加密某些特征信息（即数字签名），表明对发送的数据的认可，然后将数据和签名信息一起发送给对方。届时接受方使用发送方的公钥来解密签名信息，并验证签名信息。典型的数字签名算法是 DSA 算法，RSA 算法也可用于数字签名。

在非对称密钥算法中，最常用的是 RSA 算法。在密钥交换协议中，经常使用 Diffie-Hellman 算法。接下来我们具体介绍 RSA 算法。

2）RSA 算法

当前最著名、应用最广泛的公钥系统 RSA 是在 1978 年，由美国麻省理工学院（MIT）的 Rivest、Shamir 和 Adleman 在题为《获得数字签名和公钥密码系统的方法》的论文中提出的。它是一个基于数论的非对称（公钥）密码体制，是一种分组密码体制。其名称来自于 3 个发明者的姓名首字母。

拓展提高

RSA 算法的安全性是基于大整数素因子分解的困难性，而大整数素因子分解问题是数学上的著名难题，至今仍没有有效的解决方法，因此可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

RSA 算法是第一个既能用于数据加密也能用于数字签名的算法，因此它为公用网络上信息的加密和鉴别提供了一种基本的方法。它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册，人们用公钥加密文件发送给个人，个人就可以用私钥解密接受。为提高保密强度，RSA 密钥至少为 500 位长，一般推荐使用 1024 位。

该算法基于下面的两个事实，这些事实保证了 RSA 算法的安全有效性。

①已有确定一个数是不是质数的快速算法。

②尚未找到确定一个合数的质因子的快速算法。

RSA 算法的工作原理简要介绍如下。

①任意选取两个不同的大质数 p 和 q，计算乘积 $r=p\times q$。

②任意选取一个大整数 e，e 与 $(p-1)\times(q-1)$ 互质，整数 e 用作加密密钥。注意：e 的选取是很容易的，例如，所有大于 p 和 q 的质数都可用。

③确定解密密钥 d：$(d\times e)\bmod\{(p-1)\times(q-1)\}=1$ 根据 e、p 和 q 可以容易地计算出 d。

④公开整数 r 和 e，但是不公开 d。

⑤将明文 P（假设 P 是一个小于 r 的整数）加密为密文 C，计算方法为：$C=P^e \bmod r$。

⑥将密文 C 解密为明文 P，计算方法为： $P = C^d \bmod r$。然而只根据 r 和 e (不是 p 和 q) 要计算出 d 是不可能的。因此，任何人都可对明文进行加密，但只有授权用户 (知道 d) 才可对密文解密。

3）RSA 算法实现

为了说明该算法的工作过程，下面给出一个简单例子，显然我们在这里只能取很小的数字；但是如上所述，为了保证安全，我们在实际应用中所用的数字则要很大。

例：取 p=3, q=5，则 r=15，$(p-1)\times(q-1)=8$。选取 e=11(大于 p 和 q 的质数)，通过 (d × 11)mod 8= 1，计算出 d =3。

假定明文为整数 13。则密文 C 为：

$C = P^e \bmod r$

$= 13^{11} \bmod 15$

$= 1\ 792\ 160\ 394\ 037 \bmod 15$

$=7$

复原明文 P 为：

$P = C^d \bmod r$

$= 7^3 \bmod 15$

$= 343 \bmod 15$

$= 13$

因为 e 和 d 互逆，公开密钥加密方法也允许采用这样的方式对加密信息进行“签名”，以便接收方能确定签名不是伪造的。

假设 A 和 B 希望通过公开密钥加密方法进行数据传输，A 和 B 分别公开加密算法和相应的密钥，但不公开解密算法和相应的密钥。A 和 B 的加密算法分别是 ECA 和 ECB，解密算法分别是 DCA 和 DCB，ECA 和 DCA 互逆，ECB 和 DCB 互逆。若 A 要向 B 发送明文 P，不是简单地发送 ECB(P)，而是先对 P 施以其解密算法 DCA，再用加密算法 ECB 对结果加密后发送出去。

密文 C 为：

```
C = ECB(DCA(P))
```

B 收到 C 后，先后施以其解密算法 DCB 和加密算法 ECA，得到明文 P。

```
ECA(DCB(C))
= ECA(DCB(ECB(DCA(P))))
= ECA(DCA(P))                    /*DCB 和 ECB 相互抵消 */
= P                              /*DCB 和 ECB 相互抵消 */
```

这样 B 就可确定报文确实是从 A 发出的，因为只有当加密过程利用了 DCA 算法，用 ECA 才能获得 P，只有 A 才知道 DCA 算法，即使是 B 也不能伪造 A 的签名。

（3）数字签名技术

如何保证信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性，现在大多采用数字签名、签名认证的方式加以解决。

1）数字签名技术的概念

在日常生活和经济往来中，签名盖章是非常重要的。在签订经济合同、契约、协议及银行业务等很多场合都离不开签名或盖章，它是个人或组织针对其行为的认可，并具有法律效力。而手体签字长期以来被当作一种合法的凭证而被广泛使用，这主要是由于手体签字可满足以下几个原则。

①签字是可以被确认的，即当文件上有某人的签字时，别人确信这个文件是经该人发出的。

②签字是无法伪造的，即签字是签字者的凭证。

③签字是无法被重复使用的，即任何人无法将别人在别处的签字挪到该文件上。

④文件被签字后是无法篡改的。

⑤签字具有不可否认性，即签字者无法否认自己签字文件上的签字行为。

拓展提高

在计算机网络应用中，尤其是电子商务中，电子交易的不可否认性是必要的。它一方面要防止发送方否认曾发送过消息；另一方面还要防止接收方否认接收过消息，以避免产生经济纠纷。提供这种不可否认性的安全技术就是数字签名。

数字签名包括消息签名和签名认证两个部分。对于一个数字签名系统必须满足下列条件。

①一个用户能够对一个消息进行签名。

②其他用户能够对被签名的消息进行认证，以证实该消息签名的真伪。

③任何人都不能伪造一个用户的签名。

④如果一个用户否认对消息的签名，则可以通过第三种仲裁来解决争议和纠纷。

公钥密码系统为数字签名提供了一种简单而有效的实现方法，其工作原理如图1-5所示。

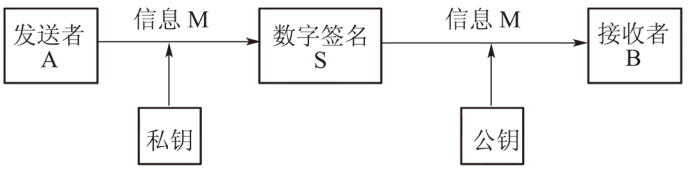

图1-5 数字签名的工作原理

假如 A 向 B 发送一个消息 M，现在使用基于公钥密码系统的数字签名方法对消息 M 进行签名和签名认证。其过程如下：

① A 使用自己的私钥加密消息 M，生成签名 S。

② A 将消息 M 和签名 S 发送给 B。

③ B 使用 A 的公钥解密 S，恢复信息 M，并比较两者的一致性来验证签名。

可见数字签名系统和数据加密系统既有联系，又有差别。在数据加密系统中，发送者使用接收者的公钥加密所发送的数据，接收者使用自己的私钥解密数据，目的是保证数据的机密性，但不验证数据。同时，它还要解决密钥的分配和分发问题。在数字签名系统中，签名者使用自己的私钥加密关键性信息 (如信息摘要) 作为签名信息，并发送给接收者，接收者则使用签名者的公钥来解密签名信息，并验证签名信息的真实性。有些数字签名算法，如 DSA(Digital Signature Algorithm) 不具有数据加密和密钥分配能力，主要通过变换计算来产生和验证签名信息。而有些数据加密算法，如 RSA 则可以用于数字签名。

2）数字签名的实现方法

DSA(Digital Signature Algorithm) 是美国国家标准技术协会 (NIST) 在其制定的数字签名标准 (DSS) 中提出的一个数字签名算法。DSA 基于公钥体系，用于接收者验证数据的完整性和数据发送者的身份，也可用于第三方验证签名和所签名数据的真实性。

拓展提高

在DSS标准中规定，数字签名算法应当无专利权保护问题，以便推动该技术的广泛应用，给用户带来经济利益。由于 DSA 无专利权保护，而 RSA 受专利权保护，因此，DSS 选择了 DSA 而没有采纳 RSA。结果在美国引起很大争论，一些购买 RSA 专利许可权的大公司从自身利益出发强烈反对 DSA，给 DSA 的推广应用带来一定的影响。

DSA 是一种基于公开密钥体系的数字签名算法，它不能用作加密，只用做数字签名。DSA 使用公开密钥，为接收者验证数据的完整性和数据发送者的身份。它也可用于由第三方确定签名和所签数据的真实性。DSA 算法的安全性基于解离散对数的困难性，这类签字标准具有较大的兼容性和适用性，成为网络安全体系的基本构件之一。

在 DSA 签名算法中，用到了以下参数。

① p 是 L 位长的素数，其中 L 为 512 ~ 1024，且是 64 的倍数。

② q 是 160 位长且与 p–1 互素的因子。

③ $g=h^{(p-1)}/q \bmod p$，其中 h 是小于 p–1 并且满足 $h(p-1)/q \bmod p$ 大于 1 的任意数。

④ x 是小于 q 的数。

⑤ $y=g^{x} \bmod p$。

在上述参数中，p、q 和 g 是公开的，可以在网络中被所有用户公用，私人密钥是 x，公开密钥是 y。

如果对消息 m 签名时

①发送者产生一个小于 q 的随机数 k。

②发送者产生：

$r=(g^k \bmod p) \bmod q$

$s=(k^{-1}(H(m)+xy)) \bmod q$

r 和 s 就是发送者的签名，发送者将它们发送给接收者。

③接收者通过计算来验证签名。

$w=s^{-1} \bmod q$

$i=(H(m)w) \bmod q$

$j=(rw) \bmod q$

$v=((g^i \times y^j) \bmod p) \bmod q$

如果 v=r，则签名有效。

在 DSS 中，还推荐了一种产生素数 p 和 q 的方法，它使人们相信尽管 p 和 q 是公开的，但其产生方法具有可信的随机性，因此 DSA 是很安全的。

3）数字签名的其他问题

目前，日益激增的电子商务和其他因特网应用需求使公钥体系得以普及，这些需求量主要包括对服务器资源的访问控制和对电子商务交易的保护，以及权利保护、个人隐私、无线交易和内容完整性（如保证新闻报道或股票行情的真实性）等方面。公钥技术发展到今天，在市场上明显的发展趋势就是 PKI 与操作系统的集成，PKI 是“Public Key Infrastructure”的缩写，意为“公钥基础设施”。公钥体制广泛地用于 CA 认证、数字签名和密钥交换等领域。

公钥加密算法中使用最广的是 RSA。RSA 算法研制的最初理念与目标是努力使互联网安全可靠，旨在解决 DES 算法密钥利用公开信道传输分发的难题。而实际结果不但很好地解决了这个难题，还可利用 RSA 完成对电文的数字签名，以防止电文的否认与抵赖；同时还可以利用数字签名较容易地发现攻击者对电文的非法篡改，以保护数据信息的完整性。

拓展提高

到目前为止，很多种加密技术采用了 RSA 算法，该算法也已经在互联网的许多方面得以广泛应用，包括在安全接口层（SSL）标准（该标准是网络浏览器建立安全的互联网连接时必须用到的）方面的应用。此外，RSA 加密系统还可应用于智能 IC 卡和网络安全产品。

但目前 RSA 算法的专利期限即将结束，取而代之的是基于椭圆曲线的密码方案(ECC 算法）。与 RSA 算法相比，ECC 有其相对优点，这使得 ECC 的特性更适合当今电子商务需要快速反应的发展潮流。此外，一种全新的量子密码也正在发展中。

至于在实际应用中应该采用何种加密算法则要结合具体应用环境和系统，不能简单地根据其加密强度来做出判断。因为除了加密算法本身之外，密钥合理分配、加密效率与现有系统的结合性以及投入产出分析都应在实际环境中具体考虑。加密技术随着网络的发展更新，将有更安全更易于实现的算法不断产生，为信息安全提供更有力的保障。今后，加密技术会何去何从，我们将拭目以待。

（4）密钥管理

密码系统的两个基本要素是加密算法和密钥管理。加密算法是一些公式和法则，它规定了明文和密文之间的变换方法。由于密码系统的反复使用，仅靠加密算法已难以保证信息的安全了。事实上，加密信息的安全可靠依赖于密钥系统，密钥是控制加密算法和解密算法的关键信息，它的产生、传输、存储等工作十分重要。

1）私钥分配

两个用户在用单钥加密(私钥)体制进行保密通信时，必须有一个共享的秘密密钥。为防止攻击者得到密钥，还必须时常更新密钥。因此，密码系统的强度也依赖于密钥分配技术。用户 A 和 B 获得共享密钥的方法基本上有以下几种。

①密钥由 A 选取并通过物理手段发送给 B。

②密钥由第三方选取并通过物理手段发送给 A 和 B。

③如果 A、B 事先已有一密钥，则其中一方选取新密钥后，用已有的密钥加密新密钥并发送给另一方。

④如果 A 和 B 与第三方 C 分别有一保密信道，则 C 为 A、B 选取密钥后，分别在两个保密信道上发送给 A、B。

前两种方法称为人工发送，密钥的人工发送在网络的链路加密时还是可行的。因只有该链路上的两端交换数据，密钥的人工发送在网络的端到端加密方式中将不再可行。因为若是在网络层加密，则网络中任一对主机都必须有一共享密钥。如果有 N 台主机，则密钥数目为 N(N−1)/2。当 N 很大时，密钥分配的代价将非常大。

第三种方法对链路加密和端到端加密方式都是可行的，但是攻击者一旦获得一个密钥就可获取以后的所有密钥。其初始密钥的分配代价仍然很大。

第四种方法广泛用于端到端加密方式时的密钥分配，其中的第三方通常是一个负责为用户分配密钥的密钥中心 (Key Distribution Center，KDC)。每个用户必须和 KDC 有一个共享密钥，称为主密钥。通过主密钥分配给一对用户的密钥称为会话密钥，用于这一对用户之间的保密通信。

拓展提高

通信完成后，会话密钥即刻被销毁。若用户数为 N 个，则会话密钥为 N(N−1) /2。但主密钥数却只需 N 个，即可通过物理手段发送主密钥。

2）公钥分配

公钥加密的一个主要用途是分配单钥加密体制使用的密钥。公钥加密体制大致有以下几种公开密钥的分配方式。

①公开发布。

用户将自己的公钥发给每一个其他用户或向某一团体广播。这种方法虽简单却使任何人都可伪造这种公开发布。假冒者可解读发向被伪造方的加密消息，还可用伪造的密钥获得认证。

②公用目录表。

公用目录表是指建立一个公用的公钥动态目录表，由某个可信的实体或组织承担目录表的建立、维护以及公钥的分布。这种方法比前一种安全性更高，但仍然容易受到攻击。

③公钥管理机构。

公钥管理机构是在公钥目录表中对公钥的分配施加更严密的控制，使其安全性更强。公钥管理机构在为各用户建立、维护动态的公钥目录的同时，还提供每个用户都可靠地知道管理机构的公钥，而只有管理机构自己知道相应的密钥。公钥的分配如图 1-6 所示，分配步骤如下所示。

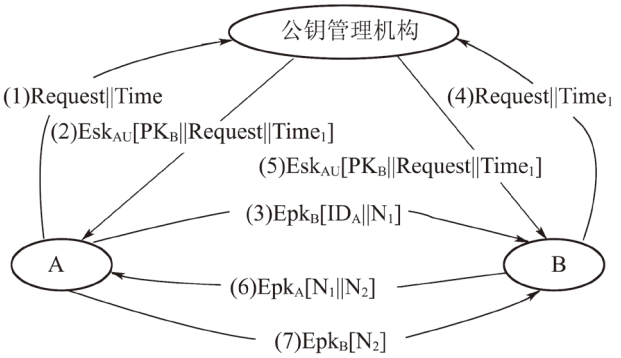

图 1-6 公钥管理机构分配公钥

STEP 1 用户 A 向公钥管理机构发送一带有时间戳的消息，其请求获取用户 B 当前的公钥。

STEP 2 管理机构用自己的密钥 SKAU 加密对 A 的请求做出应答。A 可以用管理机构

的公钥解密，并使 A 相信这个消息的确是来源于管理机构。其应答的消息有以下作用。

- B 的公钥 PKB，A 可用其对将要发往 B 的消息加密。
- A 验证自己最初发出的请求在被管理机构收到以前未被篡改。
- 时间戳使 A 相信管理机构发来的消息是 B 当前的公钥。

STEP 3 A 用 B 的公钥对一个消息加密后发送给 B，其中一项是 A 的身份 IDA，另一项是一个一次性随机数用于 N1，用于唯一地标识本次业务。

STEP 4 用户 B 向公钥管理机构发送一带有时间戳的消息，其请求获取用户 A 当前的公钥。

STEP 5 管理机构用自己的密钥 SKAU 加密对 A 的请求做出应答。此时，A 和 B 都已安全地得到了对方的公钥，但仍需要有进一步的相互认证。

STEP 6 B 用 PKA 对一个消息加密后发送给 A，其消息有 A 的一次性随机 N1 和 B 产生的一个新的一次性随机数 N2。因为只有 B 能解密第 3 步中的消息，所以 A 收到的消息中的 N1 可使其相信通信的另一方的确是 B。

STEP 7 A 用 B 的公钥对 N2 加密后返回给 B，可使 B 相信通信的另一方的确是 A。

以上 7 个消息中的前 4 个消息用于获取对方的公钥。用户得到对方的公钥后保存，使之以后使用时只发送第 6、7 步确认消息即可。但还必须定期地通过密钥管理机构中心获取对方的公钥，以免对方的公钥更新后无法保证当前的通信。

④公钥证书。

公钥分配的另一种方法是公钥证书，用户通过公钥证书相互之间交换自己的公钥而无须与公钥管理机构联系。公钥证书由证书管理机构 (Certificate Authority, CA) 为用户建立，其证书的数据项有用户的公钥、身份和时间戳等，这些数据项经 CA 用自己的密钥签字后就形成了证书，其形式为 CA =ESKCA[T.IDA.PKA] ，其中 IDA 用户 A 的身份，PKA 是 A 的公钥，T 是当前时间戳，SKCA 是 CA 的密钥，CA 即为用户 A 产生的证书，如图 1-7 所示。

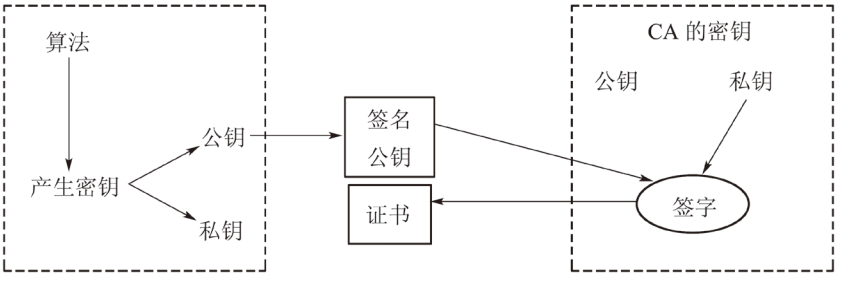

图 1-7　证书的产生过程

拓展提高

用户可将自己的公钥通过公钥证书发给另一用户，接收方可用 CA 的公钥 PKCA 对证书加以验证，因为只有用 CA 的公钥才能解读证书，同时获得发送方的 IDA 和公钥 PKA。时间戳用于鉴定收到的证书是否是当前或有效的。

3）用公钥加密分配私钥密码体制的密钥

由于公钥加密过程复杂且速度慢，所以不太适合进行保密通信，但却适合于分配单钥密码体制的密钥。

①简单分配。

简单地使用公钥加密算法建立用户 A 和用户 B 会话密钥的过程可有以下几个步骤。

STEP 1 用户 A 产生自己的一对密钥 $\{PK_A, SK_A\}$，并向 B 发送 $PK_A \| IDA$。

STEP 2 B 产生会话密钥 Ks，并用 A 的公钥 PK_A 对 K_S 加密后发给 A。

STEP 3 A 由 $DSK_A[EPK_A[KS]]$ 恢复会话密钥。因为只有 A 能解读 Ks，所以仅 A 和 B 知道该共享密钥。

STEP 4 A 销毁 $\{PK_A, SK_A\}$，B 销毁 PKA。

此时用户 A、B 用私钥加密算法以 Ks 作为会话密钥进行保密通信。通信完成后，又都将 Ks 销毁。

拓展提高

这种分配方法尽管简单却易受到主动攻击。攻击方 E 可通过以下方式截获用户 A 和 B 的通信。

STEP 1 用户 A 产生自己的一对密钥 $\{PK_A, SK_A\}$，并向 B 发送 $PK_A \| ID_A$。

STEP 2 E 截获 A 发给 B 的消息后，建立自己的一对密钥 $\{PK_E, SK_E\}$，并将 $PK_E \| ID_E$ 发送给 B。

STEP 3 B 产生会话密钥 K_S 后将 $EPK_E[K_S]$ 发送出去。

STEP 4 E 截获 B 发送的消息后，由 $DSK_E[EPKE[K_S]]$ 解读 K_S。

STEP 5 E 再将 $EPK_A[K_S]$ 发给 A。

此时，A 和 B 将用 K_S 进行通信，但并不知 E 的存在，E 可以对 A 和 B 实施监听。

②具有保密性和认证性的密钥分配若用户 A 和 B 双方已完成公钥交换，可按以下步骤建立会话密钥，如图 1-8 所示。

STEP 1 A 用 B 的公钥加密 A 的身份 ID_A 和一个一次性随机数 N_1 后发给 B，其中 N_1 用于唯一地标识此次业务。

STEP 2 B 用 A 的公钥 PK_A 加密 A 的一次性随机数 N1 和 B 新产生的一次性随机数 N_2

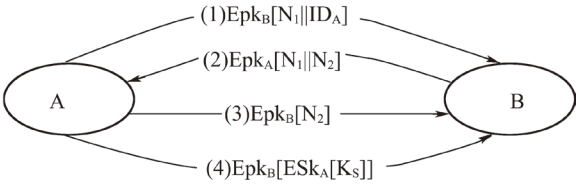

图 1-8　具有保密性和认证性的密钥分配

后发给 A。因为只有 B 能解读 A 发给 B 的消息，而 B 所发的消息中 N_1 的存在可使 A 相信对方的确是 B。

STEP 3　A 用 B 的公钥 PK_B 对 N_2 加密后返回给 B，以使 B 相信对方的确是 A。

STEP 4　A 选一个会话密钥 K_S，然后将其 M =EPK B[ESK A[K_S]] 发给 B，其中用 B 的公钥加密是为了保证只有 B 能解读加密结果，用 A 的密钥加密是保证该加密结果只有 A 能发送。

STEP 5　B 以 DSK_A[DSK B[M]] 恢复会话密钥。

这种密钥分配过程具有保密性和认证性，既可防止被动攻击，也可防止主动攻击。

（5）认证

认证 (Authentication) 是证实某人或某个对象是否有效合法或名副其实的过程。它与身份识别 (Identification) 不同，也与授权 (Authorization) 不同。在非保密的计算机网络中，验证远程用户 (或过程实体) 是合法授权用户还是恶意的入侵者就属于认证问题。认证是对通信对象的验证；授权是验证用户在系统中的权限；识别则是判别通信对象是哪种身份。

知识链接

有两种形式的认证，一种是在初始化登录的过程中，用户和机器之间的认证，另一种是在操作过程中机器和机器之间的认证。

在登录过程中，应当验证用户“知道什么”，其次应当验证“他拥有什么”，如智能卡、通行证等，最后，应当验证他拥有什么生物特征，如指纹、声音等。

机器和机器之间的认证一般分为密码方法和秘密 (非公开的协议) 方法。

1）身份认证

身份认证，也称为身份甄别。身份认证是对网络中通信双方的主体进行验证的过程。用户必须提供他是谁的证明。例如，系统中存储用户的指纹，或者用户的视网膜血管分布图，或者用户的声音波纹图等。当用户登录系统时，系统将对其辨认，比较、验证该用户的真实性。

通常有以下 3 种方法验证主体身份：

①拥有该主体知道的秘密，如密码、密钥。

②主体携带的物品，如智能卡、令牌卡。

③主体具有的唯一特征，如指纹、声音、视网膜或签名等。

密码有时由用户选择，有时由系统分配。密码的优点是简单可行，无须特殊硬件设备。但密码是无形的，可能告知别人或被别人猜测、窃听，因此密码不是强有力的认证手段。除非使用一次性密码，才能增强安全性。一次性密码的配置可以因时因地因不同信息而异。系统要用户回答的密码约每分钟变化一次，绝不会重复。合法用户要使用手持式认证器或称为解密器 (Descrambler)，或令牌 (Token)。认证器通常包含一个内部时钟、某种类别的一个密钥以及一个显示屏。显示屏显示现在的时间和密钥的某种函数。

主机通过使用其秘密密钥的副本及其时钟计算出的所希望的输出值，对用户进行证实。如果用户的回答与输出值匹配，则登录被接收。考虑到双方的时间偏差，通常会有几个候选密码，如果用户密码及输出密码与该组密码匹配，也能通过验证。

另一种一次性密码系统使用来自主机而不是时钟的非重复性质询。用户拥有的是一台利用秘密密钥编程的设备。主机的质询输入该设备，然后由秘密密钥计算出该次的密码。由于不存在时钟偏差，唯一要求的是用户要每次输入主机的质询。

在这两种方式中，如果手持式认证器或用户的编程设备被窃取，将给网络安全带来隐患。因此，每个设备使用前，还要输入用户的 PIN(Personal Identification Number)。

知识链接

智能卡 (Smart Card) 具有自己的 CPU、输入输出端口和只能通过卡上 CPU 进行访问的小容量、非易失性存储器，它可集成到用户终端上，便于携带，方便验证。

生物技术，如采取指纹、声音或签字的认证方法，除了需要特殊的阅读器外，有些生物特征具有模糊性，同一个人不同时刻的签字会受多种因素干扰，绝对不可能相同。

2）主机之间的认证

如果要认证的对象是主机或站点。例如，银行之间，银行与商家之间的通信，需要确认的是对方主机的身份。据此判别通信是否在指定的主机 (或站点) 之间进行，这样的过程被称为站点认证或主机认证。

认证可以有多种形式。如果双方通过电话、直接见面的方式事先确定了一个共享秘密密钥 KAB。那么，一种可行的协议是查询—应答协议。一方发送一个随机数给另

一方，即查问，后者将它用秘密密钥加密后作为应答。通过检查应答来确定对方是否拥有该秘密密钥。

在所有的通信实体间预先分配一个密钥是不现实的，特别是在因特网通信当中。因此，在通信开始前，密钥分发中心 (KDC，Key Distribution Center) 可以在通信双方之间充当一个中间人的角色。每一个通信主体，如 A 方和 B 方各自与 KDC 共享一个密钥。这就说明， A 方和 KDC、B 方和 KDC，它们之间是相互信任的。通过共享的密钥，可以确认对方是谁。因此，认证协议就成了 3 个主体之间的通信。在协议执行中，除了要为 A 方和 B 方建立一个秘密会话密钥 (Session Key) 外，还要使 A 方和 B 方达到相互信任。同时要防止黑客可能的攻击。

黑客的攻击手段一般采用重发攻击。例如，A 方要通过银行 (B 方) 发送一笔钱给 C 方，A 方选择一个会话密钥 Ks，传送消息 $A=K_A(B，Ks)$ 给 KDC 收到这个消息后，知道是 A 方传送的，就用 K_A 将 $K_A(B，Ks)$ 解密，得到 (B，Ks)。现在 KDC 知道 A 方要和 B 方通信，就用 K_B 把 (A，Ks) 加密后发给 B。B 用 K_B 解密后，知道是 A 方的连接请求，并且得到密钥 Ks。这样，A 方和 B 方就可以通过 Ks 直接会话了。

假定 A 方要 B 方发送支付报文，也就是说 A 方想让 B 方支付一笔钱给 C 方。B 方将照此办理，支付了一笔钱。但是，过了一会儿，有人顶替 A 方将支付报文又重发给 B 方，在 B 看来，它是正常的报文，于是又从 B 方的账户中支付一笔钱给 C 方。这样，同一笔钱支付两次或更多次，认证协议失败。

解决的办法是在每一条消息上加上时间戳，如果发现信息中包含的时间戳是重复的，则将它丢弃。因此，当 A 方或别人重发这条消息时，B 方 (银行) 查看消息中的时间戳后，就知道该消息是过时的，不是有效的消息。这种方法的难度在于要求网络系统中所有主机的时间保持一致，在时间误差范围内，重发的消息不容易被识别。

第二种方法是在每条消息中赋予一个一次性的唯一的序列号，随消息发送。如果收到的消息序列号重复，则丢弃。为此，主机应记住所有收到的序列号，且序列号应足够大，保证在正常使用的情况下，不至于重复。

知识链接

基于密钥分发中心的认证方法还有多种。例如，使用多次查问一应答方式的 Needham-Schroeder 协议及 Otway-Rees 协议，都是一些更加成熟的协议。

3）Kerberos 认证

Kerberos 是为 TCP/IP 网络系统设计的可信的第三方认证协议。网络上的 Kerberos 服务基于 DES 对称加密算法，但也可用其他算法替代。因此，Kerberos 是一个在许多

系统中获得广泛应用的认证协议，Windows 2000 就支持该协议。

Kerberos 最初是美国麻省理工学院为 Athena 项目开发的。其中第 1 版至第 3 版为内部开发版，第 4 版提供扩散密码分组链接 (PCBC) 模式。该模式存在一个问题：交换两个密文分组，将使两个对应的明文分组不能被正确解密，但根据明文和密文异或的性质，错误将被抵消。

所以，如果完整性检查只检查最后几个解密的明文分组，它可能欺骗接收者，让接收者接收部分错误的消息。因此，Kerberos 第 5 版使用 CBC(Cipher Block Chaining) 模式。下面讨论 Kerberos 第 5 版。

① Kerberos 工作原理

当客户从 Kerberos 请求一张票据许可服务 (TGS，Ticket Granting Service)，该票据用用户的秘密密钥加密后发送给用户。为了使用特定的服务器，客户需要从 TGS 中请求一张票据。假定所有事情均按序进行，TGS 将票据发回给客户，客户将此票据显示给服务器和认证器，如果客户身份没有问题，服务器便让客户访问。Kerberos 的认证步骤如图 1-9 所示。

- 请求许可票据。
- 返回许可票据。
- 请求服务器票据。
- 返回服务器票据。
- 请求服务。

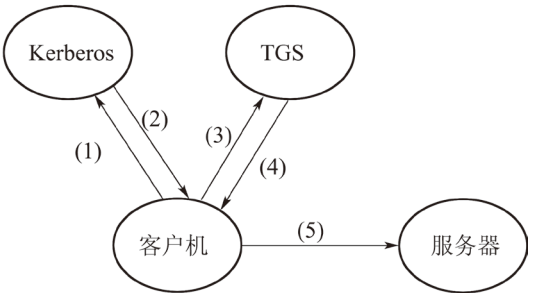

图 1-9 Kerberos 鉴别协议工作原理

② Kerberos 的凭证

Kerberos 使用两类凭证，票据 (Ticket) 和认证码 (Authenticator)。

Kerberos 票据的格式为：

$Tc,s=s,\{c, a, v, kc,s\}K_s$

上式中 Tc,s 表示使用服务器的客户机票据，s 表示服务器，c 表示客户机，a 表示客户机的网络地址，v 表示票据的有效起止时间，kc,s 表示客户机与服务器的会话密钥，

Ks 表示服务器的秘密密钥，{m}Ks 表示以 Ks 加密的信息 m。

对单个服务器和客户而言，票据有较大的用处。它包括用户名、服务器名、网络地址、时间标记和会话密钥等。这些信息用服务器的秘密密钥加密，客户一旦获得该票据，可多次使用它访问服务器，直到票据过期。

知识链接

客户无法解密票据，这是因为客户不知道服务器的秘密密钥。但客户可以以其加密的形式呈递服务器。票据以密码形式传送，使网上窃听者无法阅读或修改。

Kerberos 认证码的格式为

Ac,s={c, t, Key}Kc,s

上式中 Ac,s 表示从客户机 c 到服务器 s 的认证码。c 为客户机，t 为时间标记，Key 为可选的附加会话密钥。{c, t, Key}Kc,s 表示利用服务器和客户机共享的会话密钥，Kc,s 对 c, t, Key 加密与票据不一样，认证码只用一次。如果用户需要，可再产生一个认证码。

这样，认证码可以达到两个目的：首先，它表明认证码的发送者也知道密钥，这是身份认证的目的；其次，封装的明文包括了时间标记，可以防止窃听者重发攻击。

③ Kerberos 的消息

Kerberos 第 5 版有 5 个消息，如图 1–8 所示。

第一个消息，客户到 Kerberos：c,tgs 。

客户注册程序发送客户名及其 TGS 服务器名的请求给 Kerberos 服务器。服务器在数据库中查找客户，如有该客户，则 Kerberos 产生一个会话密钥，在客户和 TGS 之间使用，这叫票据许可票据 (TGT)。

第二个消息，Kerberos 到客户：{ Kc,tgs}Kc,{Tc,tgs}Ktgs。

Kerberos 利用客户的秘密密钥加密会话密钥，然后为客户产生一个 TGT 向 TGS 证实自己的身份，并用 TGS 的秘密密钥对其加密：｛ T c,tgs｝Ktgs 。Kerberos 将这两个消息发送给客户。

第三个消息，客户到 TGS：{Ac,s}Kc,tgs ,{Tc,tgs}Ktgs 。

客户收到认证服务器的响应消息，如果客户是一个合法用户，将可以方便地解密。如果客户是一个非法用户或骗子，他不知道密码，因而无法解答。系统拒绝访问，他无法获得票据或会话密钥。

客户将 TGT 和会话密钥保存起来，并销毁密码和单向散列函数，防止泄密。该信息只在 TGT 的有效期内才有用。一旦 TGT 过期，这些消息便一文不值。

客户可在 TGT 的有效期内向 TGS 证实自己的身份。{Ac,s} Kc,tgs 表示利用客户和 TGS 共享的会话密钥，Kc,tgs 对客户机到服务器的认证码 Ac,s 进行加密。

第四个消息，TGS 到客户：{Kc,s}Kc,tgs ，{Tc,s} Ks。

TGS 接收到客户的请求后，用自己的密钥解密此 TGT，然后再用 TGT 中的会话密钥解密认证码。最后，TGS 比较认证码中的信息与票据中的信息，客户的网络地址与发送的请求地址，以及时间标记与当前时间。如果每一项都吻合，便允许处理该请求。

如果请求时间相差太远（假设所有机器都有同步时钟，至少在几分钟内应同步），则 TGS 可把该请求当作以前请求的重发，与已收到的请求具有相同票据和时间标记的请求则被忽略。

TGS 通过将客户有效的票据返回给服务器的方式响应一个有效请求。TGS 还为客户服务器产生一个新的会话密钥，此密钥由客户和 TGS 共享的会话密钥加密。然后将这两种消息返回给客户。客户解密消息，同时获得会话密钥。

第五个消息，客户到服务器：{ Ac,s} kc,s,{Tc,s} ks 。

现在，客户向服务器产生一个认证码，认证码由用户名、客户网络地址和时间标记组成，用 TGS 为客户和服务器产生的会话密钥加密得到。向服务器的请求由从 Kerberos 接收到的票据和加密的认证码组成。

知识链接

服务器检查解密后的票据和认证码，以及客户地址和时间标记，当一切无误后，根据 Kerberos，服务器可判断该客户的身份。在需要相互认证的应用中，服务器给客户返回一个包含时间标记的消息，该消息由会话密钥加密。这证明服务器知道客户的秘密密钥而且能解密票据和认证码。这样，客户和服务器可以用共享的密钥加密消息，并能确认消息是否来自对方。

④ Kerberos 的安全性

由于认证码基于网络中的所有时钟基本上是同步的事实，如果能欺骗主机，使它的正确时间发生错误，那么旧的认证码毫无疑问能被重发。

Kerberos 对猜测密码攻击也很脆弱，攻击者收集票据并试图破译它们。只要票据足够多，就有很多机会找出密码。

Kerberos 依赖于 Kerberos 软件。因此，黑客可以自己编写该软件代替所有客户的 Kerberos 软件。在不安全的计算机网络环境中，它很容易成为攻击的目标。

为了加强 Kerberos 的安全性，建议采用基于公开密钥的算法和智能卡接口进行密钥的管理。

任务实施

（1）安装使用 OpenSSH

这里主要讲的是基于 FreeBSD 的 OpenSSH 的配置，其他 UNIX 及派生系统使用 OpenSSH 的方法大致是 FreeBSD 中集成了 OpenSSH，在很多 Linux 的发行版中都没有包括 OpenSSH。但是，用户可以从网络上下载并安装 OpenSSH（通过访问 OpenSSH 的主页 http://www.openssh.org）。

1） 生成密钥对

使用 ssh-keygen 生成密钥对，比如用 DSA 加密算法生成一个 4096 位的密钥对，可以输入如下命令（具体参数请参阅 man ssh-keygen）。

```
#ssh-keygen -b 4096 -t dsa
%ssh-keygen -b 4096 -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/fdy84/.ssh/id_dsa) :
（密钥对将要存的路径，括号内为默认）
Created directory '/home/fdy84/.ssh'.
Enter passphrase (empty for no passphrase) :
（输入密码）
Enter same passphrase again:
（再次输入密码，如果忘记，则只能重新生成密钥）
Your identification has been saved in /home/fdy84/.ssh/id_dsa.
（使用者的私钥）
Your public key has been saved in /home/fdy84/.ssh/id_dsa.pub.
（使用者的公钥）
The key fingerprint is:
bb:1b:f5:1c:77:62:90:21:59:7e:c6:65:e5:24:c6:e5 fdy84@freebsd
```

2） 分发密钥

刚才生成了一对密钥，把私钥放在自己的机器上的 ~/.ssh/ 目录下，并保证访问权限是 “-rw——”（即 600）。再把生成的公钥放在要连接的远程主机的 ~/.ssh/ 目录下，并改名为 authorized_keys，并且保证文件除了属主外没有被人修改的权限。

（2）配置使用 SSH

1） 配置服务端，启动 SSH 服务端很简单，只需要运行： # sshd 就可以了。或者在 /etc/rc.conf 中加入： sshd_enable=“YES”

就可以在每次启动时自动运行 SSH 服务端。

SSH 服务端的配置使用的配置文件是“/etc/ssh/sshd_config”，并且 OpenSSH 1.x 和 2.x 的服务器配置文件均为此文件。

2）配置客户端，客户端想连接远程服务器只需要输入：

```
#ssh 域名（或 ip）
```

就可以了。

比如想以 fdy84 用户连接 IP 地址为 192.168.0.6 的一台远程服务器，需要键入：

```
# ssh 192.168.0.6 -l fdy84
```

只要配置正确就可以连上远端的服务器。

（3）使用 Windows 下的 SecureCRT 进行 SSH 连接

如何在 Windows 下通过 SSH 远程管理服务器？其实 Windows 有很多远程管理软件，在此主要介绍 SecureCRT 中 SSH 连接的使用。（以 Version 4.1.1 为例介绍）

Create Public Key…

1）SecureCRT 也可以生成密钥对，不过 SecureCRT 最大只支持 2048 位的密钥，选择菜单 Tools|Create Public Key，选择密钥算法和密钥长度，输入密码后再反复移动鼠标以生成密钥的足够的随机量之后，就等待计算机生成密钥对，如图 1-10 所示。

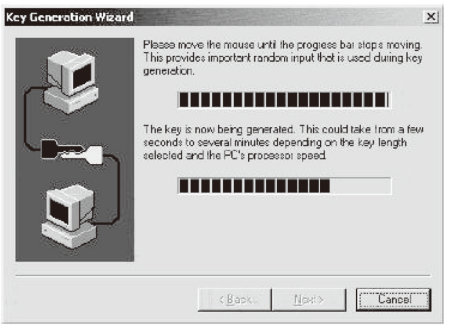

图 1-10 生成密钥对

2）单击左上角的 Connect 按钮，打开 Connect 对话框，如图 1-11 所示。

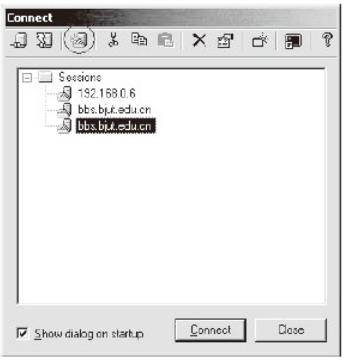

图 1-11 Connect 对话框

3）再单击图 1-11 中的 New Session 按钮，打开 Session Options 对话框，如图 1-12 所示。

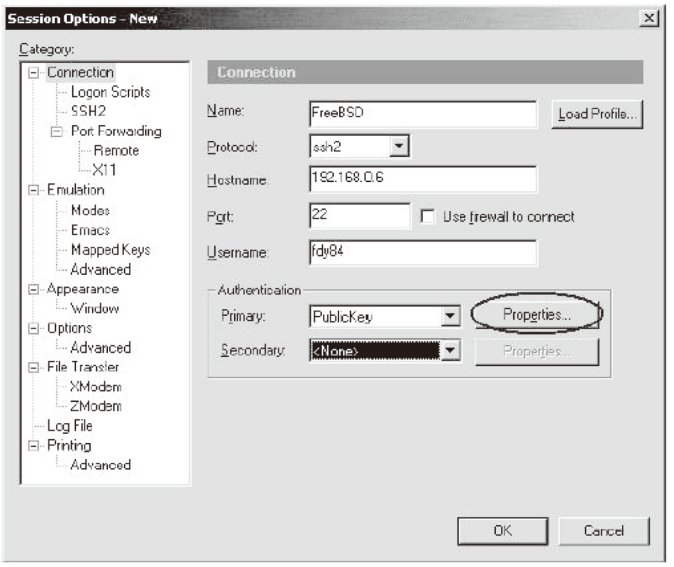

图 1-12　Session Options 对话框

4）选择 SSH 连接，并填入要连接的主机名称（或者 IP 地址）和用户名，再选择基于公钥方式的认证，单击 Properties 按钮，进入密钥配置对话框，如图 1-13 所示。

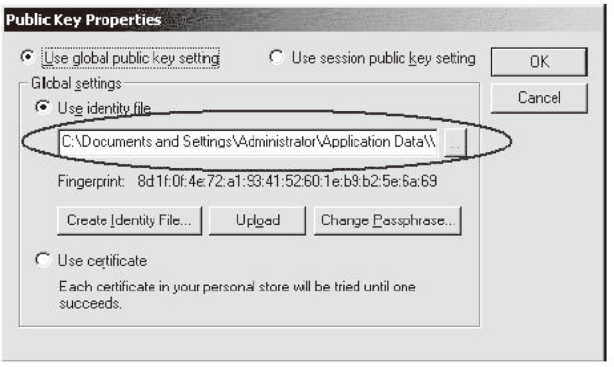

图 1-13　确定私钥文件

5）在圈中所示的位置填入私钥文件。

单击刚才建立的那个连接进行 SSH 连接，根据提示进行操作，就连接上远程的服务器了，如图 1-14 所示。

注意：由 SecureCRT 生成的密钥对和用 OpenSSH 生成的密钥对在格式上不一样，而且二者都只能识别自己的密钥格式，所以在用 SecureCRT 同 OpenSSH 连接时，都要用它们自己的密钥格式。可以用任何一个方法生成，然后使用 ssh- keygen-i 命令

把 SecureCRT 生成的密钥转换成 OpenSSH 的密钥格式，或者用 ssh-keygen-e 命令把 OpenSSH 的密钥格式转换成 SecureCRT 能够识别的 IETFSECSH 格式。

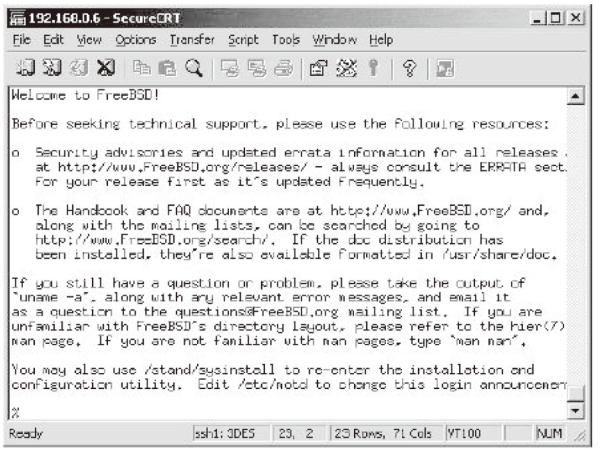

图 1-14 连接成功窗口

虽然 SSH 提供基于密码的登录，不过基于安全考虑，我们并不推荐使用这种登录。鉴于现在机器的速度普遍已经很快，因此可以使用 4096 位的密钥以加强安全性。

项目小结

本项目主要讲解了网络安全和计算机网络的密码技术的相关知识，其主要包括对称密码体制、公钥密码体制、数字签名技术、密钥管理以及认证等主要内容。

项目考核

填空题

1. 机密性指确保信息不暴露给 _____的实体或进程。

2. 常见的密码技术有 _____、 _____和 _____。

3. 认证是对 _____的验证；授权是验证 _____在系统中的权限，识别则是判断通信对象是哪种身份。

选择题

1. 以下不属于非对称密码算法特点的是（ ）。

A. 计算量大　　B. 处理速度慢

C. 使用两个密码　　D. 适合加密长数据

2. 对于一个数字签名系统的非必要条件有（　　）。

A．一个用户能够对一个消息进行签名

B．其他用户能够对被签名的消息进行认证，以证实该消息签名的真伪

C．任何人都不能伪造一个用户的签名

D．数字签名依赖于诚信

3. 不属于公钥管理的方法有（　　）。

A．公开发布　　B．公用目录表

C．公钥管理机构　　D．数据加密

问答题

1. 什么是网络安全？网络中存在哪些安全威胁？
2. 什么是主机网络安全？简单描述其体系结构。
3. TCSEC 每个级别标准各有什么特点？我国的信息安全标准有什么特点？
4. 常见的网络安全组件有哪些？它们分别完成什么功能？
5. 安全工作的目的是什么？如何进行安全策略的实施？
6. 简述公钥体制和私钥体制的主要区别？
7. 数据加密算法可以分为几大类型，各举一例说明。
8. 简要说明 DES 加密算法的关键步骤。
9. RSA 算法的基本原理和主要步骤是什么？
10. 什么情况下需要数字签名？简述数字签名的算法。
11. 简要说明密钥管理的主要方法。
12. 什么是身份认证？用哪些方法可以实现？
13. Kerberos 是什么协议？简要描述 Kerberos 的鉴别原理。