模块八：电子商务安全与防范

【学习目标】

通过本模块的学习与训练，要求学生掌握电子商务信息安全要素与防范措施；熟悉计算机病毒及其防治方法，了解信息加密技术与电子商务认证技术。学会 CA 证书的申请与使用；能够分析电子商务信息传递过程的安全防范措施。

【能力标准】

工作任务	能力标准	相关知识
网络安全隐患分析与防范	1．能够识别计算机病毒的种类 2．掌握预防、检测和清除计算机病毒的方法	电子商务系统安全 计算机病毒的概念及产生 计算机病毒的种类与识别
电子商务安全技术分析	1．能够运用“凯撒”密码算法进行加解密 2．能分析公开密钥密码体制下的文件保密传输和数字签名	电子商务信息安全要素 公开密钥密码体制 数字摘要 数字签名
CA 证书的申请与使用	1．能够在网上申请个人免费数字证书 2．能管理和使用个人免费数字证书	CA 认证中心 数字证书

【关键概念】

电子商务安全 计算机病毒 通用密钥密码体制 公开密钥密码体制 数字摘要 数字签名 CA 认证中心 数字证书

任务一：网络安全隐患分析与防范

一、案例学习

案例学习 8-1

少年网银大盗

2006 年 7 月份厦门市公安局网安处成功抓捕“新网银大盗”病毒作者刘某。犯罪嫌疑人刘某系厦门市某中专校在校生，被捕时年仅 16 岁。他通过攻陷网站种植木马的形式，盗窃某银行网上银行用户密码帐号，然后通过多次转账的形式提取现金。截止案发时，刘某已经窃取现金达 62500 余元。

该病毒将发作日期定于 2005 年 8 月 1 日，病毒通过记录用户键盘输入，盗取工行个人网上银行的帐号密码，并通过网页脚本把获得的非法信息提交给病毒作者。病毒运行后会创建 kv2005.dll 和 kvshell2005.dll 两个文件，企图伪装成杀毒软件程序欺骗普通电脑用户，事实上江民杀毒软件 KV2005 并无此程序。自从新网银木马被发现后，陆续有网民报告在网络上交易以后，账户上的钱常常莫名其妙地丢失。

据警方介绍， 16 岁时的刘某考上了厦门市某中专校。刘某平时不爱读书，整天泡在网上，玩些黑客的小程序，后来热衷玩灰鸽子木马，利用灰鸽子木马可全面地监控别人的电脑，中毒电脑中的任何信息都可以被随意控制甚至删除。当时只是觉得木马好玩，又有钱赚，就开始盗取别人网上银行账号，把别人卡上的钱转到自己卡上。

网银大盗最终没有给刘某带来金钱，却带走了他一生的前途。

案例分析 8-2：

电脑病毒历史

你可知道，电脑病毒的概念来自一场游戏？

电脑病毒的概念其实源起相当早，在第一部商用电脑出现之前好几年时，电脑的先驱者冯·诺伊曼（John Von Neumann）在他的一篇论文《复杂自动装置的理论及组识的进行》里，已经勾勒出病毒程序的蓝图。不过在当时，最早由冯·诺伊曼提出一种可能性----现在称为病毒，但没引起注意。

1977 年夏天，托马斯·捷·瑞安 (Thomas.J.Ryan) 的科幻小说《P-1 的春天》(The Adolescence of P-1) 成为美国的畅销书，作者在这本书中描写了一种可以在计算机中互相传染的病毒，病毒最后控制了 7,000 台计算机，造成了一场灾难。

1983 年 11 月 3 日，弗雷德·科恩 (Fred Cohen) 博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼 (Len Adleman) 将它命名为计算机病毒(computer viruses)，并在每周一次的计算机安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上运行，第一个病毒实验成功，一周后又获准进行 5 个实验的演示，从而在实验上验证了计算机病毒的存在。

1986 年初，在巴基斯坦的拉合尔 (Lahore)，巴锡特 (Basit) 和阿姆杰德(Amjad) 两兄弟经营着一家 IBM-PC 机及其兼容机的小商店。他们编写了 Pakistan 病毒，即 Brain。在一年内流传到了世界各地。

1988 年 11 月 2 日，美国六千多台计算机被病毒感染，造成 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，计算机系统直接经济损失达 9600 万美元。这个病毒程序设计者叫罗伯特·莫里斯 (Robert T.Morris)，当年 23 岁，是在康乃尔 (Cornell) 大学攻读学位的研究生。

二、相关知识

1．电子商务与网络安全

电子商务的发展给人们的工作和生活带来了很多的便利，也为人们带来无限商机。但许多商业机构对电子商务仍持观望态度，主要原因是对网上运作的安全问题存有疑虑，一旦信息失窃，企业的损失将不可估量。因此，在运用电子商务模式进行贸易的过程中，安全问题就成为电子商务最核心的问题，也是电子商务得以顺利推行的保障。

电子商务系统是一个计算机网络系统，其安全性是一个系统的概念，不仅与计算机系统结构有关，还与电子商务应用的环境、人员素质的社会因素有关。它包括电子商务系统的硬件安全、软件安全、运行安全、电子商务安全立法等。

安全是电子商务的核心和灵魂，没有安全保障的电子商务应用只是虚伪的炒作或欺骗，任何独立的个人或团体都不会愿意让自己的敏感信息在不安全的电子商务流程中传输。

2．计算机病毒的概念及产生

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码

病毒不是来源于突发或偶然的原因．一次突发的停电和偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的，病毒则是一种比较完美的，精巧严谨的代码，按照严格的秩序组织起来，与所在的系统网络环境相适应和配合起来，病毒不会通过偶然形成，并且需要有一定的长度，这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒是由人为故意编写的，多数病毒可以找到作者和产地信息，从大量的统计分析来看，病毒作者主要情况和目的是：一些天才的程序员为了表现自己和证明自己的能力，处于对上司的不满，为了好奇，为了报复，为了祝贺和求爱，为了得到控制口令，为了软件拿不到报酬预留的陷阱等．当然也有因政治，军事，宗教，民族．专利等方面的需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒。

3．计算机病毒的种类与识别

（1）蠕虫 它是一种短小的程序，这个程序使用未定义过的处理器来自行完成运行处理。它通过在网络中连续高速地复制自己，长时间的占用系统资源，使系统因负担过重而

瘫痪。如震荡波、冲击波、尼姆达、恶邮差等。

（2）逻辑炸弹 这是一个由满足某些条件（如时间、地点、特定名字的出现等）时，受激发而引起破坏的程序。逻辑炸弹是由编写程序的人有意设置的，它有一个定时器，由编写程序的人安装，不到时间不爆炸，一旦爆炸，将造成致命性的破坏。如欢乐时光，时间逻辑炸弹。

（3）特洛伊木马 它是一种未经授权的程序，它提供了一些用户不知道的功能。当使用者通过网络引入自己的计算机后，它能将系统的私有信息泄露给程序的制造者，以便他能够控制该系统。如 Ortyc.Trojan 木马病毒，木马 Backdoor.Palukka，酷狼，IE 枭雄，腾讯 QQ 木马病毒。

（4）陷阱入口 陷阱入口是由程序开发者有意安排的。当应用程序开发完毕时，放入计算机中，实际运行后只有他自己掌握操作的秘密，使程序能正常完成某种事情，而别人则往往会进入死循环或其他歧路。

（5）核心大战 这是允许两个程序互相破坏的游戏程序，它能造成对计算机系统安全的威胁。

互联网上存在很多的病毒，而且逐年成倍的增加。各个反病毒公司为了方便管理，按照病毒的特性，将病毒进行分类命名。虽然每个反病毒公司的命名规则都不太一样，但大体都是采用一个统一的命名方法来命名的。一般格式为：

<病毒前缀>.<病毒名>.<病毒后缀> 。

病毒前缀是指一个病毒的种类，是用来区别病毒的种族分类的。不同的种类的病毒，其前缀也是不同的。比如常见的木马病毒的前缀 Trojan ，蠕虫病毒的前缀是 Worm 等等还有其他的。

病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的“ CIH ”，振荡波蠕虫病毒的家族名是“ Sasser ”。

病毒后缀是指一个病毒的变种特征，是用来区别具体某个家族病毒的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指 振荡波蠕虫病毒的变种 B，因此一般称为 “振荡波 B 变种”或者“振荡波变种 B”。

下表例举了一些常见的病毒前缀的解释（针对我们用得最多的 Windows 操作系统）：

中文解释	病毒名	特征
系统病毒	Win32、PE、Win95、W32、W95	可以感染 windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如 CIH 病毒。
蠕虫病毒	Worm	通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络），小邮差（发带毒邮件） 等。
木马病毒	Trojan	通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息。
黑客病毒	Hack	有一个可视的界面，能对用户的电脑进行远程控制。病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能。
脚本病毒	Script 、VBS、JS	使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）
宏病毒	Macro	第二前缀是：Word、 Word97、 Excel、 Excel97 等。能感染

		OFFICE 系列文档，然后通过 OFFICE 通用模板进行传播
种植程序病毒	Dropper	运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN 射手(Dropper.Worm.Smibag)等。
破坏性程序病毒	Harm	本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化 C 盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。
玩笑病毒	Joke	本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户电脑进行任何破坏。如：女鬼（Joke.Girlghost）病毒。
捆绑机病毒	Binder、DoS、Exploit	使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。如：捆绑 QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。

三、任务与训练

1．任务

四川成都广贸发展有限公司是一家小型贸易公司，公司只有 8 位员工，公司的网上贸易和网络维护都由刚毕业的电子商务专业学生李明负责。最近李明发现公司的几台电脑纷纷中了病毒，而且次数很频繁。李明用杀毒软件扫描发现几个病毒名如下：

Backdoor.RmtBomb.12

Trojan.Win32.SendIP.15

Trojan.LMir.PSW.60

李明虽然用杀毒软件清除了病毒，但他还是不知道这些病毒的名称是什么，有什么特征，怎样才能预防公司电脑不再重复中毒。

现在请你帮助李明识别这三种病毒分别叫什么，有什么特征，并制定一个公司内部网络病毒防治计划。

2．分析思考

1） 公司内部网络组网模式是怎样的?

2） 公司电脑防毒软件是那种类型的？。

3） 公司电脑防毒软件升级期限是多久？是否开启 microsoft update 程序?

4） 公司电脑是否做系统和重要数据备份?

3．训练方法与步骤

1) 根据本教材的内容写出三种病毒的名称及特征。

2）安装杀毒软件，并进行升级时间设置。

3）开启操作系统的 microsoft update 程序。

4）下载与安装 GHOST XP 程序，为电脑系统盘和重要数据制作镜像文件。

5）查阅网站或相关资料，结合公司内部网络状况制订病毒防治计划。

4．任务训练结果与评价

1） 列表填写任务中的三种病毒名称及特征

病毒全称	病毒种类	病毒名	变种	特征
教师评语				

2）写出公司内部网络病毒防治计划。

预防电脑病毒计划	
查杀电脑病毒计划	
教师评语	

四、拓展任务

请在互联网上查找最近流行的计算机病毒及爆发时间。

任务二：电子商务信息安全技术分析

一、案例学习

案例学习 8-2

钓鱼网站窃取银行帐号密码

2005 年 2 月份发现的一种骗取美邦银行（Smith Barney）用户的帐号和密码的“网络钓鱼”电子邮件，该邮件利用了 IE 的图片映射地址欺骗漏洞，并精心设计脚本程序，用一个显示假地址的弹出窗口遮挡住了 IE 浏览器的地址栏，使用户无法看到此网站的真实地址。当用户使用未打补丁的 Outlook 打开此邮件时，状态栏显示的链接是虚假的。当用户点击链接时，实际连接的是钓鱼网站 http://**.41.155.60:87/s。该网站页面酷似 Smith Barney 银行网站的登陆界面，而用户一旦输入了自己的帐号密码，这些信息就会被黑客窃取。

案例分析 8-2

信息窃密案例

信息窃密指的是秘密地从某机构复制计算机信息并非法拿走它们。近些年来，国外已发生多次信息窃密活动。

日本某杂志社发行代理公司，将耗资 5 亿元收集到的订户名单等公司商业绝密信息委托给太平洋计算机中心处理，在转手处理过程中，其信息磁带被人转录，并以 82 万日元出手获利。

20 世纪 70 年代，美国太平洋安全银行雇佣的计算机上技术顾问，通过银行计算机，将一千多万美元转到瑞士苏黎世银行，构成美国当时最大的盗窃案。

俄罗斯一家贸易公司的计算机人员，通过计算机互联网络把纽约华尔街花旗银行计算机系统中的三家银行账户资金，转到他们在美国加利福尼亚州银行和以色列银行账户中，非法转账资金高达 1000 万美元。后来虽经客户银行发现并提出指控，警方将作案罪犯逮捕，追回 960 美元赃款，但此案以使人民警觉到 Internet 上的信息海洋并非安全之地，信息窃密活动随时可能侵入计算机网络

二、相关知识

1．电子商务信息安全要素

电子商务面临的威胁的出现导致了对电子商务安全的需求，真正实现一个安全电子商务系统所要求做到的各个方面主要包括保密性、完整性、认证性和不可抵赖性等。下面从几方面分析电子商务的安全要素。

（1）信息的保密性

保密性是指防止未授权的数据暴露。在电子商务环境下,信息直接代表着个人、企业或国家的商业机密，所以必须确保信息的严格保密。传统贸易都是通过邮寄信件或通过可靠的通信渠道（人员送抵）发送商业机密来达到保守机密的目的。电子商务是建立在开放的

网络环境上,防止非法的信息存取和信息在传输过程中被非法窃取就更为重要。

电子商务是建立在一个较为开放的网络环境上，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防信息大量传输过程中被非法窃取，必须确保只有合法用户才能看到数据，防止信息被窃看。

（2）信息的完整性

完整性是防止未授权的数据修改。电子商务减少了人为的干预,同时就带来维护贸易各方商业信息的完整、统一的问题。由于数据输入时的意外差错或欺诈行为,可能导致贸易各方信息的差异。此外,数据传输过程中的信息丢失、信息重复（有可能是恶意的）或信息传送的次序差异也会导致贸易各方信息的不同。必须保证数据信息的完整性才能保证合法商务活动的正常进行。

（3）信息的不可否认性

不可抵赖性是为了防止毁约。在传统的商务模式下，部分交易者由于利益原因可能会违约，发生抵赖行为。在电子商务环境下，非面对面的约束性显然没有传统商务模式强，所以对抵赖等行为更要通过管理、技术手段加以严格控制。

在电子商务环境中，一方发送了商务信息给另一方，就不能抵赖，就像在传统的商务环境下签订了合同一样，一旦完成就必须履行。可通过验证接收方收到的信息的真实性判断是否是发送方发送的信息，作为认证机构和专门的仲裁机构管理和裁决纠纷的依据。

（4）交易身份的真实性

真实性是确保发信息的数据源的真实性，即要确保与我们交易的个人或实体的身份可靠，正是它所声称的个人或实体。由于电子交易中各方并不是面对面的，因此必须设置一定的机制验证与我们交易的对方身份的真实性。

2．加密与解密

数据加密技术是保护信息安全的主要手段之一，它是结合数学、计算机科学、电子与通信等诸多科学于一身的交叉学科。它不仅具有保证信息机密性的信息加密功能，而且可以利用其基本原理进行数字签名、身份验证、系统安全等功能。使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确切性，防止信息被篡改、伪造和假冒。

密码技术的基本思想是伪装信息，隐藏信息的真实内容，以使未授权者不能理解信息的真正含义，达到保密的作用。具体的就是对信息进行一组可逆的数学变换。伪装前的信息称为明文（Plaintext），伪装后的信息称为密文（Ciphertext）。这种将信息伪装的过程称为加密（Encryption）。加密在加密密钥（key）的控制下进行。用于对数据加密的一组数学变换称为加密算法（Encryption Algorithm）。发信者将明文数据加密成密文，然后将密文传递，被授权的接受者收到密文后，进行与加密变换相逆的逆变换，即加密的逆过程，将密文再还原为明文，这一过程称为解密（Decryption）。解密是在解密密钥（key，只有拥有解密密钥才能对信息解密）的控制下进行的，用于解密的这组数学变换称为解密算法（Decryption Algorithm）。这样，数据不管是以密文的形式存储在计算机上还是在通信网络

中传递，即使被未授权者非法窃取或因为其他原因造成数据泄漏，未授权者也不能理解数据的真正含义，从而达到数据保密的目的。同样，未授权者也不能伪造合理的密文，因而不能篡改、伪造数据，从而达到确保数据真实性的目的。

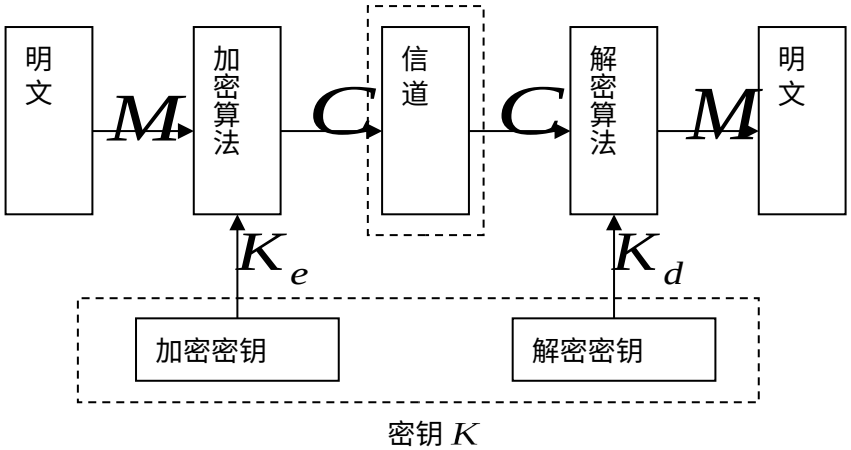

图 8-1 密码体制的构成

加解密必须要依赖于两个要素，算法和密钥。不管使用那一种密码技术进行安全保密，加解密算法都是相对固定的，一种密码技术对应一种加解密算法，真正保密性好的算法不多，而且如果在电子商务中使用过多种算法在存储和管理上也会非常烦琐，不利于交易各方通信。因此，多以使用相对单一的算法而变换密钥的方法实现加解密，所以密钥在密码体制中的作用举足轻重，加密系统的保密性不是取决于算法而是取决于密钥，包括密钥的长度、密钥的保密性等。根据密钥可以将密码体制分为通用密钥密码体制（也称对称密码体制）和公开密钥密码体制（也称非对称密码体制）。

通用密钥密码体制

通用密钥密码体制的加密密钥和解密密钥相同，或者虽然不相同，但是由其中一个可以很容易地推导出另一个。在这种体制中，信息拥有者和被授权者（接收者）拥有的为相同或可互推的密钥，就必须基于共同保守秘密来实现系统的保密性，若一方泄漏了密钥就必须停止该密钥的使用。

现以英语为例来说明使用凯撒密码方式的通用密钥密码体制原理：替换（substitution）加密算法。

替换加密算法，加密时每一个字母都给替换成另一个字母，例如：

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：q w e r t y u I o p a s d f g h j k l z x c v b n m

这样，apple 就被加密成 qhhat

上述例子中，密钥长度 26，如果单从密钥而言，加密强度是比较强的，因为密钥共有 26！个组合。但是这种方法实际上是十分容易破译的（只要密文长度适当），破译方法采用自然语言的统计特性，在英语中每一个字母有一定的出现频率，破译时只要对密文的每一个字母进行频率统计，对照自然语言的字母频率，就可以十分方便地进行破译。

公开密钥密码体制

数据加密中，有一个比较重要的问题需要解决，这就是密钥分配，即如何把密钥送到对方，由对方来进行解密。不管一个加密方法如何强壮，一旦解密密钥被入侵者获得，

那么加密也就没有意义。对于对称加密体制而言，加密密钥和解密密钥是相同的，这时产生一个两难的矛盾，一方面密钥必须受到保护，另一方面密钥必须分发给解密者，因为解密者必须用这个密钥来解密。

1976 年，美国斯坦福大学两位研究人员提出了一种全新密码体制，即公开密钥密码体制又叫非对称密钥体制，这个体制中必须具备以下条件：

a.加密密钥和解密密钥不同，解密密钥不能从加密密钥推算获得；

b.只有解密密钥是保密的，称为私人密钥（privete key）,加密密钥完全公开，称为公共密钥（public key）；

c.解密密钥和加密密钥是互解的关系。

使用该体制时，例如，与 X 秘密通信时，可以用 X 的公共密钥 Kex 生成密文 C=E（Kex,M）,伟输给 X，X 收到密文后，用只有自己知道的私人密钥，即保密的解密密钥 Kdx,计算出明文 M=K（Kdx,C）,用这种公开密钥密码体制，可以与任何对象秘密通信。

公开密钥密码体制的另一个优点是可以确认发送方的身份，即具有“数字签名”的功能。例如，接收方 Y 想在能信文上署名时，可以用自己的私人密钥 Kdy 生成署名文 V=D（Kdy,M）,然后，将 V 和自己的姓名 Ny 一起传输给对方。接送方从姓名 NY 检索出 Y 的公共密钥 Key,计算 M=E（Key,V）,如果复原的 M 文是有意义的信息，则可确认 Y 是合法的受信者，并确认通信途中未发生篡改信息的事件。利用 Internet 通信时，具有数字证书身份的人所持有的公共密钥可在网上查到，也可请对方在授信时主动将公共密钥传送过来，以方便信息的加、解密，从而保证在 Internet 网上传输信息的安全保密。

3．数字摘要

数字摘要（digital digest）也称安全 Hash(散列)编码法（SHA，secure hash algorithm）或 MD5（MD：standards for message digest）,由 Ron Rivest 所设计。

该编码法采用单向 Hash 函数将需加密的明文“摘要”成一串 128bit 的密文，这一串密也称为数字指纹（finger print）,它有固定的长度，且不同的明文摘要成密文，其结果总是不同的，而同样的明文其摘要必定一致。这样，这串摘要便可成为验证明文是否“真身”的“指纹”了。数字摘要的应用交易文件的完整性（不可修改性）得以保证。

4．数字签名

所谓数字签名（Digital Signature），也称为电子签名，是指利用电子信息加密技术实现在网络传送信息报文时，附加一小段只有信息发送者才能产生而别人无法伪造的特殊个人数据标记(数字标签)，代表发送者个人身份，起到传统书面文件的上手书签名或印章的作用，表示确认、负责、经手、真实作用等。

数字签名可以用来证明消息确实是由发送者签发的，它在要发送的信息报文上，附加一个特殊的且惟一个人数据标记，用来证明信息报文是由发送者发来的。

一个数字签名方案一般由两部分组成：签名算法和验证算法。其中，签名算法是秘密的，只有签名人知道，而验证算法是公开的，任何接收方都可进行验证。

把数字摘要和公钥算法这两种机制结合起来就可以产生所谓的数字签名。数字签名技术利用公开密钥加密算法和数字摘要技术，分别解决电子文件或信息报文网络传送与交换后的不可否认性与真实性，通俗地讲，就是防抵赖与防伪、防篡改。具体讲，数字签名的应用原理可以通过如下七步进行描述。如图 8-2 所示。

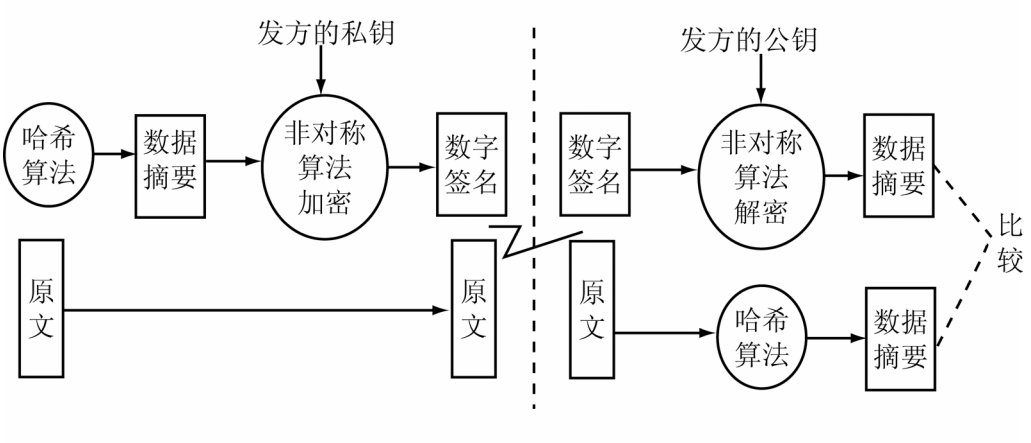

图 8-2 使用公钥密码体系的数字签名

(1)发送方利用数字摘要技术，使用单向 Hash 函数对信息报文进行数学变换，得到信息报文的数字摘要；

(2)发送方使用公开密钥加密算法，利用自己的私人密钥对数字摘要进行加密(数字签名)，得到一个特殊的字符串，称为数字标记，这个特殊的数字标记就是发送者加在信息报文上的数字签名；

(3)发送方把产生的数字签名附在信息报文（原文）之后，一同通过因特网发给接收方；

(4)接收方收到数字签名和信息报文（原文）。由于信息报文（原文）可能在传输过程中被篡改，接收方收到信息报文（原文）与发送方发送的信息报文（原文）可能有区别。

(5) 接收方收到附加签名的信息原文后，需验证对方的真实身份，接收方利用发送方的公开密钥对收到的对签名部分进行解密，得到数字摘要，并且由此确定发送方的确发来了他的数字标记，认证发送方的身份，其行为不可抵赖；

(6)接收方再将得到的信息报文（原文）利用单向 Hash 函数进行数学变换，产生信息报文的数字摘要；

(7)接收方比较数字摘要是否相同，如果相同，说明信息报文与信息报文是一致而真实的，数字签名有效，否则收到的信息报文不是发送方发送的真实报文，签名无效。

数字签名使接收方可以确认文件确实来自声称的发送方，并且鉴于签名私钥只有发送方自己保存，他人无法做一样的数字签名，因此他不能否认参与了交易。所以数字签名解决了信息的完整性和不可否认性问题。

在实际应用中，实现数字签名的方法有很多种，凡是能够确保数据的真实性的公开密钥密码都可用来实现数字签名，例如 RSA 密码、E1Gamal 密码、椭圆曲线密码等都可以实现数字签名。许多国际标准化组织都采用公开密钥密码数字签名作为数字签名标准，例如 1994 年颁布的美国数字签名标准 DSS，俄罗斯数字签名标准(GoST)等。著名的国际安全电子交易标准 SET 协议也采用 RSA 密码数字签名和椭圆曲线密码进行数字签名的。

三、任务与训练

1．任务

为了确定发送信息者的身份，商务数据传输的安全保密，需要采用电子签名技术（也称数字签名）。张明在网上下载了一个 ChinaTCP 个人控件数字签名系统 1.00 软件，用这个软件对公司的一份合同文本进行数字签名，请你帮助张明完成操作。

2．分析思考

1） 公司重要文件加密技术主要采用哪种密钥体制?

2） 公钥密码体系的数字签名的原理是什么?

3．训练方法与步骤

(1) 在 Windows 2000/XP 中安装 ChinaTCP 个人控件数字签名系统 1.00 软件并运行，如图 8.8 所示。

图 8.8 个人数字签名系统界面

(2) 单击“创建数字证书”按钮，创建一份数字证书，如图 8.9 所示。

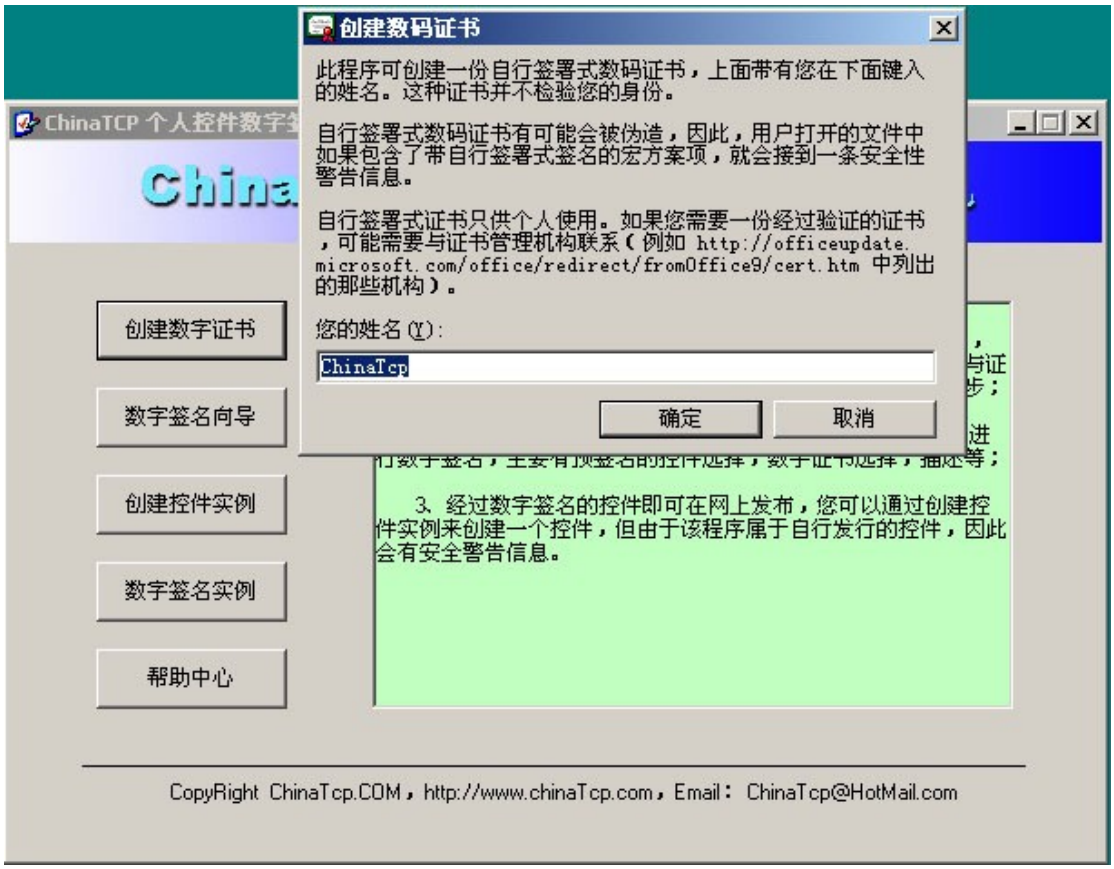

图 8.9 创建数码证书

创建证书成功,如图 8.10 所示.

图 8.10 成功创建证书

(3) 单击“数字签名向导”按钮，开始对控件进行数字签名，如图 8.11 所示。

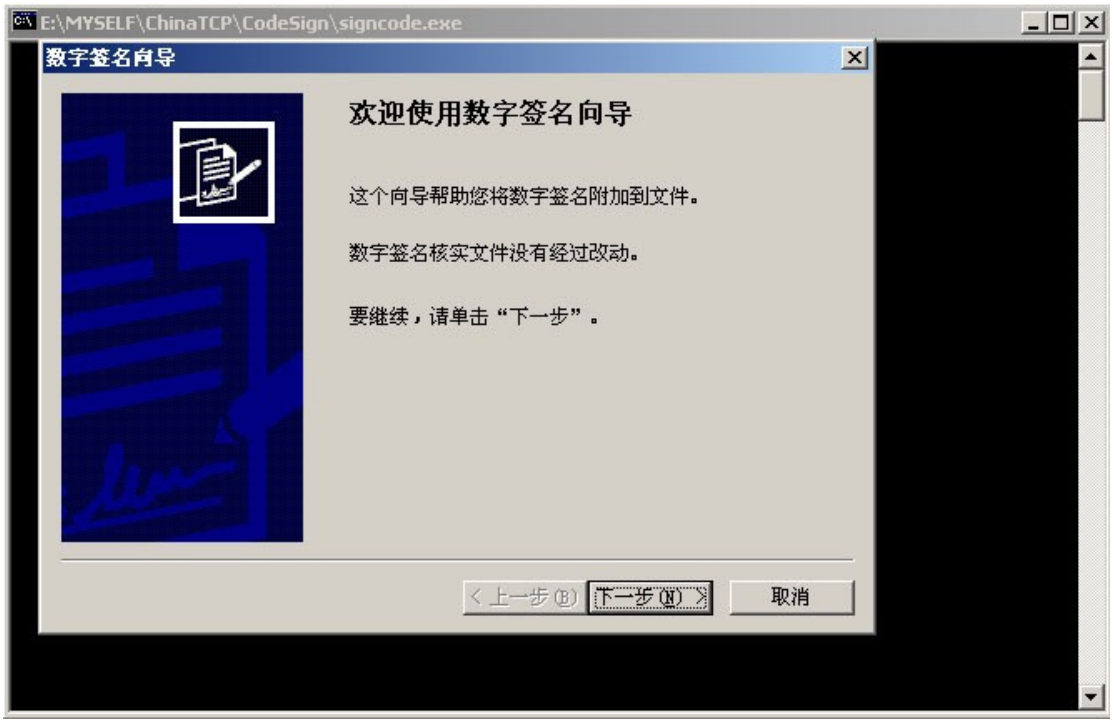

图 8.11 数字签名开始

(4) 单击“下一步”按钮，选择要进行数字签名的文件，如图 8.12 所示。

图 8.12 选择签名文件

(5) 单击“下一步”按钮进入下一个对话框，再单击“下一步”按钮又进入下一个对话框，单击“从存储区选择”按钮，在弹出的“选择证书”对话框中选择一个证书，如图 4.13 所示。

图 8.13 选择证书

(6) 单击“确定”按钮回到“数字签名向导”对话框再单击“下一步”按钮，添加正在签名的数据描述，如图 8.14 所示。

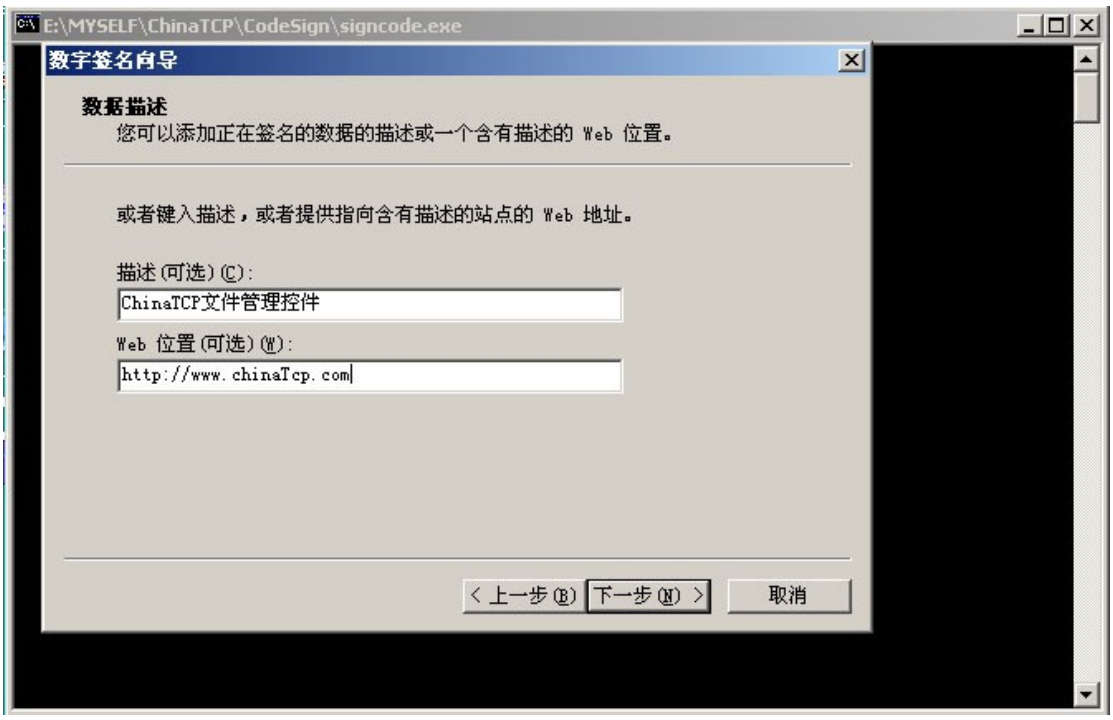

图 8.14 文件描述

(7) 完成数字签名，如图 8.15 所示。

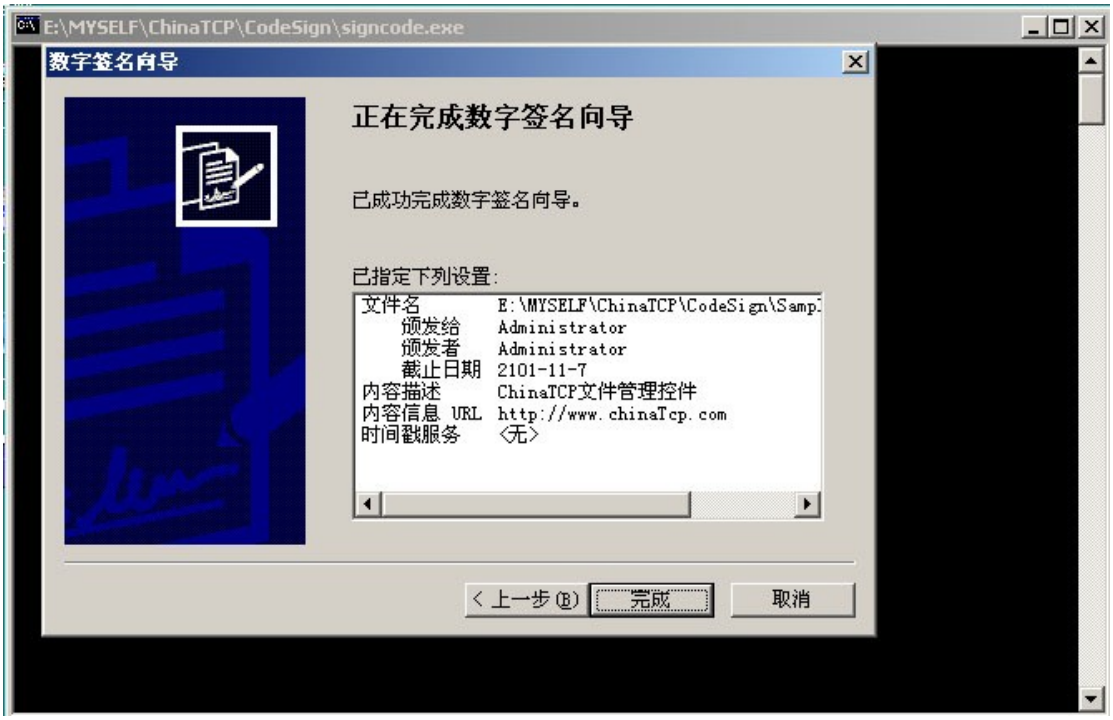

图 8.15 完成文件签名

3．任务训练结果与评价

分析比较通用密钥密码体制和公开密钥密码体制

项目	通用密钥密码体制	公开密钥密码体制
原理或条件		
密钥（位数）		
算法		
教师评语		

四、拓展任务

1、课余时间学习电脑设置密方式和方法：BIOS 密码、系统开机密码、系统登录帐户密码 、office 文档密码

2、在网上查找与下载单文件加密软件。

任务三：CA 证书的申请与使用

一、案例学习

案例学习 8-3

上海市数字认证中心

中国第一家专业的第三方网络安全和信任服务提供商------上海市数字认证中心（简称 SHECA），成立于 1998 年，专门从事信息安全技术认证和安全信任服务以及相关产品的研发和整合，以其领先的技术和精湛的服务为客户提供信息安全整体解决方案与第三方服务。

SHECA 提出“一证在手、走遍天下”的理念，联合北京、山东、安徽、天津和无锡、昆明等地的 CA 认证机构，成立了全国性的认证联合体——协卡认证体系（United Certification Authority），并在全国各个省、市、自治区设有近 400 家证书受理机构。并且，SHECA 为遍布全国的客户提供了复杂多样、满足需要的信息化安全解决方案和网络安全信任服务。

SHECA 是由上海市政府授权建立， 上海市唯一从事数字证书的签发和管理业务的权威性认证中心。SHECA 被有关部门称为“上海市信息安全别动队”，为上海的信息化事业提供安全和信任服务。

案例分析 8-3

《电子签名法》与《电子认证服务管理办法》

2005 年的 4 月 1 日对我国信息化的发展来说，意味着一个新时代的开始，因为从这一天起我国信息化将告别过去无法可依的历史，我国第一部电子商务相关法律----《电子签名法》正式出台。

与上海市数字认证中心一样，在《电子签名法》出台之前，我国已存在着很多家不同类型、各种性质的认证机构在从事着不同程度的电子认证服务，这些机构普遍存在着无法律规定、无标准规范、无主管部门的“三无”问题，急需对它们进行规范。

与《电子签名法》相配套，同样于 2005 年 4 月 1 日实施的还有《电子认证服务管理办法》。表面上看以信息产业部第 35 号部令形式出现的《电子认证服务管理办法》只是一部部门规章，但因为它是国家法律特别授权制定的，是与《电子签名法》配套同步实施，具有重要法律效力和作用，所以它又有别于一般的部门规章。

《电子认证服务管理办法》的制定与实施有其特殊的现实意义，表现在三个方面。

一是由于我国电子认证服务业还处于起步阶段，靠市场引导与行业自律的条件还不具备，政府部门有必要对从事电子认证服务的机构实施适度监督管理。

二是政府部门如何进行适度监管，还需要在实践中进行探索，要边实践边总结经验。

三是不能等到条件完全成熟后再出台相关法律，必须提前制定，以保证《电子签名法》的顺利实施。

二、相关知识

1．数字证书

数字证书是由权威公正的第三方机构即 CA 中心签发的，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。

数字证书采用公钥密码体制，即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一把仅为本人所掌握的私有密钥（私钥），用它进行解密和签名；同时拥有一把公共密钥（公钥）并可以对外公开，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，即使被第三方截获，由于没有相应的私钥，也无法进行解密。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。在公开密钥密码体制中，常用的一种是 RSA 体制。 用户也可以采用自己的私钥对信息加以处理，由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。采用数字签名能够确认以下两点：

(1)保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

(2)保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。

数字证书并将实体身份和公钥绑定。是网络通讯中标志通讯各方身份信息的一系列数据，提供了一种在 internet 上验证身份的方式。其作用类似于司机的驾驶执照和日常生活中的身份证。它是由一个由权威机构-----CA 机构，又称为证书授权(Certificate Authority)中心发行的，人们可以在交往中用它来识别对方的身份。 数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间，发证机关(证书授权中心)的名称，该证书的序列号等信息，证书的格式遵循 ITUT X.509 国际标准。

数字证书的工作原理，就是信息接收方在网上收到发送方发来的业务信息的同时，

还收到发送方的数字证书，这时通过对其数字证书的验证，可以确认发送方的真实身份。在发送方与接收方交换数字证书的同时，双方得到对方的公开密钥。由于公开密钥是包含在数字证书中的，且借助证书上数字摘要的验证，确信收到的公开密钥肯定是对方的。通过这个公开密钥，双方就可完成数据传送中的加／解密工作。

数字证书主要包括以下内容：

(1) 版本信息(Version)：用来区分 X．509 证书格式的版本；

(2) 数字证书序列号, 每个证书的序列号是惟一的；

(3) 有效使用期限，包括起始、结束日期；

(4) 证书颁发者信息：包括颁发数字证书的单位及其数字签名；

(5) 证书与公钥的使用者的相关信息，包括证书拥有者的姓名，证书拥有者的公钥；

(6) 公钥信息，包括公开密钥加密体制的算法名称、公钥的有限期。

(7)发行数字证书的 CA 签名与签名算法，用以验证数字证书是否是由该 CA 的签名密钥签署的，以保让证书的真实性与内容的真实性。

数字证书由发证机构——数字证书认证中心(CA)发行。该机构负责在发行数字证书之前，证实个人或组织身份和密钥所有权。一般情况下，证书要由社会上公认的公正的第三方的可靠组织发行。如果它签发的证书造成不恰当的信任关系，该组织就要承担责任。图 8-16 所示某网络公司服务器证书的内容页。

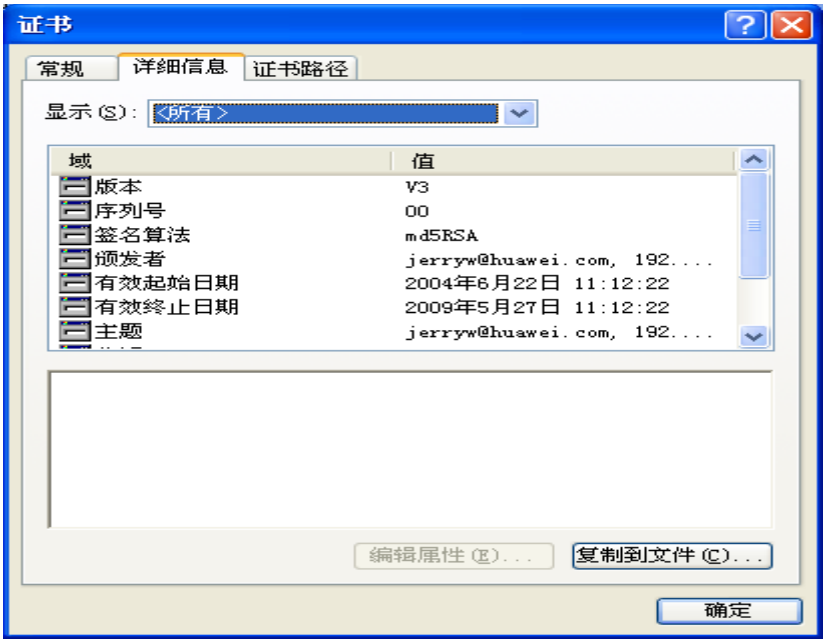

图 8-16 网络服务器证书的内容页

数字证书方要通过 CA 中心来验证真伪，并逐级往上验证各级认证机构数字证书的真伪。各级认证机构是按根认证机构(Root CA)、品牌认证机构(Brand CA)以及持卡人、商户或收单银行支付网关认证机构由上而下按层次结构建立的。

数字证书根据使用者不同分为个人证书、服务器证书、支付网关证书和认证中心证书。

(1)个人证书

个人证书即客户证书，也是持卡人证书，它主要证实客户的身份和密钥所有权。在网络支付时，为了取得客户证书，用户可向某个 CA 中心申请，CA 经过审查后决定是否向客户颁发客户证书。例如，工商银行直接向自己的网络银行客户颁发客户证书，其证书中包含客户的身份信息、公开密钥及工商银行的签名，并可以存储在软盘、硬盘、IC 卡、USB 盘中。

(2)服务器证书

服务器证书即网络站点证书，它主要证实银行或商家业务服务器的身份和公开密钥。当客户收到证书后，客户检查证书是由哪家 CA 中心发行的，这家 CA 是否被客户所信任。如果客户不信任这家 CA，浏览器提示用户接受或拒绝这个证书。在 IE 浏览器里，客户可以设置总是接受某个站点的证书，如你的开户网络银行的证书。这样，该站点的证书被存放在客户计算机的数据库里，客户可以随时查看这些证书。

(3)支付网关证书

如果在网络支付时利用第三方的支付网关，那么这个第三方要为支付网关申请一个数字证书，以证实自己的身份。

(4)认证中心 CA 证书

CA 是数字证书的认证中心，一样需要拥有自己的数字证书，证实其 CA 的真实身份。在客户浏览器里，用户可以看到浏览器所接受的 CA 证书，也可选择是否信任这些证书。在服务器端，管理员可以看到服务器所接受的 CA 证书，也可选择是否信任这些证名。

数字证书是由用户向认证中心申请的，认证中心是有权威性、可信赖性和公正性的第三方机构，负责发放和管理用户的数字证书。证中心在发放证书时要遵循一定的准则。如保证所发证书的序号各不相同，不同实体所申请的证书的主体内容不一致，不同主体内容的证书所包含的公开密钥各不相同。

数字证书的申请步骤是：用户向认证中心提出申请证书，并说明自己的身份，提供有关证明材料。认证中心在验证用户身份和核实证明材料后，向用户发放数字证书。

证书管理的管理也是由认证中心来完成的，管理功能包括：用户能够方便地查找各种证书，包括已经撤销的证书，根据用户请求或证书的有效期撤销用户证书，完成证书数据库的备份工作，并有效地保护证书和密钥服务器的安全，特别是认证中心的签名密钥不被非法使用。

因为证书是不可伪造的，因此无需对存放证书的目录施加特别的保护。如果所有用户都由同一认证中心签署证书，则这一认证中心就必须取得所有用户的信任。用户证书除了能放在目录中供他人访问外，还可以由用户直接把证书发给其它用户。如果用户数量极多则仅一个认证中心是不够的，通常应有多个认证中心，每个认证中心为一部分用户发行、签署证书。所有认证中心以层次结构组织起来，这样任意用户都可从层次结构组织中得到相应的证书。

从证书的格式上我们可以看到，每一证书都有一个有效期，然而有些证书还未到截止日期就会被发放该证书的 CA 吊销，这可能是由于用户的秘密密钥已被泄漏，或者该用户不

再由该 CA 来认证，或者 CA 为该用户签署证书的秘密密钥已经泄露。为此，每一 CA 还必须维护一个证书吊销列表 CRL(Certificate Revocation List)，其中存放所有未到期而被提前吊销的证书，包括该 CA 发放给用户和发放给其它 CA 的证书。CRL 还必须由该 CA 签字，然后存放于目录中以供他人查询。

CRL 中的数据域包括发行者 CA 的名称、建立 CRL 的日期、计划公布下一 CRL 的日期以及每一被吊销的证书数据域。被吊销的证书数据域包括该证书的序列号和被吊销的日期。对一个 CA 来说，它发放的每一证书的序列号是惟一的，所以可用序列号来识别每一证书。

所以每一用户收到他人消息中的证书时，都必须通过目录检查这一证书是否已被吊销，为避免搜索目录引起的延迟以及因此而增加的费用，用户自己也可维护一个有效证书和被吊销证书的局部缓存区。

数字证书可以应用于公众网络上的商务活动和行政作业活动，包括支付型和非支付型电子商务活动，其应用范围涉及需要身份认证及数据安全的各个行业，包括传统的商业制造业、流通业的网上交易，以及公共事业、金融服务业、工商税务海关、政府行政办公、教

育科研单位、保险、医疗等网上作业系统。

2.CA 认证中心

CA (Certification Authority)是认证机构的国际通称，它是对数字证书的申请者发放、管理、取消数字证书的机构。CA 的作用是检查证书持有者身份的合法性，并签发证书(用数学方法在证书上签字)，以防证书被伪造或篡改。CA 认证是顺应我国电子商务和电子政务的发展应运而生的。随着网上银行的普遍应用和在线支付手段的不断完善，网上交易已经变得越来越大众化，安全问题就显得日益重要。而网络间的身份认证成为根本。认证机构相当于一个权威可信的中间人，它的职责是核实交易各方的身份，负责电子证书的发放和管理。理想化的状态是，上网的每一个企业或者个人都要有一个自己的网络身份证作为唯一的识别。而这些网络身份证的发放、管理和认证就是一个复杂的过程，也就是所谓的 CA 认证。

CA 的建立并不是任何一个组织想建立就能建立起来的。除了作为第三方所要求的保持公正和具备良好信誉之外，关键是 CA 的建立与运作需要强大的技术支撑，因为这涉及许多先进的密码技术。比如，CA 提供的公开密钥与数字摘要机制等必须是先进的，密钥的位数必须达到一定长度，以保证 CA 及其发行的证书的安全可靠，并且在服务质量与认证速度、管理机制上均需达到很高的水平。到目前为止，我国的电子商务以及网络支付没有得到大规模普及发展的一个重要原因就是还没有建立起高水平的跨区域的认证中心。近些年各个地方建立了一些 CA，但规模均较小，没有得社会的普遍信赖。

CA 的技术基础是 PKI(Public Key Infrastructure)体系,即公开密钥体系或公开密钥基础，是一种遵循既定标准的密钥管理平台，能为所有网络应用服务提供加密和数字签名等密码服务及其必需的密钥和证书管理体系。PKI 利用公钥理论和技术建立网络安全服务的基础设施，PKI 技术是信息安全技术的核心，也是电子商务交易与网络支付的关键和基础技术。PKI 的基础技术包括加密、数字签名、数字摘要、数字信封、双重数字签名等。一个完整的 PKI 系统的基本构成包括权威的认证中心 CA，数字证书库，密钥备份及恢复系统，证书作废系统，应用接口等。

CA 作为数字证书的签发与管理机构，公开密钥的承载者，是 PKI 的核心。密码服务系统的核心内容是实现密钥管理。公钥体制涉及一对密钥，私人密钥只由用户独立掌握，无需在网上传输；而公开密钥则是公开的，需要在网上传送。故公钥体制的密钥管理主要是针对公钥的管理问题，目前较好的解决方案是数字证书这种密钥管理。

（一）认证分级体系

在实际应用中，一个 CA 很难得到所有用户的信任，并且接收它所发行的数字证书。而且，也不可能一个 CA 就对所有的用户了解，掌握每一个需要数字证书的用户的情况。因此，在现实的电子商务安全系统中，有很多的 CA 从事身份认证和证书发放的工作。这就有必要在这些 CA 之间建立起可以相互信赖的关系，通过它才能建立起可信赖的数字证书链，使拥有不同 CA 颁发的证书的用户可以相互认证，保证终端用户的安全和交易的方便性。

层次树状结构是一种较好的对 CA 进行管理的理论结构。将用户作为树的端节点，这些端节点又分为几个组，每组有一个上级节点作为可信赖的机构（CA），这些节点又可以分为几组，每一个组都有其上级节点作为可信赖的机构，以此类推，最后到达根结点，也就是最高级别的认证中心。在这种结构中任意两个端节点都可以形成一个有效的相互认证。认证数字证书就是通过这种信任分级体系来验证的，每一个数字证书与签发它的 CA 联系，这个 CA 又与其上一级 CA 相连，沿着这条线路就可以找到一个交易各方都信任的组织，就可以确定证书的有效性。

SET（安全电子交易）体系是为在网上购物时用银行卡来进行结算类业务而建立的，如图 8-17，这种结构分为三层：

第一层为根 CA，即 Root CA，简称为 RCA。它负责制定和审批 CA 的总政策，签发并管理第二级 CA 证书，与其他的 RCA 进行交叉认证。

第二层 CA 为品牌 CA,Brand CA，简称 BCA。为各个商业银行所发放的不同信用卡品牌发放证书。它的职责是根据 RCA 的各种规定和总政策，制定具体的政策、管理制度和运行规范。安装 RCA 为其签发的证书，并为下一级 CA 签发证书，管理证书及管理证书撤销列表。

第三层 CA 为终端用户 CA，End user CA，简称 ECA。为 SET 电子商务参与各实体颁发证书，即为支付网关（Payment Gateway）、商家（Merchant）及持卡人（Cardholder）签发证书，签发这三种证书的对应 CA 为 PCA、MCA、CCA。

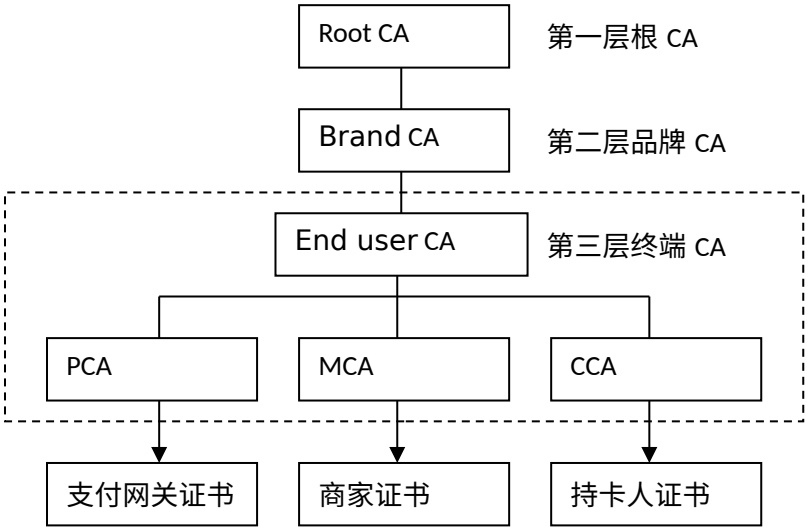

图 8-17 SET CA 体系结构

（二）认证中心功能

CA 在整个公钥加密体制以及安全的网络支付过程中的地位是至关重要的。其主要功能包括八个方面：

(1)生成 CA 证书及公共密钥对

CA 要向申请证书各方颁发证书，同时生成公钥体系中自己的密钥对，并对私钥进行有效的保护，以在签名的使用。已经建立的或正在建立的 CA 系统，很多都是自成体系的，这样的 CA 系统不仅做根 CA，还做品牌 CA、持卡人 CA、商家 CA 和网关 CA。作为自成体系的、封闭的 CA 系统，CA 必须生成自己的根密钥对，且在此基础上生成根证书，就可以为各级 CA 以及客户生成证书，保证证书持有者有不同的密钥对。

(2)验证申请人身份

网络上进行信息交换各方，如电子支付中的持卡人、商家、支付网关等，在向 CA 申请数字证书时，CA 必须对其真实的身份进行认证，防止数字证书被冒领。因此 CA 有一套严密的身份认证流程。

(3)颁发数字证书

CA 系统的主要任务就是颁发数字证书。CA 系统必须能在 Internet 上接收证书申请，在签名验证申请者的真实身份并且通过资格检查后，有 CA 签名的申请者的数字证书将通过 Internet 发送给申请者。

证书的发放也有通过离线方式的，比如 CA 将申请者的数字证书加密后放入软盘或 IC 卡等载体，由证书申请者亲自到 CA 机构领取，再用特定的方法，将数字证书装入自己的计算机应用系统中。如招商银行企业网络银行目前采用的 IC 卡证书发放方式就是这样。

(4)证书以及持有者身份认证查询

利用 CA 服务器，用户可在线查询证书的生成情况，也可在线认证证书持有者，CA 必

须保证 24(小时)×365(天)的跨区域服务，并且要有足够的带宽，保证较快的查询速度。

(5)证书管理及更新

CA 要及时记录所有颁发的证书以及所有被吊销的证书，使得证书失效以后能及时更新数字证书。

(6)吊销证书

CA 根据证书持有者的应用情况，可在数字证书有效期内使其无效，并且公布于众 。CA 系统能生成被吊销证书黑名单，证书黑名单中包括被废除的分支 CA 数字证书和网关的数字证书。这些证书黑名单通过在线发给持有证书的种类用户。

(7)制定相关政策

CA 的政策是指 CA 必须对信任它的事务各方负责，它的责任大部分体现在政策的制定和实施上。CA 的政策越公开越好，信息发布越及时越好。CA 除了拥有先进的技术和雄厚的实力之外，还应具有良好的政策，这样才能受到不同用户的信任。

(8)有能力保护数字证书服务器的安全

CA 必须有能力采取相应措施保证其数字证书服务器的安全性，如加强对系统管理员的管理，加强对防火墙保护等。否则，其提供的数字证书服务的安全就无从说起。

三、任务与训练

1．任务

陈斌是电子商务专业大一的学生，他在上了互联网技术基础这门课之后，知道了原来自己发送和接收到的 E-mail 邮件都存放在提供免费服务的邮件服务器上，看似非常的不安全，于是他想下载一个免费邮件数字证书来保护电子邮件的安全。请你帮他完成操作。

2．分析思考

1） 电子邮件的传输原理是什么。

2） 数字证书的用途有哪些?

3） 数字证书有时效性吗?

3．训练方法与步骤

(1) 打开中国数字认证网(http://www.ca365.com)，安装 ActiveX 控件，如图 8.18 所示。

图 8.18 中国数字认证网界面

安装 ActiveX 控件的对话框，如图 8.19 所示。

图 8.19 安装控件

(2) 在网页上单击“如果您是第一次访问本站点请下载并安装根 CA 证书”超链接，弹出“文件下载-安全警告”对话框，如图 8.20 所示。

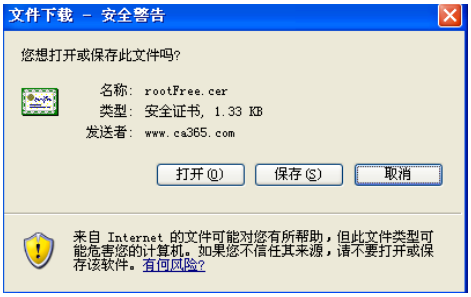

图 8.20 安装根 CA 证书

如图 8.21 所示，根证书安装成功。

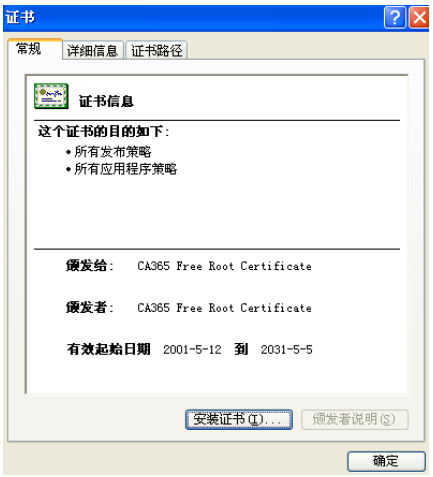

图 8.21 证书信息

(3) 安装根证书后，在网页上单击“用表格申请证书”超链接，如图 8.22 所示。

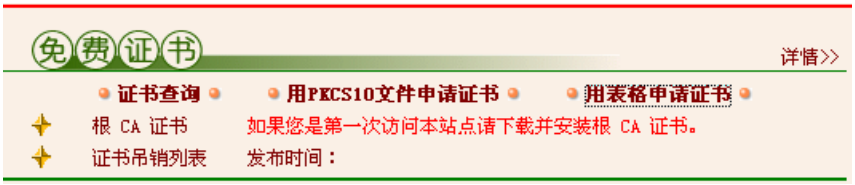

图 8.22 申请证书

(4) 进行注册，单击“提交”按钮，如图 8.23 所示。

图 8.23 申请人注册信息

(5) 认证中心创建 RSA 交换密钥，单击“确定”按钮，如图 8.24 所示。

图 8.24 创建交换密钥

(6) 证书产生，如图 8.25 所示。

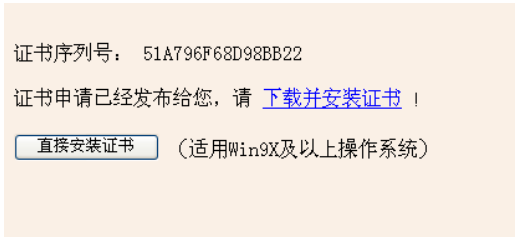

图 8.25 成功产生证书

可以看到证书信息，如图 8.26 所示。

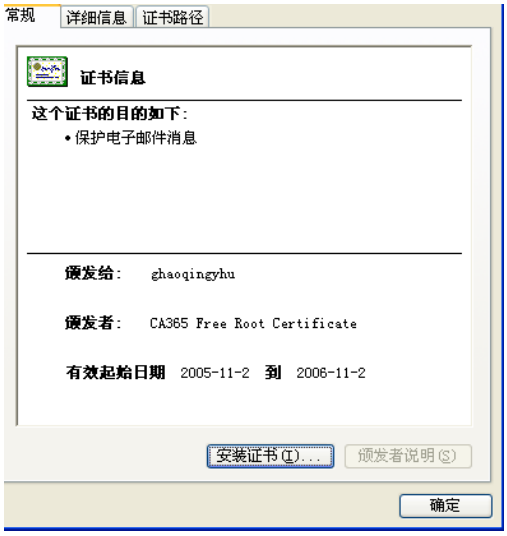

图 8.26 证书信息

（说明：要有效地申请数字证书，需要缴纳费用。它是你在网上交易的身份，同时能保护电子邮件的安全。）

4．任务训练结果与评价

登录中国数字认证网，申请个人数字证书，并将步骤记录下来。

网站网址	
申请步骤	

密码信封序列号	
证书有效时间	
证书是否下载安装	

四、拓展任务

请搜索和访问其他的数字证书管理网站，并尝试下载免费证书。