第 3 章　数字签名技术与应用

对文件进行加密只解决了传送信息的保密问题，而防止他人对传输的文件进行破坏以及如何确定发信人的身份还需要采取其他的手段，这一手段就是数字签名。在电子商务安全技术中，数字签名技术有着特别重要的地位，在电子商务安全服务中的源鉴别、完整性服务、不可否认服务中，都要用到数字签名技术。

并且，数字签名经过长时间的研究，已经有了自己的研究体系，并形成了各自的理论框架，目前数字签名的研究内容非常丰富，既有 RSA、椭圆曲线等经典签名，也出现了盲签名、代理签名、团体签名、不可否认签名、双联签名、不可否认签名、具有消息恢复功能的签名等与具体应用环境密切相关的特殊签名。

如果说公开密钥技术和数字签名是电子商务安全的基础，那么数字证书则是将这些技术广泛地应用于大型的、全球性的电子商务的关键。因此，本章也将会围绕数字证书的相关问题展开讨论。

数字签名的应用还涉及到法律问题，联合国已经出台了电子签名示范法，法国、美国等几十个国家颁布了各自的电子签名法。我国也于 2005 年正式实施电子签名法。

本章主要介绍：数字签名的基本原理，常规和特殊数字签名方法，美国数字签名标准、数字证书技术以及数字签名相关法律。

3.1　数字签名的基本原理

数字签名其实是伴随着数字化编码的消息一起发送并与发送的信息有一定逻辑关联的数据项，借助数字签名可以确定消息的发送方，同时还可以确定消息自发出后未被修改过。数字签名的整个过程如图 3.1 所示。

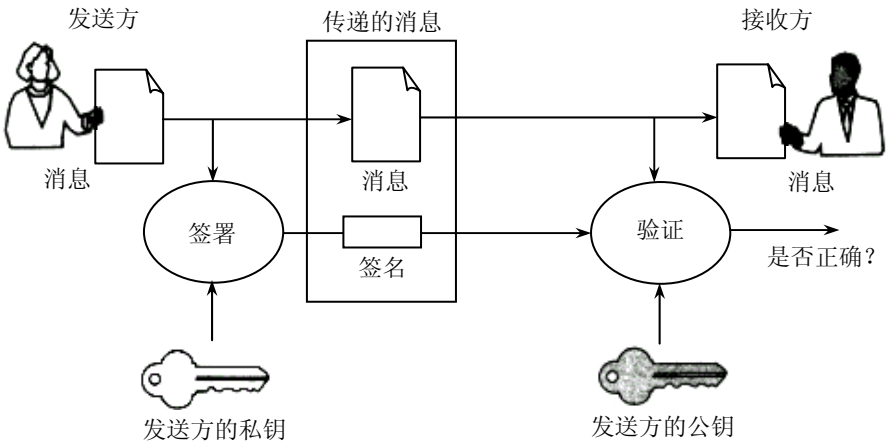

图 3.1　数字签名

在该过程中，发送方用自己的私有密钥进行签署，由此产生签名，接收方则用发送方的公开密钥进行验证操作。借此，接收方能确信所收到的信息确实是由发送方发出的，而且在发送方发出该信息后相应的内容未被篡改过。在电子商务中，利用这样的数字签名机制，交易中接收订单的一方可以对发送方发出的订购要求进行验证，确认该订单不是由不怀好意的网上黑客伪造的。

从某些方面来说，数字签名类似于消息验证码（MAC），但它们也有不同之处。最主要的不同在于，数字签名可以支持不可否认服务，也就是说，消息的接收方可以用数字签名来证明发送方身份。如果用数字签名来解决电子商务交易中发送方与接收方在交易信息上的争端，则最可能得到伪造信息的一般都是接收方，所以对接收方来说，应该不能生成与发送方所生成的签名信息一样的数字签名。但 MAC 不具有进行数字签名的功能，因为接收方知道用于生成 MAC 的密钥。数字签名机制克服了 MAC 的弱点，可以利用公开密钥技术来建立。

3.1.1　数字签名的要求

政治、军事、外交等领域的文件、命令和条约，商业中的契约以及个人之间的书信等，传统上都采用手书签名或印章，以便在法律上能认证、核准和生效。随着计算机通信网的发展，人们希望通过电子设备实现快速、远距离的交易，数字（或电子）签名法便应运而生，并开始用于商业通信系统，如电子邮递、电子转账和办公自动化等系统中。

类似于手书签名，数字签名也应满足以下要求：

（1）收方能够确认或证实发方的签名，但不能伪造。

（2）发方发出签名的消息送收方后，就不能再否认他所签发的消息。

（3）收方对已收到的签名消息不能否认，即有收到认证。

（4）第三者可以确认收发双方之间的消息传送，但不能伪造这一过程。

3.1.2　数字签名的分类

数字签名是许多现代验证协议的基础。客户端通过签署某个协议信息，或在信息的某个字段中使用密钥，来证明拥有某个特定的私人密钥。在签名数据中可以包含提问值或时间戳，由此来防止重放攻击。

根据不同的标准，数字签名方案有不同的分类方法。

1. 基于签字内容的分类

可分为两种：一种是对整体消息的签字，它是消息经过密码变换的被签消息整体；一种是对压缩消息的签字，它是附加在被签字消息之后或某一特定位置上的一段签字图样。

若按明、密文的对应关系划分，每一种中又可分为两个子类：一类是确定性数字签名，其明文与密文一一对应，它对一特定消息的签字不变化（使用签名者的密钥签名），如 RSA 签名；另一类是随机化的或概率式数字签名，它对同一消息的签字时随机变化的，取决于签字算法中的随机参数的取值。一个明文可能有多个合法数字签名，如 ElGamal 等。

2. 基于数学难题的分类

根据数字签名方案所基于的数学难题，可分为：

（1）基于离散对数问题的签名方案。如 ElGamal 型数字签名方案和美国数字签名算法（DSA）。

（2）基于素因子分解问题的签名方案。如 RSA 数字签名方案。二次剩余作为素因子分解

问题的特殊情况，当前也发展了好几种基于二次剩余的签名方案，如 Rabin 数字签名方案和 1997 年 Nyang 和 Song 所设计的快速数字签名方案等。

（3）上述两种的结合签名方案。如 1994 年 Harn 设计的一种数字签名方案；1997 年 Laih 和 Kuo 设计的一种新的数字签名方案。

3. 基于签名用户的分类

根据签名用户的情况，可将数字签名方案分为单个用户签名的数字签名方案和多个用户的数字签名方案。

4. 基于数字签名所具有特性的分类

根据数字签名方案是否具有消息自动恢复特性，可将之分为：

（1）不具有自动恢复特性的数字签名方案。一般数字签名不具有此特性，如 EIGamal 数字签名。

（2）具有消息自动恢复特性的数字签名方案。1994 年，Nyberg 和 Ruepple 首次提出一类基于离散对数问题的具有消息恢复特性的数字签名方案。

5. 基于数字签名所涉及的通信角色分类

根据数字签名所涉及的通信角色可分为直接数字签名（仅涉及通信的源和目的两方）和需仲裁的数字签名（除通信双方外，还有仲裁方）。

3.1.3 数字签名的使用

安全的数字签名使接收方可以确认文件确实来自声称的发送方。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，因此他不能否认他参与了交易。

数字签名的加密解密过程和私有密钥的加密解密过程正好相反，使用的密钥对也不同。数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密。这是一个一对多的关系：任何拥有发送方公开密钥的人都可以验证数字签名的正确性。而私有密钥的加密解密则使用的是接收方的密钥对，这是多对一的关系：任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有惟一拥有接收方私有密钥的人才能对信息解密。在实际应用过程中，通常一个用户拥有两个密钥对，另一个密钥对用来对数字签名进行加密解密，一个密钥对用来对私有密钥进行加密解密。这种方式提供了更高的安全性。

在实际运用中，直接用公开密码的私钥对文件进行签字并不完全可行，如需对相当长的文件进行签名认证怎么办？若将文件按比特划分成一块一块，用相同的密钥独立地签每一个块，这样速度太慢。

通常的解决办法是引入可公开的密码散列函数（Hash function，也叫摘要函数、哈希函数）。它将取任意长度的消息做自变量，结果产生规定长度的消息摘要。如数字签名标准 DSS 中的消息摘要为 160bit，然后签名消息摘要。它发生在签名后、加密前，对邮件传输或存储都有节省空间的好处。

利用散列函数进行数字签名和验证的文件传输过程如下：

（1）发送方首先用哈希函数从原文得到数字摘要，然后采用公开密钥体系用发送方的私有密钥对数字摘要进行签名，并把签名后的数字摘要附加在要发送的原文后面。

（2）发送一方选择一个秘密密钥对文件进行加密，并把加密后的文件通过网络传输到接收方。

（3）发送方用接收方的公开密钥对秘密密钥进行加密，并通过网络把加密后的秘密密钥传到接收方。

（4）接收方使用自己的私有密钥对密钥信息进行解密，得到秘密密钥的明文。

（5）接收方用秘密密钥对文件进行解密，得到经过加密的数字摘要。

（6）接收方用发送方的公开密钥对数字签名进行解密，得到数字摘要的明文。

（7）接收方用得到的明文和哈希函数重新计算数字摘要，并与解密后的数字摘要进行对比。如果两个数字签名是相同的，说明文件在传输过程中没有被破坏。

上述流程可用图 3.2 表示。

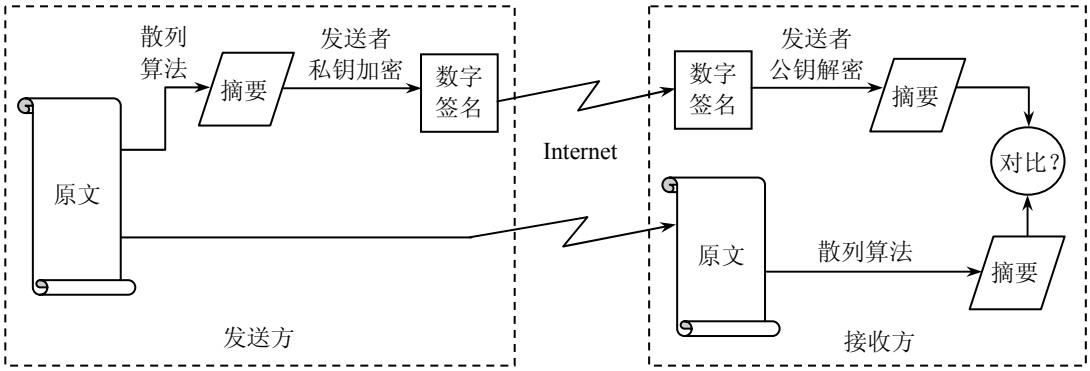

图 3.2　数字签名过程

如果第三方冒充发送方发出了一个文件，因为接收方在对数字签名进行验证时使用的是发送方的公开密钥，只要第三方不知道发送方的私有密钥，解密出来的数字签名和经过计算的数字签名必然是不相同的。这就提供了一个确认发送方身份的方法。

随着计算机网络的发展，过去依赖于手书签名的各种业务都可用这种电子化的数字签名代替，它是实现电子贸易、电子支票、电子货币、电子出版及知识产权保护等系统安全的重要保证。数字签名已经并将继续对人们如何共享和处理网络上信息以及事务处理产生巨大的影响。

例如，在大多数合法系统中对大多数合法的文档来说，文档所有者必须给一个文档附上一个时间标签，指明文档签名对文档进行处理和文档有效的时间与日期。在用数字签名对文档进行标识之前，用户可以很容易地利用电子形式为文档附上电子时间标签。因为数字签名可以保证这一日期和时间标签的准确性和证实文档的真实性，数字签名还提供了一个额外的功能，即它提供了一种接收者可以证明确实是发送者发送了这一消息的方法。

使用电子汇款系统的人也可以利用电子签名。例如，假设有一个人要发送从一个账户到另一个账户转存 10000 美元的消息，如果这一消息通过一个未加保护的网络，那么“黑客”就能改变资金的数量从而改变这一消息。但是，如果发送者对这一消息进行数字签名，由于接收系统核实错误，从而识别出对此消息的任何改动。

大范围的商业应用要求变更手书签名方式时，可以使用数字签名。其中一例便是电子数据交换（EDI）。EDI 是商业文档消息的机对机交换机制。美国联邦政府用 EDI 技术来为消费者购物提供服务。在 EDI 文档里，数字签名取代了手写签名，利用 EDI 和数字签名，只须通过网络介质即可进行买卖并完成合同的签订。

数字签名的使用已延伸到保护数据库的应用中。一个数据库管理者可以配置一套系统，它要求输入消息到数据库的任何人在数据库接收之前必须数字化标识该消息。为了保证真实性，系统也要求用户标识对消息所作的任何修改。在一个用户查看已经标识过的消息之前，系统将核实创建者或编辑者在数据库消息中的签名，如果签名核实结果正确，用户就知道没有未经授权的第三者改变这些消息。

3.1.4 数字签名与手写签名的区别

数字签名与手书签名的区别在于，手书签名是模拟的，且因人而异。数字签名是 0 和 1 的数字串，因消息而异。数字签名与消息认证的区别在于，消息认证是收方能验证消息发送者及所发消息内容是否被篡改过。当收发者之间没有利害冲突时，这对于防止第三者的破坏来说是足够了。但当收者和发者之间有利害冲突时，单纯用消息认证技术就无法解决他们之间的纠纷，此时需借助满足前述要求的数字签名技术。

为了实现签名目的，发方须向收方提供足够的非保密信息，以便使其能验证消息的签名。但又不能泄露用于产生签名的机密信息，以防止他人伪造签名。因此，签名者和证实者可公用的信息不能太多。任何一种产生签名的算法或函数都应当提供这两种信息，而且从公开的信息很难推测出用于产生签名的机密信息。再有，任何一种数字签名的实现都有赖于精心设计的通信协议。

3.2 常规数字签名方法

目前的数字签名是建立在公共密钥体制基础上的，它是公共密钥加密技术的另一类应用。已经具有大量数字签名算法，如 RSA 数字签名算法、ElGamal 数字签名算法、Fiat-Shamir 数字签名算法、Guillou-Quisquarter 数字签名算法、Schnorr 数字签名算法、美国的数字签名标准算法（DSS/DSA）、椭圆曲线数字签名算法和有限自动机数字签名算法等。本节将介绍两种基本的数字签名算法，即 RSA 数字签名算法和 ElGamal 数字签名算法，许多数字签名方案都是基于这两种算法。

3.2.1 RSA 签名

RSA 是最为流行的数字签名方法，许多产品内核中都有 RSA 的软件和类库。

简化的数字签名技术使用了像 RSA 这样可逆的公开密钥加密系统，其数字签名过程中运用了消息的验证模式。签名过程如下：

- 发送方用自己的私有密钥对要发送的信息进行加密，形成数字签名。
- 发送方将数字签名附加在消息后通过网络传送给接收方。
- 接收方用发送方的公开密钥对接收到的签名信息进行解密，得到信息明文。
- 接收方将解密得到的消息与接收到的消息进行比较，若两者相同，则说明消息未被篡改过。

简化的 RSA 数字签名过程如图 3.3 所示。

在这一过程中，消息的发送方已验证模式用 RSA 生成加密的信息，也就是说加密密钥是发送方的私有密钥。加密后的信息附加在明文上一起传送出去。在接收方那里，接收方必须要知道相应的解密密钥，即发送方的公开密钥，才能有这把密钥来解密加密后的信息，并将解密

后的信息与明文作比较。如果两者相同，则接收方就能确信发送方确实拥有加密密钥，同时还可以确信在传输的过程中消息未被篡改过。

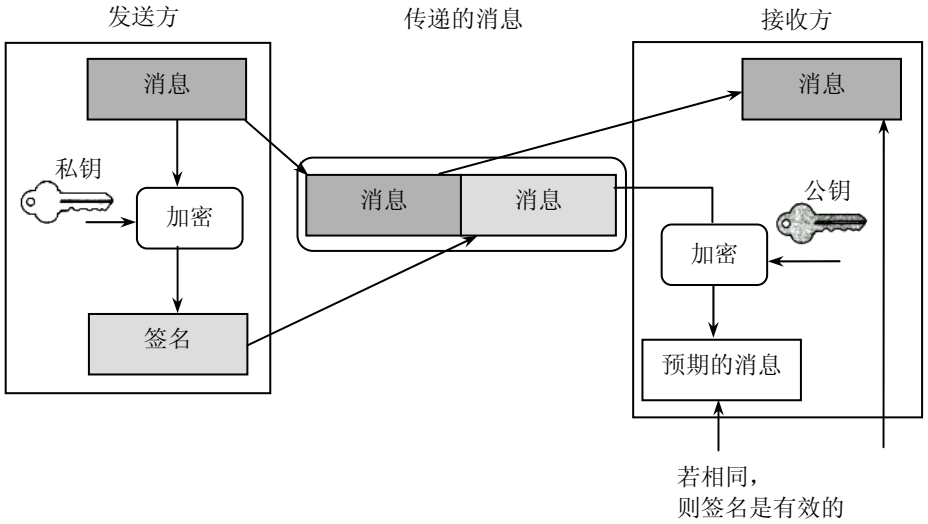

图 3.3　简化的 RSA 数字签名

这种基于公开密钥的数字签名的优点在于，对任何可能的消息接收方来说都能检查签名，因为解密密钥即发送方的公开密钥向公众公开是不会危及安全的。

但这种方案也存在着一定的问题，特别是用于处理和通信的成本过高，因为加密和解密不得不对整个信息内容进行，并且发送的数据量至少是原始信息的两倍。为了对此方案进行改进，可以运用散列函数来进行处理。散列函数是一种单向函数，可以把大量信息映射成相对较小的信息范围。例如，一条成千甚至上百万位长度的信息，经过散列函数的操作，得到的输出信息只有 160 位长。散列函数的另外一个特点是，如果信息发生了变化，哪怕只改动了一位，用散列函数产生的值就会完全不同。由此就可以知道信息是否被篡改过。利用散列函数的数字签名过程如下：

- 发送方对要发送的消息运用散列函数形成数字摘要。
- 发送方用自己的私有密钥对数字摘要进行加密，形成数字签名。
- 发送方将数字签名附加在消息后通过网络传送给接收方。
- 接收方用发送方的公开密钥对接收到的签名信息进行解密，得到数字摘要。
- 接收方运用同样的散列函数对接收到的消息形成数字摘要。
- 发送方对两个数字摘要进行比较，若两者相同，则说明消息未被篡改过。

整个签名过程如图 3.4 所示。

在这一过程中，利用散列函数，可以对要签名的消息内容生成一个固定长度的数据项，即数字摘要。摘要具有这样的特性，即只要消息内容发生了任何改变，所形成的摘要就是不同的。

在这种机制下，发送方用散列函数来获得数字摘要，然后用 RSA 对数字摘要进行加密形成数字签名，并与消息一起传送出去。接收方收到信息后，重新计算摘要，同时用 RSA 对数字签名进行解密，然后比较两个摘要值。如果相符，则接收方就可以确信发送方确实拥有该私有密钥，即该消息确实是由该发送方发来的，并且信息内容在传送途中未被篡改过。

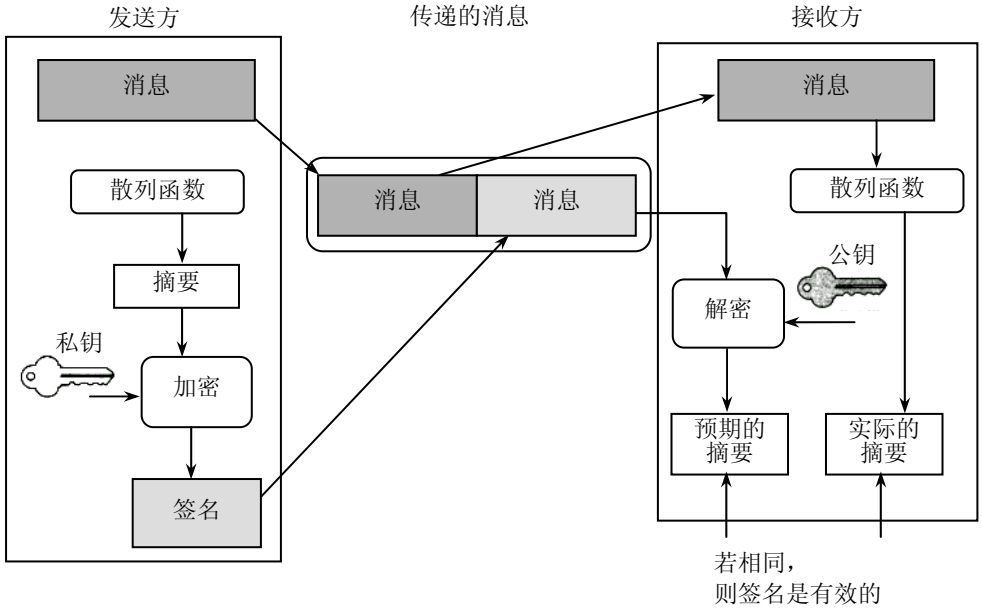

图 3.4 用散列函数进行 RSA 签名

RSA 数字签名算法的安全性基于数论中大整数分解的困难性，算法如下：

安全参数：选两个大素数 p 和 q，令 n=pq，选 e 并计算出 d，使 ed = 1 mod （p-1）（q-1），公开 n 和 e，将 p，q，和 d 保密。

数字签名：对于消息 $M \in Z_n$，定义

$S=Sig（M）=M_d \bmod n$

为对 M 的签名。

签名验证：对给定的 M，S 可按下式验证：设 $M' = S^e \bmod n$，如果 M=M′，则签名成立，否则，不接受签名。

3.2.2 ElGamal 签名

该体制由 T.ElGamal 在 1985 年提出，是专门为签名的目的而设计的，其修正形式已经被美国 NIST 作为数字签名标准（DSS）。它是一种非确定性的双钥体制，即对同一明文消息，由于随机参数选择的不同而有不同的签名。这种方案的安全性基于求离散对数的困难性，即对于 $y \equiv g^x \bmod p$（p 为素数，g 是 p 的原根），已知 x，g，p 计算 y 是容易的，但是在已知 y，g，p 的情况下，计算 x 是非常困难的。

1. ElGamal 算法参数说明:

p：一个大素数，使得求解离散对数为困难问题；

g：g 是 p 的模数序列中较大的一个元素；

M：明文；

x：1<x<p，x 为私钥；

y： $y=g^x \bmod p$，（p，g，y）为公钥；

H(x)：Hash 函数。

2. 签名及验证过程

（1）给定消息 M，选择随机数 k，k<p。

（2）计算 H(M)，并计算 $r=g^k \bmod p$，$s=(H(M)-xr)k^{-1} \bmod (p-1)$，签名结果是(M,r,s)。

（3）收信人收到(M,r,s)，先计算 H(M)，并验证 $y^r r^s=g^{H(M)} \bmod p$，若两者相等，则签名有效。

除了这两种数字签名算法外，椭圆曲线数字签名算法（ECDSA）和美国数字签名标准算法（DSA）也是比较常用的数字签名方法。椭圆曲线加密系统是一种运用 RSA 和 DSA 来实施的数字签名方法。基于椭圆曲线的数字签名具有与 RSA 数字签名和 DSA 数字签名基本上相同的功能，但实施起来更有效，因为椭圆曲线数字签名在生成签名和进行验证时要比 RSA 和 DSA 快。椭圆曲线数字签名还可以用在一些较小、对资源有一定限制的设备（如智能卡，即含有微处理器芯片的塑料片）中。

美国数字签名标准算法 DSA 将在 3.4 节中介绍。

3.3　特殊数字签名方法

根据电子商务具体应用的需要，形成了许多特殊的数字签名应用，如盲签名、多重签名、代理签名、定向签名等。本节将对它们进行简单介绍。

3.3.1　盲签名

盲签名是根据电子商务具体的应用需要而产生的一种签名应用。在一般的数字签名中，总是要先知道文件内容后才签署。但是有时候需要某人对一个文件签名，而又不让他知道文件的内容，这时就需要盲签名。盲签名是 Chaum 在 1983 年首先提出的，一般用于电子货币和电子选举中。

A 要从 B 处获得盲签名的过程如下：

（1）A 取一文件 M 并以一随机数乘之得 M′，这个随机数通常称为盲因子，A 将 M′发送给 B。

（2）B 在 M′上签名，将其签名发送给 A。

（3）A 去除盲因子（作逆盲运算），从 B 关于 M′的签名中得到 B 关于原始文件 M 的签名。

Chaum 对盲签名有一个形象的比喻：所谓盲签名，就是先将要签名的文件放到一个信封里，文件在信封中无人可读。去除盲因子的过程就是打开信封的过程。对文件签名相当于在信封里放一张复写纸，当签名者在信封上签名后，就得到了他对文件内容的签名。

盲签名有两个要求：第一，消息内容对签名者不可见；第二，签名被接收者泄漏后,签名者无法追踪签名。下面将介绍几种盲签名方案，这些方案都是在 ElGamal 签名方案上构造的。

1. 盲消息签名

在盲消息签名方案中，签名者仅仅对盲消息 M′签名，而并不知道真实消息 M 的具体内容。这里，对 M 的签名简记为 Sig（M）。这类签名的特征是：$Sig(M)=Sig(M')$ 或 $Sig(M')$ 含 Sig（M）中的部分数据。因此，只要签名者保留关于盲消息 M′的签名，便可确认自己关于 M 的签名。

在盲消息签名方案中，只要签名者保留 $Sig(M')$，便可将 Sig(M)和 $Sig(M')$ 相联系。因此，

为了保证真实消息 M 对签名者保密，盲因子尽量不要重复使用。

盲消息签名方案在电子商务中一般不用于构造电子货币支付系统，因为它不保障货币持有者的匿名性。

2. 盲参数签名

在盲参数签名方案中，签名者知道所签消息 M 的具体内容。按照签名协议的设计，签名收方可改变原签名数据，即改变 Sig(M)而得到新的签名，但又不影响对新签名的验证。因此，签名者虽然签了名，却不知道用于改变签名数据的具体安全参效。

盲参数签名方案的这些性质可用于电子商务系统 CA 中心，为交易双方颁发口令。任何人虽然可验证口令的正确性，但包括 CA 在内谁也不知道变化后的口令。在实际应用中，用户的身份码 ID 相当于 M，它对口令产生部门并不保密。用户可以从管理部门为自己产生的非秘密口令中得到秘密口令。这种秘密口令并不影响计算机系统对用户身份进行的认证。

3. 弱盲签名

在弱盲签名方案中，签名者仅知Sig(M′)，而不知 Sig(M)。如果签名者保留Sig(M′)及其他有关数据，待 Sig(M)公开后，签名者可以找出Sig(M′)和 Sig(M)的内在联系，从而达到对消息 M 拥有者的追踪。

盲消息签名方案与弱盲签名方案的不同之处在于，弱盲签名不仅将消息 M 做了盲化，而且还对签名Sig(M′)做了变化，但两种方案都未能摆脱签名者将 Sig(M)和Sig(M′)相联系的特性，只是后者的隐蔽性更大一些。因而，弱盲签名方案与盲消息签名方案的实际应用也较为类似。

4. 强盲签名

在强盲签名方案中，签名者仅知Sig(M′)，而不知道 Sig(M)。即使签名者保留Sig(M′)及其他有关数据，仍难以找出Sig(M′)和 Sig(M)之间的内在联系，因此不可能对消息 M 的拥有者进行追踪。

强盲签名方案是性能较好的一个盲签名方案，电子商务中使用的许多数字货币系统和电子投票系统的设计都采用了这种技术。

3.3.2 多重签名

类似于日常生活中手写签字，数字签名有时也需要多个用户对同一消息进行签名，这就是多重数字签名问题。根据签名过程的不同，多重数字签名方案可以分为两类：一类为有序多重数字签名方案，另一类为广播多重数字签名方案。每一种方案都有三个过程：系统初始化，签名的产生过程和签名的验证过程，同时每一种方案都包含消息发送者、消息签名者和签名验证者。在广播多重数字签名方案中还包含有签名收集者。

现说明两种方案的签名过程。假设有 n 个用户，U_1，U_2，…，U_n签署同一份消息 M，有序多重签名方案的签名过程如下：消息发送者预先设计一种签名顺序（U_1，U_2，…，U_n），并将这种签名顺序发送到每一位签名者。然后将待签消息 M 发送到第一个签名者 U_1，第一个签名者签名后，将消息发给第二个签名者 U_2。从 U_2开始，每一位签名者收到签名消息后，首先验证上一签名的有效性，如果签名有效，则继续签名，并将签名消息发送到下一个签名者；如果签名无效，则拒绝对消息签名，终止整个签名。当签名验证者收到签名消息后，验证签名的有效性，如果有效，多重签名有效；否则，多重签名无效。可以看出，在有序多重数字签名方案中，签名者 U_i（i=1，2，…，n）要对 U_1，U_2，…，U_{i-1}的签名进行验证，同时签名验证者

对所有签名者 U_1，U_2，…，U_n 的签名进行验证。

在广播多重签名方案中，消息发送者同时将待签消息 M 发送给每一位签名者 U_i（i=1，2，…，n）进行签名，然后 U_i（i=1，2，…，n）将签名的结果发送到签名收集者，由收集者签名消息进行整理并发送给签名验证者。签名验证者验证多重签名的有效性。

多重签名在办公自动化、电子金融和 CA 认证等方面有重要的应用。

3.3.3　代理签名

在现实世界里，人们经常需要将自己的某些权力委托给可靠的代理人，让代理人代表本人去行使这些权利。在这些可以委托给他人的权力中包括人们的签名权。例如，某公司的经理需要到外地出差，为了不影响公司的业务，该经理可以委托一个可靠的助手，让该助手在他出差期间代表他在一些重要文件上签字。委托签名权力的传统方法是使用印章，因为印章可以在人们之间灵活地传递，在电子化的信息社会，同样会遇到委托签名权力的问题。代理签名的目的就是当某签名人(这里称为授权人)因公务或身体健康等原因不能行使签名权力时，将签名权委派给其他人替自己行使签名权。换言之，代理签名就是原始签名人将自己的签名权委托给可靠的代理人，让代理人代表本人去行使某些权力。这种签名机制在许多领城都有重要的应用，因此引起了人们的极大兴趣。

1. 代理签名的基本要求

代理签名应满足以下条件：

（1）签名容易验证。

（2）源签名者与代理签名者的签名容易区分。

（3）签名事实不可否认。

2. 几种代理签名方案介绍

针对于应用的需要，在原始代理签名方案的基础上，人们又提出了一些新的方案，以解决现实生活中出现的应用需求，下面对其中一些方案进行介绍。

（1）一次性代理签名方案。在通常的代理签名中，一旦原始签名人将签名权委托给某人后，无法控制代理人的签名次数，这将对原始签名人的权益产生不良影响。一次性代理签名方案使得代理人最多签名一次，如果超过规定次数，代理签名人的密钥将被破解。采用此方案的优点是：代理人不但可以控制授权人无法传送秘密信息，而且又能保障授权人的权益不被代理人侵犯，代理人的代理签名权同时也受到授权人的制约，即达到了双向制约的功能。

（2）代理多重签名。代理多重签名是指某人同时受多人委托进行代理签名。下面举例子说明代理多重签名的应用。如果一个公司将要发布一个涉及到财务部门、工程部门以及行政管理部门的文件。该文件必须由这些部门联合签名才有效，或者这些部门也可以委托它们都信任的一个代理人同时代替它们在该文件上签字。对于前一种情况，可以用前面提到的多重签名方案解决。而对于后一种情况，即多个部门同时委托一个代理人在一个文件上签名，仅仅多重签名或者代理签名都是不够的。因为一般的代理签名中，一个代理签名只能代表一个原始签名人。在这种情况下，可以用代理多重签名方案进行解决。多重数字签名的应用比较广泛，它还可以用于数字货币,特别是对大额数字货币的签发上，以加强系统或交易的安全性。

（3）盲代理签名。在一般的代理签名中，原始签名人可以从自己得到的代理签名中辨认出签名人的身份。对于原始签名人来说，他们可以利用这一性质对代理签名人的签名行为进行

监督，以防止代理签名人滥用他们的代理权力。但在有些情况下，尽管代理签名人忠实地行使着原始签名人委托给自己的代理签名权力，但他们却不希望自己的代理签名受到原始签名人的监督，不希望原始签名人能根据代理签名确定出他们的身份。电子问卷调查就是一个很好的例子，被调查者希望能够毫无顾忌的回答问题，同时不希望调查者知道自己的身份。为了满足这个要求，可以采用盲代理签名方案。在盲代理签名方案中，原始签名人在得到代理签名时，不能根据代理签名确定出代理签名人的身份。

3.3.4 定向签名

当通过网络传输电子邮件和有关文件时，为了维护有关的权力和合法利益，为了维护网上信息在法律上的严肃性，发送者应当对所发信息进行数字签名，使接收者确信接收到的信息是可信的、合法的和有效的，它可以防止不法者的冒充行为。

对许多签名方案而言，无论什么人，只要获得签名就可验证签名的有效性。这些签名方案包括 RSA 签名方案和 ElGamal 签名方案，任何拥有签名拷贝的人都可以利用签名者的公钥验证签名的有效性。这一特性对于如公开声明之类的文件的散发是必须的，但是对另一些文件如个人或公司的信件特别是有价值的文件的签名，如果也可以随便散发和验证，就会造成灾难。例如一些数字签名可能包含有对签名接收者敏感的信息，如汇票、医疗记录、税务信息等等，这些签名最好只能由接收者直接验证。为了使特定的收方才能验证签名的有效性，对 RSA 签名而言，可以对签名采用加密传送的方法。由 Chaum 等人提出的不可否认签名方案也具有对签名验证者进行控制的能力。但这种方案的实施需要签名者和验证者之间相互传送有关信息(交互式验证)。从实际应用看，一般并不需要对签名进行加密，更不必采用较为繁琐的交互式验证。

因此有了定向签名的概念，并产生了一些定向签名方案。这些方案仅允许特定的收方对签名进行验证，但它们不需要像 RSA 签名那样要对签名加密，也不需要像不可否认签名那样要进行交互式验证。由于具有有向性，这些方案的安全性也得到了加强，极大地缩小了受攻击和受伪造的范围。

目前主要有 ElGamal 型签名方案和 MR 型定向签名方案，MR 型定向签名方案是具有消息还原功能的签名方案，它是由 Nyberg 等人建立的。它们的区别在于，在验证 ElGamal 型签名的有效性时，签名人应将消息 M 连同签名一起送收方。而在使用 MR 型定向签名方案时不必传送消息 M。任何人收到签名后，利用签名便可还原 M。使用 MR 型定向签名方案的优点在于：即使在未使用加密方案的情况下，除了收方外，任何人无法看到消息 M 的内容。因此，MR 型定向签名方既是签名方案，同时又起到了对消息 M 进行加密的作用。

3.3.5 双联签名

在商务活动中经常出现这种情形，即持卡人给商家发送订购信息和自己的付款账户信息，但不愿让商家看到自己的付款账户信息，也不愿让处理商家付款信息的第三方看到订货信息。双联签名技术可以解决这个问题。

双联签名的使用方法如下：

（1）持卡人将发给商家的信息 M1 和发给第三方的信息 M2 分别生成报文摘要 MD1 和报文摘要 MD2。

（2）持卡人将 MD1 和 MD2 合在一起生成 MD，并签名。

（3）将 M1、MD2 和 MD 发送给商家，将 M2、MD1 和 MD 发送给第三方。接收者根据收到的报文生成报文摘要，再与收到的报文摘要合在一起，比较结合后的报文摘要和收到的 MD，确定持卡人的身份和信息是否被修改过。双联签名解决了三方参加电子贸易过程中的安全通信问题。

3.3.6　团体签名

David Chaum 提出了下述问题：

一个公司有几台计算机，每台都连在局域网上。公司的每个部门有它自己的打印机（也连在局域网上），并且只有本部门的人员才被允许使用他们部门的打印机。因此，打印前，必须使打印机确信用户是在那个部门工作的。同时，公司想保密，不可以暴露用户的姓名。然而，如果有人在当天结束时发现打印机用得太频繁，主管者必须能够找出谁滥用了那台打印机，并给他一个账单。

对这个问题的解决方法称为团体签名。它具有以下特性：

（1）只有该团体内的成员能对消息签名。

（2）签名的接收者能够证实消息是该团体的有效签名。

（3）签名的接收者不能决定是该团体内哪一个成员签的名。

（4）在出现争议时，签名能够被“打开”，以揭示签名者的身份。

下面是一个具有可信仲裁者 T 的团体签名方案：

（1）T 生成一大批公开密钥/私钥密钥对，并且给团体内每个成员一个不同的惟一私钥表。在任何表中密钥都是不同的（如果团体内有 n 个成员，每个成员得到 m 个密钥对，那么总共有 n • m 个密钥对）。

（2）T 以随机顺序公开该团体所用的公开密钥主表。T 保持一个哪些密钥属于谁的秘密记录。

（3）当团体内成员想对一个文件签名时，他从自己的密钥表随机取一个密钥。

（4）当有人想验证签名是否属于该团体时，只需查找对应公钥表并验证签名。

（5）当争议发生时，T 知道哪个公钥对应于哪个成员。这个协议的问题在于需要可信的一方。T 知道每个人的私钥因而能够伪造签名。而且，m 必须足够长以避免试图分析出每个成员用的哪些密钥。

3.3.7　不可争辩签名

不可争辩签名是在没有签名者自己的合作下不可能验证签名的签名，它是由 Chaum 和 van Antwerpen 提出的。它拓展了普通签名概念，使签名者能够限制签名的验证权，即不可争辩签名的验证必须在签名者的帮助下完成。这一性质有效地防止了签名接收者滥用签名。

不可争辩包括两层含义：

（1）签名的证实和否定必须与签名者合作完成，这一点可以有效地防止一些有价值的文件被随意复制或分发。

（2）签名者不能抵赖他曾签过的签名，由于签名者可以通过拒绝执行证实协议来否认他曾签过的签名，为了防止此类事件发生，不可否认签名增加了一个否认协议，签名者可以利用否认协议证明一个伪造的签名是假的；而如果签名者拒绝执行否认协议，就表明签名事实上是

由他签署的。

不可争辩签名可用于软件产品的分发上，以保护知识产权。软件公司 A 采用不可否认签名方法对其软件产品签名，使得只有合法的用户能够与 A 合作验证签名的有效性。若某个第三方实体 B 私自售卖或分发产品的拷贝，那么从 B 那里得到产品的用户将无法验证签名的有效性，从而不能确定得到的产品是否是正品。

不可争辩的一种变化是把签名者与消息之间的关系与签名者与签名之间的关系分开。在这种签名方案中，任何人能够验证签名者实际产生的签名，但签名者的合作者还需要验证该消息的签名是有效的。

3.4 美国数字签名标准

3.4.1 DSS 简介

1991 年 8 月 30 日，美国国家标准与技术局（NIST）在联邦注册书上发表了一个通知，提出了一个联邦数字签名标准，NIST 称之为数字签名标准（DSS）。DSS 提供了一种核查电子传输数据及发送者身份的一种方式。NIST 提出：“此标准适用于联邦政府的所有部门，以保护未加保密的信息……它同样适用于 E-mail、电子金融信息传输、电子数据交换、软件发布、数据存储及其他需要数据完整性和原始真实性的应用”。

尽管政府各部门使用 NIST 提出的 DSS 是命令所迫，但是他们对 DSS 的采纳使用会对私人领域产生巨大的影响。除了提供隔离生产线以满足政府和商业需求外，许多厂家设计所有的产品都遵守 DSS 要求。为了更好地理解 DSS 成为私人领域标准的可能性，我们可以回想 NIST 的前身——美国国家标准局于 1977 年将数字加密标准(DES)确定为政府标准后不久，美国国家标准机构采用了它，从而使它成为一个广泛使用的工业标准。

美国政府在推行 DSS 时，遭到了不少非议。DSS 当时受到的批评主要有：

（1）太神秘（这是 NSA 设计的协议，它使用了 ElGamal 算法）。

（2）太慢（在验证签名时比 RSA 慢了 10 倍至 40 倍）。

（3）太新（ElGamal 算法当时还没有被完全分析透彻）。

（4）太不安全（固定的 512 位密钥）。

在后续的修订版本中，以上的问题逐渐得到了解决。

3.4.2 数字签名算法（DSA）

自从 NIST 引荐数字签名标准以来，它对 DSS 签名作了广泛的修改。DSS 签名为计算和核实数字签名指定了一个数字签名算法(DSA)。经过公众的评议并作了少许改进后，1994 年，DSS 首次作为联邦信息处理标准（FIPS）对外公布。

DSA 基于的是离散对数问题，其困难之处在于要在有限域内进行数学取幂的逆操作。美国联邦信息处理标准 186-2 中对数字签名算法（DSA）作了详尽的规定。

数字签名算法是一种单向不可逆的公开密钥系统，其安全性取决于离散对数的计算难度。数字签名算法令：

$$y=g^x \bmod p$$

其中 p 是质数，g 是 p 的模数序列中较大的一个元素。有了 g、x 和 p，可以很容易地计算出 y；但给出 y、g 和 p，要计算 x 则极为困难。这就为公开密钥系统奠定了基础，其中 y 就是公开密钥，x 则是私有密钥。

该系统中用到三个整数 p，q 和 g，可对组内的所有用户公开。模数 p 为质数，其范围在 512 至 1024 位之间。q 是小于 160 位的一个质数，为 p-1 的因子。而 g 是这样确定的：

$$g = j^{[(p-1)/q]} \bmod p$$

其中 j 为任意整数，其范围是 1<j<p，故：

$$j^{[(p-1)/q]} \bmod p > 1$$

对于某一个确定的发送方来说，私有密钥 x 是随机选定的，且 1<x<q。而公开密钥 y 则是根据上述公式计算得来的。利用 DSA 进行数字签名时，签名者首先用散列函数生成一个待签名的信息摘要，然后由 DSA 签名算法利用私有密钥 x 对该摘要进行处理，形成两个由 160 位数字 r 和 s 组成的签名数据，该签名信息与原始的发送信息一起保存或发送。例如，要对摘要为 h 的信息进行签名，用户可随机选择一个整数 k（0<k<q），并进行下列计算：

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

$$s = [k^{-1}(h + xr)] \bmod q$$

其中 k^{-1} 是模数为 q 的 k 的反函数，即（$k^{-1}k$）mod q=1，且 $0<k^{-1}<q$。r 与 s 这一对数字构成了对信息的签名。

为了验证所接收到的相伴摘要 h′ 的签名信息 r′ 和 s′，接收方首先要检查 r′ 与 s′ 的取值是否满足 0<r′<q 和 0<s′<q 的条件。只要其中的任何一个条件得不到满足，系统就会拒收签名。若条件全部满足，接收方就可以根据 s′ 和 h′ 的值来计算数值 v。若 v 等于签名中 r′，则验证了签名是正确的。v 的计算过程如下：

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

$$u1 = (h' \ w) \bmod q$$

$$u2 = (r' \ w) \bmod q$$

$$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$$

从用户使用相应算法的角度看，DSA 和 RSA 稍微有点不同。前半部分与 RSA 签名一样，系统也是利用散列函数来生成要进行签名的信息的摘要，但随后 DSA 在对摘要进行处理时，需要使用私有密钥，并生成由两个 160 位数字组成的签名，签名与发送的信息同时传送或存储。接收方运用散列函数对接收到的信息重新计算摘要，由此来验证数字签名。然后将计算出来的摘要、收到的数字签名以及公钥反馈给 DSA 进行验证操作，根据验证的结果可以说明数字签名是否正确。

RSA 和 DSA 在技术上最重要的不同在于：DSA 的验证过程中对资源的处理要比 RSA 更彻底。除此之外，两者在加密强度和其他的技术特征方面没有什么明显的不同。但由于 RSA 早期在市场上做了大量推广工作，所以相对于 DSA 而言，RSA 占据了市场的统治地位。

3.5　数字证书技术

由于在电子商务交易中，买卖双方在交易过程中是互不照面的，因此就需要有一种事物

来表明自己的身份，以示自己是一个合法的用户或合法的商家。电子商务中的数字证书就是这样一种由权威机构发放的用来证明身份的事物。

在网上，双方要想谈一笔生意，任何一方都要鉴别对方是否是可信的，也就是要确定交易双方的身份。但是，如何才能保证所得到的公开密钥的正确性，即如何保证交易对方的真伪呢？为了解决这个问题，就引出了认证机制，其中就涉及到数字证书和认证机构 CA。

3.5.1 数字证书简介

公开密钥数字证书，是一种将某方的身份（证书主体）与某个公开密钥值安全地联系在一起的数据结构。数字证书是由认证机构颁发的、包含了公开密钥持有者信息以及公开密钥的文件，证书上还有认证机构的数字签名。就像驾驶执照能将照片、姓名、出生日期进行有公证效果的关联一样，一个用户的数字证书就是一个有公证效果的将公开密钥与所有者的身份信息相联系的“数字身份证”。在网上的电子交易中，如果双方出示了各自的数字证书，并用它来进行交易操作，那么双方都可不必为对方的身份担心。

数字证书系统通过认证机构为公-私密钥对的持有者发放和管理数字证书。每一个数字证书包含了数字证书主体的一个公钥值和对其所作的无二义性的身份确认信息。其中，数字证书主体是指持有相应私钥的个人、设备或其他实体，而认证机构则用自己的私钥对数字证书进行数字签名。

对于用户来说，如果他已经安全地获得了某一认证机构的公钥，而且该用户是信任该认证机构的，那么该用户就可以获得此认证机构的任一用户的公钥。方法是先获得该认证机构用户的一个数字证书拷贝，然后抽出其中的认证机构公钥值，并用认证机构的公钥来检验数字证书上的数字签名。这样，借助数字证书，用户只要知道了一个通信方（即认证机构）的公钥，就可以获得其他很多通信方的公钥。因而，可以获得很好的规模效应。

数字证书不是一劳永逸的，需要对它进行有效期的检验，它有一个预定的有效期限，包括一个起始和终止的日期及时间。在数字证书期满后，数字证书主体和公钥间的捆绑就不再有效，因而数字证书也不再受信任。用户不能使用一个已过期的数字证书，除非是为了重新确认数字证书有效期内所发生过的某一项活动，如，检验某一旧文档上的数字签名。在数字证书期满后，如果数字证书的主体仍然拥有一个有效的公钥，则发放数字证书的认证机构可以给该用户发放一个新的数字证书。

此外，由于各种各样的原因，认证机构也可能会在数字证书到期之前撤销数字证书。例如，在已知或怀疑相应的私钥被泄露时，为保护公钥用户，就需要防止其继续运用在私钥被泄露前发放的数字证书来使用公钥。

3.5.2 数字证书的类型

数字证书一般分为三种类型。

1. 个人数字证书

个人数字证书主要为某一个用户提供证书，以帮助个人用户和其他用户交换信息或者使用在线服务时，验证用户的身份，保证信息的安全，主要是针对个人的电子邮件安全。个人身份的数字证书通常安装在浏览器内，并通过安全的电子邮件来进行操作。目前常用的 Netscape 浏览器和 IE 浏览器都支持该功能。

2. 服务器证书

服务器证书主要为网上的某个 Web 服务器提供证书，拥有 Web 服务器的企业就可以用具有凭证的互联网站点进行安全的电子交易。拥有数字证书的服务器可以自动与客户进行加密通信，具有数字证书的 Web 服务器会自动地将其与客户端的 Web 浏览器的通信加密。服务器拥有者有了证书，就可以进行安全的电子交易了。

3. 开发者证书

开发者证书通常为互联网中被下载的软件提供证书。开发者证书又称为代码签名数字证书，借助这种数字证书，软件开发者可以为软件做数字标识，在互联网上进行安全的传送。在用户从互联网上下载软件时，开发者证书与微软的 Authenticode（认证码）技术共同提供他们所需的软件信息和对该软件的信任。当客户从开发者网站上下载经过数字标识了的 Active X 控制命令、Java 程序、动态链接库、HTML 内容时，就能够确信该代码的确来自于开发者，而且没有被改变或破坏。开发者证书就好像是软件的外包装，如果它被篡改了，客户就知道代码实际已经不可信了。

在上述三类证书中，前两类是常用的证书，第三类则用于特殊场合。大部分认证机构都只提供前两类证书，能提供全部三类证书的认证机构并不多。

3.5.3　利用数字证书实现信息安全

下面，我们分别从信息的发送方和接收方的角度来介绍如何利用数字证书实现信息安全。

如图 3.5 所示，发送方的工作主要有下面几步（对应图中的编号）：

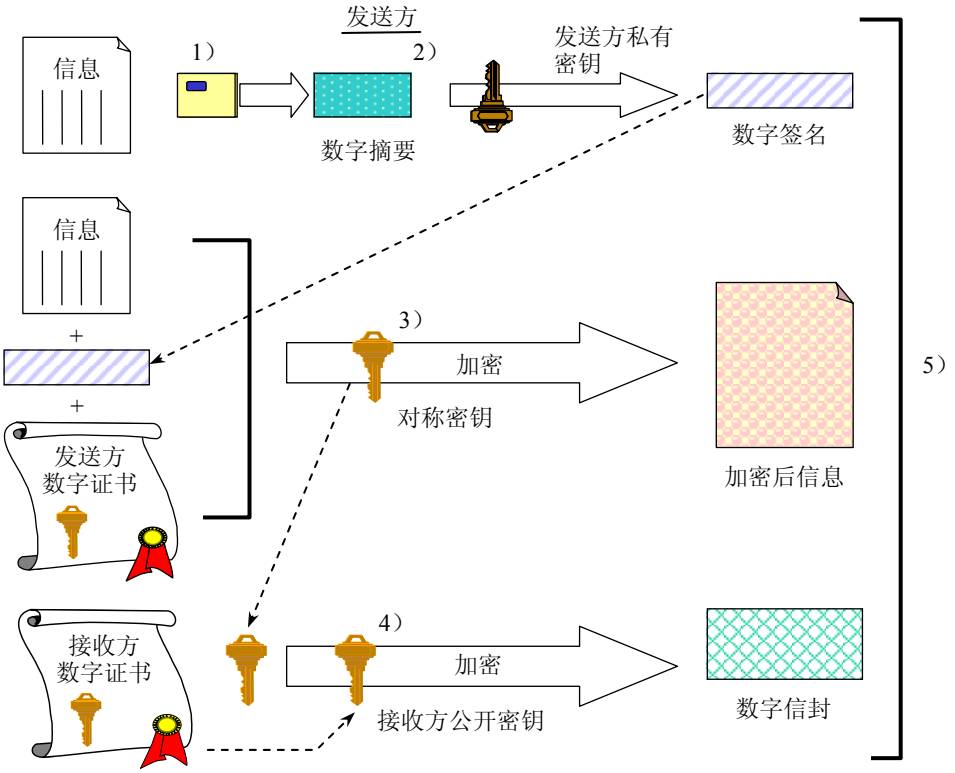

图 3.5　发送方的工作

1）发送方利用散列函数，把要发送的信息散列成固定长度的数字摘要。

2）发送方用自己的私有密钥对数字摘要进行加密，形成数字签名。

3）发送方把数字签名和自己的数字证书附加在原信息上，利用对称密钥进行对称加密，形成加密后的信息。

4）发送方用接收方数字证书中给出的公开密钥，来对发送方进行对称加密的密钥进行加密，将加密结果装入数字信封。

5）发送方把加密后的信息与数字信封一起通过网络发送出去。

如图 3.6 所示，接收方的工作主要有下面几步（对应图中的编号）。

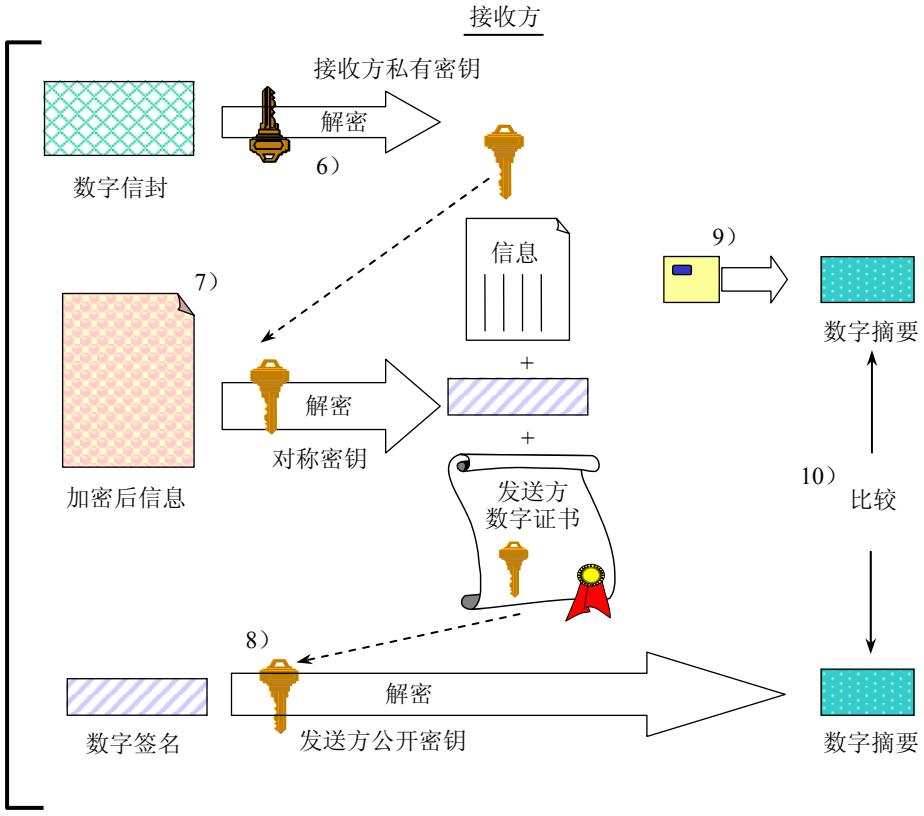

图 3.6　接收方的工作

6）接收方用自己的私有密钥对接收到的数字信封进行解密，得到发送方用于加密的对称密钥。

7）接收方用解密得到的对称密钥对接收到的加密后信息进行解密，得到信息、数字签名和发送方的数字证书。

8）接收方用得到的发送方数字证书中的公开密钥对数字签名进行解密，得到数字摘要。

9）接收方运用同样的散列函数，把解密得到信息散列成固定长度的数字摘要。

10）接收方比较两个数字摘要。若比较结果一致，则说明信息在传递的过程中未被篡改过，即保证了数据的完整性。

3.5.4　数字证书的格式

在数字证书的格式方面，被人们普遍接受并使用得最为广泛的是 ITU 的 X.509 标准数字证书格式。ITU X.509 标准也称为 ISO/IEC 9594-8 标准。

1. 基本数字证书格式

X.509 数字证书格式有三个不同的版本。

- 版本 1 格式，在 1988 年的第一版中定义。
- 版本 2 格式，在 1993 年的第二版中定义。
- 版本 3 格式，是在 1997 年的第三版中定义，并在 2000 年的第四版中又对其进行了改进。

首先介绍在版本 1 和版本 2 中所定义的 X.509 基本数字证书格式，然后介绍版本 3 中所增加的扩充内容。图 3.7 给出了基本的数字证书格式。

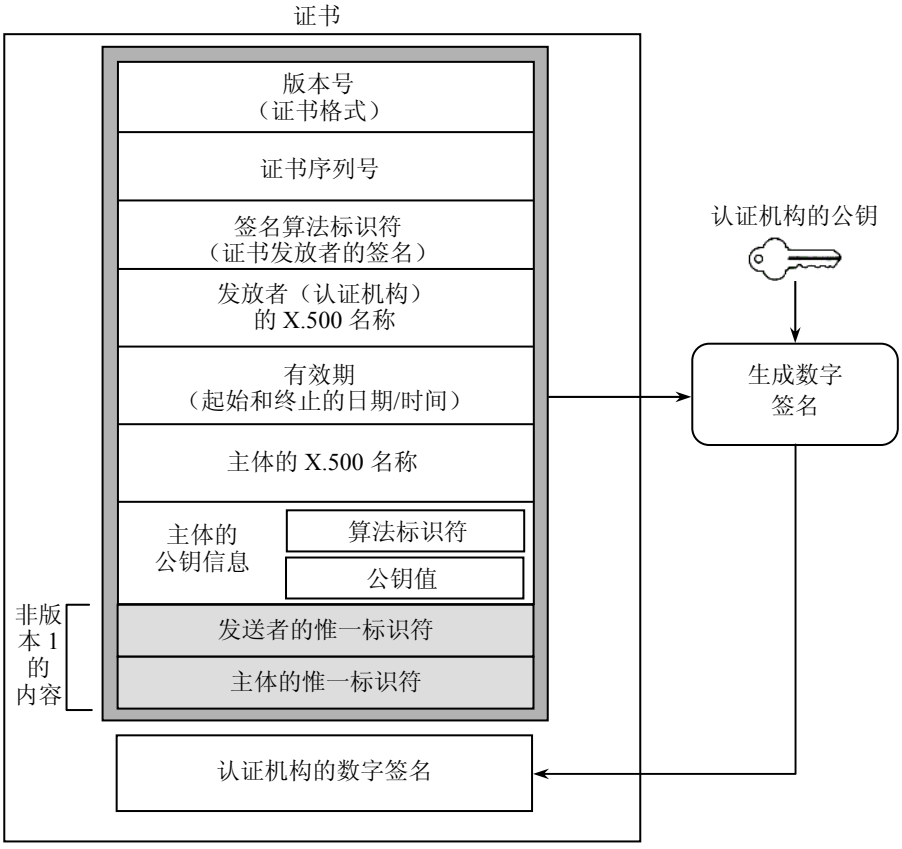

图 3.7　基本数字证书格式

基本数字证书格式中包含如下内容：

- 版本号：代表数字证书的版本格式是版本 1、版本 2 或版本 3，将来还可以是其他版本。
- 数字证书序列号：由认证机构发放的代表该数字证书的惟一标识号。
- 签名算法标识符：认证机构用来对数字证书进行签名所使用的数字签名算法的算法标识符。

- 数字证书发放者：发行数字证书的认证机构的 X.500 名称。
- 有效期：数字证书的起始和终止的日期和时间。
- 主体：与相应的被验证公钥所对应的私钥持有者的 X.500 名称。
- 主体的公钥信息：主体的公钥值以及该公钥被使用时所用的算法标识符。
- 数字证书发放者的惟一标识符：这是一个可选项，当不同的实体具有相同的名称时，利用该标识符可使发放数字证书的认证机构的 X.500 名称不具有二义性。
- 主体的惟一标识符：这是一个可选项，当不同的实体具有同样的名称时，利用该标识符可使主体的 X.500 名称不具有二义性。

尽管 X.509 数字证书并没有限定只能和 X.500 目录系统一起使用，但在其第一版和第二版的基本数字证书格式中却只使用 X.500 名称来确定主体和数字证书发放者的身份。

一个 X.500 目录由一系列目录项组成。每个目录项对应一个现实世界中的对象，如某个人、某个组织或某个设备。每一对象都有一个无二义性的名称，称为特异名（distinguished name，DN）。对象的目录项中包含了有关该对象的一系列属性值。例如，关于某人的目录项可能包含了其名字、电话号码以及电子邮件地址等属性。为支持无二义性命名的需要，所有的 X.500 目录项在逻辑上被组织成一种树型结构，称为目录信息树（Directory Information Tree，DIT）。目录信息树有一个概念上的根节点和数目不限的非根节点，除了根节点，所有节点都从属于其他节点。除根节点外，每一个节点都对应于一个目录项，并有一个特异名。根节点的特异名为空。

在基本数字证书格式中，还包含了一些用于数字证书发放者的数字签名和认证公钥的算法标识符。如，下面是一些常见算法的标识符：

- 用于数字签名的使用 SHA-1 散列函数的 DSS 算法标识符。
- 用于数字签名的使用 SHA-1 散列函数的 RSA 算法标识符。
- 用于建立加密密钥的 RSA 密钥传输算法标识符。
- 用于建立加密密钥的 Diffie-Hellman 认证技术算法标识符。

这些算法标识符是需要注册的对象类的一个实例，也就是对惟一对象标识符的一个赋值。

用于算法标识符和其他很多与电子商务相关的对象类的对象注册系统是一个对象标识符机制，该机制由国际标准指定，并受一系列国际对象注册机构的支持。

一个对象标识符是由一系列整数成分组成的一个值，该值在所有对象标识符中是惟一的，它可以赋给一个已注册的对象。对象标识符的构成依据的是一个由不同赋值机构所组成的层次结构，其中的每一层负责对象标识符值的一个整数成分。

2. X.509 版本 3 数字证书格式

从 1993、1994 年开始，X.509 数字证书开始尝试运用于大规模的商业活动中，但是基于版本 1 和版本 2 的基本数字证书格式在很多方面都显得不够完善。为了满足数字证书在电子商务应用中的需要，负责这方面工作的标准化组织（ISO/IEC，ITU 和 ANSI X9）在数字证书中增添了一个通用扩充机制，经过扩充后的数字证书格式，就是 X.509 版本 3 的数字证书格式。

图 3.8 给出了 X.509 版本 3 的数字证书格式。从图中可以看到，除了增加了扩充字段外，版本 3 的数字证书格式与基本数字证书格式是相同的。借助扩充字段，企业可以将任意数目的附加字段加入到数字证书中。

每个扩充字段都有一个需要被注册的类型，注册方法如同算法的注册，即将一个对象标识符赋值给该类型。原则上，任何人都可以来定义扩充类型。在实际操作时，为实现互操作性，

公共扩展类型必须为所有的实施者所了解。所以事实上，扩展类型的标准化工作是最重要的。但一些重要团体可能会定义自己的扩展类型以满足自己的特殊需要。

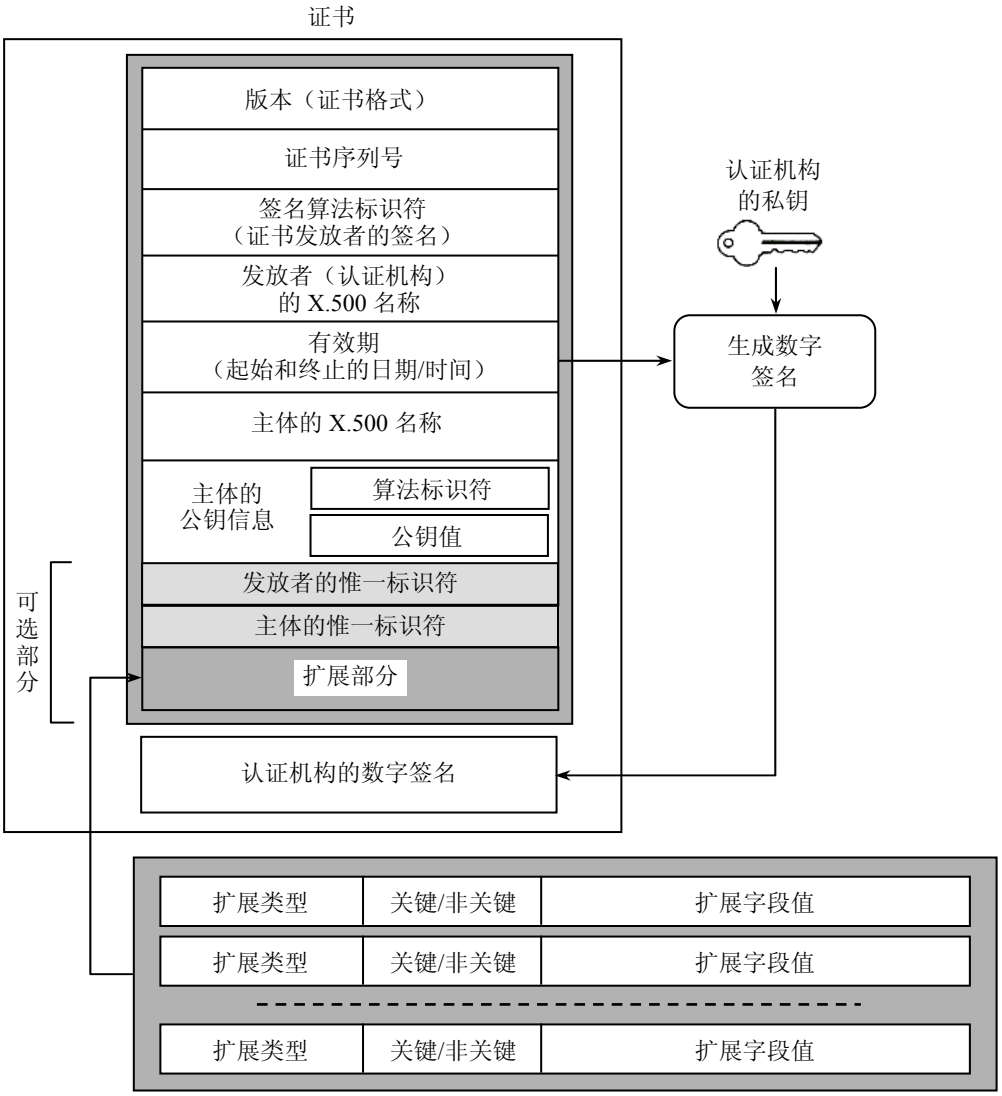

图 3.8　X.509 版本 3 的数字证书格式

在版本 3 的数字证书格式中，每个扩展字段都由三部分组成：

- 一个表示扩展类型的对象标识符值。
- 一个关键程度指示器。
- 一个扩展字段值。

其中，扩展类型规定了值的数据类型（字符串、日期或复杂数据结构）以及与值相关联的语义。

设置关键程度指示器的目的，是为了适应不同系统需识别不同扩展类型的需要。当数字证书用于支持多种应用程序需求时，或通过技术移植而引入更多的新扩展类型时，就会用到

关键程度指示器。其实关键程度指示器仅是一个简单的标志，用以指明扩展类型是关键的还是非关键的。如果关键程度指示器指明一个扩展类型是非关键的，那么当使用数字证书的系统无法识别该扩展类型时，允许忽略该扩展字段。而如果关键程度指示器指明一个扩展类型是关键的，则任何对该数字证书的部分使用都是不安全的，除非系统能识别扩展类型并调用与之关联的函数。

在 X.509 版本 3 数字证书格式中，不再仅仅局限于用 X.500 名称来确定数字证书主体和数字证书发放者的身份。任何一个实体都可以用一个或多个不同形式的名称来确定，只要名称能无二义性地标识出一个实体的身份就可以了。

3. 数字证书扩展标准

伴随着 X.509 数字证书的使用，ISO/IEC、ITU 和 ANSI X9 等标准组织制定了一系列 X.509 数字证书扩展标准。其中，ISO/IEC 和 ITU 将相应的扩展内容融入了 1997 年颁布的标准中，并于 2000 年进行了完善，而 ANSI 所做的扩展除了在技术上能与 ISO/IEC/ITU 所进行的扩展相融合外，还将重点放在了金融业的应用上。

标准的扩展主要包括如下几个部分：

（1）密钥信息的扩展。密钥信息的扩展传送了有关主体和发放者密钥的附加信息，如密钥标识符和被认可密钥用途指示器。这些扩展允许管理者限制数字证书和认证密钥的用途。

（2）政策信息扩展。政策信息扩展用于传达数字证书政策，这些扩展的使用与认证机构所制定的准则有关。

（3）主体及发放者属性扩展。主体及发放者属性的扩展支持主体和发放者的备用名。它们还可以传送关于主体的附加属性信息，以帮助数字证书用户确信数字证书适用于某个特定的人、组织或设备。

（4）认证路径约束扩展。认证路径的约束扩展帮助不同的组织将他们的基础设施连接在一起。当某一认证机构在对另一认证机构进行认证时，可以在数字证书中放入一些用以提醒数字证书用户的信息，这些信息说明了从本数字证书出发可以产生的认证路径的类型约束。

（5）与数字证书撤销表相关的扩展。

3.5.5 数字证书的申请与发放

1. 数字证书管理机构的作用

数字证书管理机构包括认证机构 CA 和注册机构 RA。

认证机构 CA 又称认证中心、证书授予机构，是承担网上认证服务，能签发数字证书并能确认用户身份的受大家信任的第三方机构。CA 通常是企业性的服务机构，其主要任务是受理数字证书的申请、签发及对数字证书进行管理。

认证机构是保证电子商务安全的关键，是公正的第三方，它为建立身份认证过程的权威性框架奠定了基础，为交易的参与方提供了安全保障，为网上交易构筑了一个相互信任的环境，解决了网上身份认证、公钥分发以及信息安全等一系列问题。

认证机构对含有公开密钥的证书进行数字签名，使证书无法伪造。每个用户都可以获得认证机构的公开密钥，以此来验证任何一张数字证书的数字签名，从而确定该证书是否由某认证机构签发的，该数字证书是否合法。数字证书与驾驶执照一样，用来表示个人的身份，且有一定的有效期，有效期结束后必须重新申请。认证机构作为证书的发行机构具有一定的权威性，

因而数字证书被社会所承认和接受。

目前，在全球处于领导地位的认证机构是美国的 VeriSign 公司。VeriSign 公司提供的数字证书服务遍及世界各地，提供了我们在前面提到的所有三类数字证书，即个人数字证书、服务器数字证书和开发者数字证书。

认证机构 CA 负责对于数字证书的管理，认证机构与其用户或数字证书申请人间的交互工作则是由注册机构 RA 来完成的。一个认证机构可能对应了多个注册机构，而且这些注册机构可能是分散在各处的。这是因为在发放数字证书时，申请人需亲自到场，出具自己的身份证明文件、交换实物标记或进行生物测定，以此来确定申请人的身份。

注册机构本身并不发放数字证书，但注册机构可以确认、批准或拒绝数字证书申请人的申请，随后由认证机构给经过批准的申请人发放数字证书。注册机构的主要功能如下：

- 注册、注销、批准或拒绝对用户数字证书属性的变更要求。
- 对数字证书申请人进行合法性确认。
- 批准生成密钥对和数字证书的请求及恢复备份密钥的请求。
- 接受和批准撤销或暂停数字证书的请求（需要相应认证机构的支持）。
- 向有权拥有身份标记的人当面分发标记或恢复旧标记。

注册机构与认证机构可能是不同的法律实体，但也有些注册机构是认证机构的某一特殊组成部分。

2. 数字证书的申请注册

在电子商务环境中，数字证书可以发放给各种不同类型的实体，包括个人、组织和设备。一般来讲，数字证书的申请注册从数字证书申请人提出请求发放数字证书的申请开始。

数字证书的申请注册手续在不同的环境中可能是各不相同的。例如，雇主在给其雇员发放数字证书时，其注册过程可以是自动的。因为雇主对雇员是很了解的，由雇主管理的认证机构很有可能可以对雇员数据库进行自动的和可靠的存取，从中获得代表雇员的注册信息并对其进行确认。

在 Internet 环境中，数字证书的申请注册大多是通过在线注册过程或全部地在线方式来进行的。例如，用户可以利用 Web 浏览器与充当认证机构服务前端的服务器进行在线注册。但注册机构必须对用户进行合法性验证，以确定公钥值及其他的用户信息真正来自于该用户，且在传送的过程中未被篡改过。注册机构还可能需要了解有关该用户的更多信息，这些信息可以通过与用户间的在线对话来获得，也可通过查询第三方的相关数据库而获得。由于单纯通过在线注册系统获得的确认信息是有一定的局限性的，因此，在更多的情况下，有些确认过程是在网下进行的。例如，数字证书申请人向注册机构出具身份证明书，或由注册机构通过邮政服务给数字证书申请人邮寄在以后的在线数字证书申请过程中提交命令所需要的秘密口令等。

一般来说，在批准和发放数字证书之前，由注册机构来对个人、设备和实体的身份及其他指定属性（如特权、作用、权限等）进行确认是十分重要的。

身份确认可以通过下述方法来进行：

- 了解私有信息：主体出具与之有关的私有信息。一般情况下，这是一些很简单的信息，如账号或姓名加上口令或身份识别号。也有些情况下，可能需要一些其他信息，如最后一次进行账户交易的日期。
- 亲自到场：一般认为，对一个令人信服的身份确认来说，很重要的一点是被确认人与

确认实体需进行面对面的交流。申请人亲自到场，使得认证机构或其代表不仅能证实数字证书申请人的存在并了解其特点，而且还能了解申请人申请数字证书的目的，以及了解申请人是否有能力遵守数字证书应用规则和进行数字证书的使用。例如，有时可以评价申请人是成年人还是未成年人，能否理解数字证书语言以及对数字证书申请人的要求等。一旦当面确定了身份，对大部分数字签名活动来说，就不再需要申请人亲自到场了。

- 身份证明文件：认证机构或其代表可以要求申请人当面出具身份证明文件，以确认申请人的身份。这些文件（特别是那些带有照片的身份证明证件，如护照、工作证或驾驶证）一般认为都是可信任的。

3. 数字证书的生成

数字证书的生成通过下列步骤实现：

数字证书申请人将申请数字证书所需要的数字证书内容信息提供给认证机构。

认证机构确认申请人所提交信息的正确性，这些信息将包含在数字证书中。

由持有认证机构私钥的签证设备给数字证书加上数字签名。

将数字证书的一个副本传送给用户，如果需要的话，用户在收到数字证书后返回一确认信息。

将数字证书的一个副本传送到数字证书数据库如目录服务，以便公布。

作为一种可供选择的服务，数字证书的一个副本可以由认证机构或其他实体存档，以加强档案服务、提供证据服务以及不可否认性服务。

认证机构将数字证书生成过程中的相关细节以及其他在数字证书发放过程中的原始活动都记录在审计日志中。

4. 数字证书的更新

每份数字证书的生命周期都是有限的。在整个生命周期中，认证机构有义务完成数字证书的撤销。一般而言，在数字证书期满后需要更换数字证书。另外，密钥对也需要定期更换，而一旦更换了密钥对，那就需要用新的数字证书。所以，数字证书的期满和数字证书的更新常常与密钥对的期满和更新结合在一起。

有时，数字证书的更新对用户来说是透明的。例如，在那些由充当认证机构的组织来有效控制用户数字证书的重要组织中，或者在那些对数字证书更新的原因是因为密钥对需要更新的重要组织中，情况就是如此。出于对后一种情况的考虑，目前有些加密技术产品已经能够自动识别出密钥对是否已到期，从而自动更新密钥对，并启动与认证机构间必须的通信对话，以发放新的数字证书，而所有这些都无需用户的介入。

如果是在其他情况下更新数字证书，如，一些包含在数字证书中的用户身份确定信息有了变动，或是认证机构规定用户必须定期确认数字证书中的细节信息，则一般就要由用户来进行数字证书的更新。这时用户会收到更新数字证书的通知，确认数字证书更新申请的内容，并接受新的数字证书。

3.5.6 数字证书的分发

在电子商务中，为了加密数据或验证数字签名，用户需要相应通信方的数字证书，还需要相应认证机构的数字证书，以此来完成相应的验证，这就涉及到了一个数字证书的分发问题。

由于数字证书具有自我保护能力，所以不需要通过具有安全性保护的系统和协议来传送。常用的数字证书分发方法有：通过数字签名来分发，或通过目录服务来分发。

1. 利用数字签名分发数字证书

利用数字签名，可以方便地进行数字证书的分发。签名者通常拥有自己数字证书的一个副本，他可以将该副本附加在数字签名中。这样，任何想检验数字签名的人就都可以拥有该数字证书的副本。类似地，签名者也可以附加上其他必需的数字证书以证实自己数字证书的有效性，例如，附加上其他认证机构给签名者的认证机构所发放的数字证书。目前，大多数使用数字签名的通信协议都规定用这种方法来将数字证书附加在数字签名上。

不过，也有人反对将数字证书附在数字签名上，理由是，这可能会浪费通信和存储容量，因为检验数字签名的通信方可能在本地已经拥有了必需的数字证书。因此，是否附加数字证书或附加什么数字证书，一般由签名者来决定。

还有，假设从各个不同的检验者到签名者具有不同的认证路径，那么对签名者来说，判断检验时到底需要哪些数字证书并不是一件容易的事情。因此，如果没有严格的认证机构结构来保证从各个检验者到某个签名者之间只具有单一的认证路径，则要由签名者来保证将所有必需的数字证书附在数字签名上是不切实际的。所以，检验者需要通过一种可靠的方法，如检索目录或数字证书数据库，来获取所缺少的数字证书。

2. 利用目录服务分发数字证书

在利用公钥技术加密信息时，信息的发送方必须首先获得所有接收方的认证公钥。虽然可能因为以前曾经与信息的接收方有过交流，信息发送方碰巧在其本地存储着必需的数字证书，因而不再需要接收方的数字证书。但在一般的情况下，信息的发送方必须去寻找必需的数字证书。在这种情形下，目录服务或数字证书数据库对于数字证书的分发就显得非常有价值了，因为信息的发送方可以通过目录检索来获得接收方的数字证书及其他的信息，如接收方的电子邮件地址等。

在线的目录服务模型及其支撑协议标准是由国际电信联盟（International Telecommunication Union，ITU）和国际标准化组织（International Organization for Standardization，ISO）共同制订的。这些曾以 ITU X.500 闻名的目录标准旨在支持全球规模的多用途分布式目录服务，包含的范围从简单的名称—地址查询到浏览及关键属性查询应有尽有。X.500 目录可以给人们、给通信网络组件、给计算机应用程序以及其他的自动系统充分的信息源。例如，对计算机网络用户来说，可以根据人名来查询并返回如电话号码、电子邮件地址等信息，还可返回该用户的设备所支持的应用协议的详细信息。

早在 1984～1988 年间首次开发 X.500 标准时，人们就已经注意到了利用 X.500 的目录进行数字证书分发的潜力，所以在该标准中包含了用 X.500 来承担该角色时所需要的数据对象的规范，同时还包括了围绕这一功能的管理流程的详细描述。这些资料都包含在 X.509 规范中。

遗憾的是，X.500 在市场推广使用中并没有达到预期的目标，因为这种技术太复杂了，因而其实施和配置的费用都太高。

在 X.500 的基础上，人们随后开发了 Internet 自己的目录存取协议，称为轻型目录存取协议 LDAP（Lightweight Directory Access Protocol）。LDAP 在目录模型上与 X.500 相兼容，但比 X.500 协议更简单，实施起来也更友好。LDAP 协议是一种用于存取储存在目录中的信息，如数字证书信息的有效的标准协议。需要注意的是，LDAP 只是一个存取协议，并不要求目录数

据库采用什么特殊的技术。IETF PKIX 工作组详细说明了通过 LDAP 来获取数字证书的过程。

在一些特殊的软件平台环境中，曾经利用专用的目录系统来分发数字证书，现在，这些系统已进行了很大程度的移植，以支持 LDAP 作为标准的存取协议。

分发数字证书的方法还有很多。由于数字证书不需要专门的安全保护，所以可以利用非安全性的协议，通过不信任的系统来分发。例如，IETF PKIX 工作组有专门的协议用于使用 HTTP 和 FTP 在 Web 上请求和获取数字证书。此外，需要重复使用的数字证书还可以存储在使用公钥的本地系统中。

3.5.7 公钥基础设施 PKI

为解决 Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的公钥基础设施 PKI。公钥基础设施（Pubic Key Infrastructure，PKI）又叫公钥体系，是一种利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范，用户可利用 PKI 平台提供的服务进行安全通信。

PKI 必须具有权威认证机构 CA 在公钥加密技术基础上对数字证书的产生、管理、存档、发放以及撤销进行管理的功能，包括实现这些功能的全部硬件、软件、人力资源、相关政策和操作程序，以及为 PKI 体系中的各成员提供全部的安全服务。如，实现通信中各实体的身份认证、保证数据的完整性、不可否认性以及保密性等。

PKI 基础设施采用数字证书来管理公钥，通过第三方的可信任机构——认证机构 CA，把用户的公钥和用户的其他标识信息捆绑在一起，在 Internet 网上验证用户的身份。

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 的主要目的是通过自动管理密钥和数字证书，来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。

一个有效的 PKI 系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解 PKI 是怎样管理数字证书和密钥的。一般来说，一个典型、完整、有效的 PKI 应用系统应具有下述功能：

- 公钥数字证书的管理。
- 证书撤销表的发布和管理。
- 密钥的备份和恢复。
- 自动更新密钥。
- 自动管理历史密钥。
- 支持交叉认证。

由于公钥基础设施是目前比较成熟、完善的 Internet 网络安全解决方案，所以国外一些大的网络安全公司纷纷推出了一系列基于 PKI 的网络安全产品，如美国的 Verisign、IBM、加拿大的 Entrust 等，这些产品为电子商务的发展提供了安全保证。

3.5.8 CA 的结构

1. 认证路径

如果能建立一个可以给世界上所有的用户发放数字证书的认证机构，并且所有的用户都

信任该认证机构的话，那么数字证书的认证问题就变得非常简单了。但遗憾的是，这是不可能的。要求一个认证机构能够对所有的潜在用户都进行充分的了解并建立适当的联系，而这些潜在的用户又都允许该机构来发放和管理证书，且证书又能被所有的用户接受，这是不切实际的。因此，在电子商务中也就必然存在着多个认证机构。

既然有多个认证机构，那么要假设某一用户已经安全地拥有了某个特定认证机构的公钥，而该认证机构又恰巧是给此用户的安全通信方发放证书的认证机构，也是不切实际的。不过，为了获得那个特定认证机构的公钥，用户也许可以找到并使用另一证书，即由另一认证机构（用户已安全地拥有了该认证机构的公钥）所发放的包含了那个特定认证机构公钥的证书。这就引出了交叉认证的问题。

根据 IETF 的 PKIX 工作小组的定义，所谓交叉认证数字证书，是由一个认证机构对另一个认证机构签发的包含了该 CA 的签名密钥的数字证书。换言之，交叉认证数字证书就是在认证过程中用到的由一个认证机构对另一个认证机构签发的证明书。

在认证过程中，我们可以这样来考虑。先在某个认证机构处申请一份数字证书，然后循环地获得越来越多的认证机构的数字证书，相应地，也就获得了大量的密钥对持有者的公钥。这就引出了被称之为证书链或认证路径的问题，而认证路径是建立大规模公钥基础设施的基础。一开始某个用户需要可靠地获得某个可信任的根认证机构的公钥，然后，只要在该公钥用户所信任的根认证机构和一些密钥对持有者之间存在着认证路径，当然中间可能会经过任意数目的中间认证机构，则该公钥用户就可以获得并使用这些密钥对持有者的公钥。

为了使用某个异地通信方的公钥，数字证书用户（使用方）必须找到一条有效的完整的认证路径，将公钥从一个或多个认证机构传送到可信任的根认证机构——数字证书用户持有该 CA 的公钥并信任该 CA。在建立公钥基础设施的过程中，一个主要的挑战就是如何使得寻找有效认证路径的过程变得简单、方便和高效，这在很大程度上要依赖于 CA 间的结构关系。

CA 间的结构关系，有时又被称为信任模型。因为只有借助 CA 间的结构关系，才能使得一些认证机构能够验证其他认证机构的身份。

2. *树型层次结构*

为了把认证路径问题简化为最简单的形式，我们可以用树型或称为层次型的结构来表示 CA 间的结构关系。利用这种方法，可以把一个由最终实体组成的庞大团体中的各个成员通过可接受的简短路径来跟一小部分可信任的根 CA 认证机构联系起来，通过其中的每条路径可以通往各个可信任的认证机构。

如图 3.9 给出的就是树型层次结构。图中大写字母 Z、X、Y 等代表的是实体——认证机构，小写字母 a、b、c 等代表的是最终实体——用户，其中的箭头代表上级认证机构已经给下级认证机构签发了数字证书，或认证机构已经给最终用户签发了数字证书。

所有的认证路径都是从根认证机构 Z 开始的，数字证书用户必须把根认证机构作为其惟一最终可信任者。换言之，他们必须持有根认证机构公钥的可靠副本，并且通过独立的途径使其生效。寻找一条通向任一个最终实体的认证路径是很容易的，比如任何数字证书用户都可以通过一个由 4 份数字证书所组成的认证路径来取得 a 实体公钥的有效副本：

- 由 Z 为 X 签发的数字证书。
- 由 X 为 Q 签发的数字证书。
- 由 Q 为 A 签发的数字证书。

- 由 A 为最终实体 a 签发的数字证书。

在使用任何认证路径时，数字证书用户必须相信该认证路径上的每一个认证机构都已经忠实地履行了自己的义务，并且已经采取了适当的防范措施，以保证排除那些自称是来自认证机构的伪造的数字证书。在这个树型模型里，所有的参与方都必须承诺恪守公钥体系所公认的行为准则。

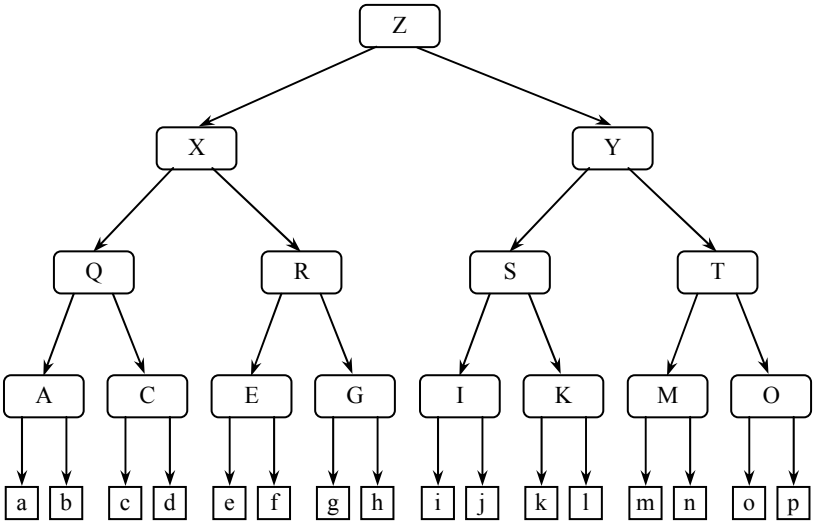

图 3.9 树型层次结构

3. 森林型层次结构

在树型结构的 PKI 中，所有参与者都要达到一定的最低信任度标准，而且必须遵循共同的行动准则。这些要求在为某个特定的团体，如在为企业的雇员、为 B2B 交易的客户团体、以及为某个垂直型行业的联合团体设计 PKI 时并不难做到。

但在现实的电子商务安全应用环境中，要为所有的参与方建立一个包容万象的树型结构似乎比较困难，所以一种可供选择的方法是建立一个如图 3.10 所示的森林型的数字证书使用体系来识别多个树型结构。如，在下面两种情况下往往就会用到这种结构：

- 数字证书用户打算信任由某个外部机构给他们的内部团体签发的数字证书，如给它们的雇员或是客户签发的数字证书。
- 数字证书用户打算信任由多个独立的商业认证机构签发的数字证书。

4. 通用结构

在 X.509 的第三版数字证书格式形成后，人们觉得树型和森林型结构并不能满足所有应用环境下的要求，有时候往往需要更加复杂的结构模型，来协调多个相互独立的 PKI，使它们顺利执行不同的任务，或是建设在不同的政策要求下可以同时支持多个应用环境的 PKI。所以，X.509 标准委员会决定给出一系列形式多样的方法，使得任何用户团体都可以建立他们认为合适的各个认证机构与它们的 PKI 之间的结构关系。不过，这种通用结构模式的实现，是以增加应用系统实施的复杂程度为代价的。

采用通用结构模式，其复杂性主要在于要解决两个核心问题：

- 如何找到合适的认证路径。

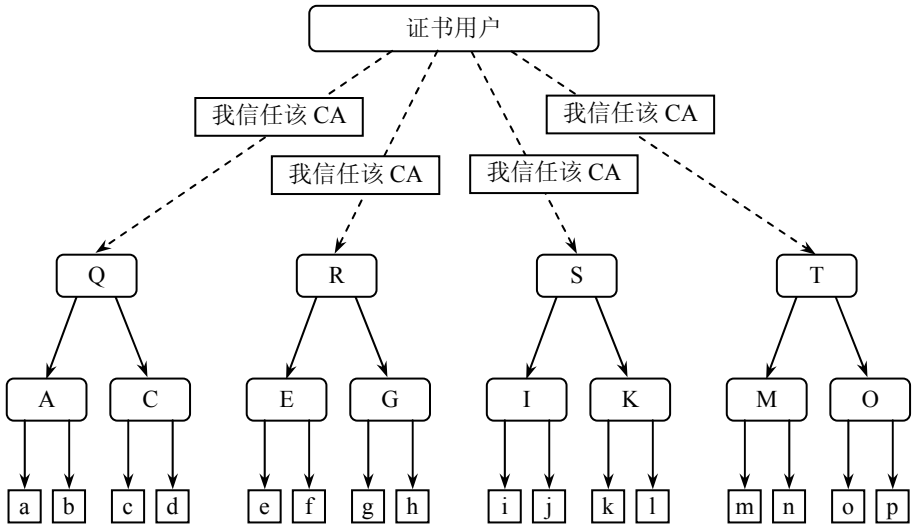

图 3.10　森林型结构

- 找到认证路径以后，如何使它生效。

在每一个数字证书使用系统中都必须具备这两个功能，而且这是两个独立的任务，其实现过程也是相对独立的。从这两个功能来说，寻找认证路径的过程并不是在实现安全性功能，而使认证路径有效则是在实现安全性功能。

3.6　电子签名法律

电子商务交易及信息传递的有效性、安全性和不可抵赖性等问题一直是关系到电子商务得以顺利开展的核心问题之一，而目前以非对称密钥系统为主的电子签名技术的应用可以基本解决交易及信息传递的有效性、安全性和不可抵赖性等问题，该技术在电子认证机构的支持下得到快速应用和发展，其安全可靠性已经过大量实践的检验。所以，从法律的角度给予电子签名以传统签名、盖章同等的法律地位就成为电子签名得以广泛应用和发挥功效的前提，也是近十年国际电子商务立法的核心内容。从 1995 年至今，已经有许多国家、地区和国际组织先后制订了电子签名法或以确立电子签名法律地位为主要内容的电子商务法，从根本上为其国内电子商务的发展奠定了基础，确立电子签名的法律地位已成为国际立法和电子商务发展的大势所趋。随着 2005 年 4 月 1 日我国首部电子签名法的实施，电子签名法律在我国也受到了相当程度的重视。本节旨对电子签名法律的相关问题进行介绍。

3.6.1　电子签名法律概述

在电子商务中，双方或多方可能远隔万里而互不相识，甚至在整个交易过程中自始至终不见面，传统的签字方式很难应用于这种交易。因此，人们试探采用一种电子签名机制来相互证明自己的身份。这种电子签名可以由符号及代码组成，它具备了上述签字的特点和作用。对每一方来说，具体采取什么符号或代码，是根据现有的技术、相关经验、可应用标准的要求及使用的安全程序来决定的。任何一方的电子签名可以不时地改变，以保护其机密的特征。

法律上关于电子签名的规定，是根据签名的基本功能得出来的，认为凡是满足签名基本功能的电子技术手段，均可认为是电子签名。如联合国贸法会《电子签名示范法》（以下简称《示范法》）中这样定义电子签名：在数据电文中，以电子形式所含、所附或在逻辑上与数据电文有联系的数据，它可用于鉴别与数据电文相关的签名人和表明签名人认可数据电文所含信息。鉴于联合国贸法会在国际上的地位，这一定义得到了广泛的认可。

需要注意的是，从概念上说，电子签名与数字签名是不同的。数字签名的概念来源于科学技术领域，特指利用公钥密码技术而实现的对数据的鉴别。而电子签名，如前所述，是法律上根据签名的基本功能而定义的。电子签名与数字签名的关系是：电子签名是法律上为了追求技术中立性而泛化的概念，数字签名是电子签名的一种特定实现形式。

3.6.2 电子签名法的主要特点

电子签名法具有以下特点。

1. 技术问题复杂，但法律问题却相对简单

虽然作为电子签名法调整对象的电子商务、电子签名所涉及的技术问题比较复杂，但这些技术问题本身并不属于法律要解决的问题。电子签名法所要解决的法律问题相对比较简单，因为商务活动的绝大多数法律问题在传统法律中已经解决，电子签名法只需解决因商务活动信息载体的变化所涉及的法律问题，而这些问题大多只需采用“功能等同”的办法作出相应规定即可。因此，联合国示范法和许多国家、地区的电子签名法的内容都很简单。例如，联合国电子商务示范法只有 17 条、电子签名示范法只有 12 条，欧盟电子商务指令只有 27 条，美国国际与国内电子签名法只有 11 条，俄罗斯电子签名法只有 21 条，我国台湾省的电子整章法只有 17 条。

2. 具有很强的国际统一趋势

电子商务最显著的优势，就在于可以利用不受国界限制的全球性互联网络方便地进行网上交易，这就必然要求电子签名法律制度应当是国际统一的。联合国有关机构为统一各国的电子签名法律制度作了大量工作，组织各国专家制定了示范法。目前，许多国家有关数据电文和电子签名法的主要规定大体上都是一致的，否则无法与电子商务的国际化接轨。我国电子签名法（草案）的基本规定，也与联合国示范法的规定大体一致。

3. 实行“技术中立”的立法原则

即法律只规定作为安全可靠的电子签名所应达到的标准，至于采用何种技术手段来实现这一标准，法律不作规定，以避免影响新技术的开发使用。联合国示范法和不少国家、地区的电子签名法，都采取这一原则。我国电子签名法（草案）也采用了这一原则。但也有一些国家和地区的电子签名法采用了技术特定化的原则，针对安全可靠的电子签名所采用的技术作了具体规定。

3.6.3 电子签名国际立法状况

国际上第一部电子签名法制定于 1995 年，由美国的犹他州制定。为了向各国立法者提供一套国际公认的规则，说明如何消除电子商务发展中的法律障碍，为电子商务发展创造一个安全的空间，联合国分别于 1995 年和 2001 年，颁布了《电子商务示范法》和《电子签名示范法》。继此之后，各国际组织、国家和地区纷纷开始了电子商务领域的立法活动。新加坡于 1998 年颁布了《电子商务法》，该法主要涉及电子商务的三个核心问题，其中之一即是“电子签名”，其内容占据了大量篇幅，是该法的核心内容。日本政府于 2000 年 6 月颁布了《数字化日本之发端——行动纲领》，

该纲领重申了电子签名认证系统对发展电子商务的重要意义，并分析了几类具体认证系统及日本应采取的态度，行动纲领建议立法要点有明确“电子签名”的法律地位，保障“电子签名”所使用技术的中立性等。此外，还有许多其他国家和地区都制定了相关的法律。

从表 3.1 中可以看到，从 1999 年至今，在短短几年时间内，就有几十个国家、组织和地区制定了电子商务的相关法律或草案，无论是美国、德国等发达国家，还是马来西亚等发展中国家，对此反应都极为迅速。尤其是联合国贸易法委员会，更起到了先锋与表率的作用，及时引导了世界各国的电子商务立法。这种高效的立法，在世界立法史上是非常罕见的。从某种意义上说，2000 年前后席卷全球的电子商务狂潮在很大程度上就要归功于这些法律。同时也可以看出来，从 1997 年到 2001 年内的 5 年时间内，是电子签名法律制定的高峰期，而我国在 2005 年实施电子签名法，已经相对滞后了。

表 3.1　世界各国数字签名立法一览表

国家或地区	法律名称	通过时间
联合国	《电子商务示范法》	1995 年
俄罗斯	《俄罗斯联邦信息法》	1995 年
马来西亚	《数字签名法》	1997 年
意大利	《数字签名法》	1997 年
德国	《数字签名法》《数字签名条例》	1997 年
新加坡	《电子交易法》	1998 年
加拿大	《统一电子商务法》	1999 年
澳大利亚	《电子交易法》	1999 年
哥伦比亚	《电子商务法》	1999 年
韩国	《电子商务基本法》	1999 年
欧盟	《欧盟电子签名统一框架指令》	1999 年
芬兰	《电子商务管理法》	2000 年
英国	《电子通信法》	2000 年
菲律宾	《电子商务法》	2000 年
爱尔兰	《电子商务法》	2000 年
西班牙	《电子签名与认证服务法》	2000 年
美国	《国际与国内商务电子签章法》	2000 年
印度	《电子签名和电子交易法》	2000 年
中国香港特别行政区	《电子交易条例》	2000 年
日本	《数字化日本之发端行动纲领》	2000 年
中国台湾省	《电子签章法》	2001 年
联合国	《电子签名示范法》	2001 年
日本	《电子签名与认证服务法》	2001 年
俄罗斯	《电子数字签名法》	2001 年
波兰	《电子签名法》	2002 年
中国大陆地区	《中华人民共和国电子签名法》	2005 年

在电子商务高速发展并逐步打破国界的大趋势下，电子商务立法中任何的闭门造车会严重阻碍电子商务与相关产业的发展。因此，各国在进行电子商务立法时，都特别注重电子签名法律的兼容性。并且，也正是这种兼容性的要求造就了电子商务立法中先有国际条约后有国内法的奇特现象。联合国贸易法委员会在其 《电子签名统一规则指南》中就曾指出：“电子商务内在的国际性要求建立统一的法律体系，而目前各国分别立法的现状可能会产生阻碍其发展的危险。”

世界各国和地区对电子签名方面的立法对规范电子签名活动，保障电子安全交易，维护电子交易各方的合法权益，促进电子商务的健康发展起到了重要作用，法律的制定及时有力地推动了电子商务、信息化和相关产业的发展。

3.6.4 我国数字签名法律

随着计算机在中国的普及与应用，中国的电子商务应用也日益广泛。而且从与国际化接轨的需要看，中国的经济正在逐步融入世界经济活动的大家庭中，这就要求中国在享受 WTO 普遍优惠的同时，其经济行为和方式也必然要受到 WTO 规则的约束。同时，中国经过 20 多年的改革开放，在世界范围内的经济地位正在不断攀升，国内及国际间的交流合作也日益频繁。这些，都要求我国必须尽快出台既与本国发展相适应，又适合于国际间交流的相关制度。《电子签名法》适时而生。《中华人民共和国电子签名法》由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于 2004 年 8 月 28 日通过，自 2005 年 4 月 1 日起施行。

《中华人民共和国电子签名法》共分 5 章 36 条。该法立法的直接目的是为了规范电子签名行为，确立电子签名的法律效力，维护各方合法权益；立法的最终目的是为了促进电子商务和电子政务的发展，增强交易的安全性。该《电子签名法》规定，民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。当事人约定使用电子签名、数据电文的文书、不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。该《电子签名法》重点解决了 5 个方面的问题。一是确立了电子签名的法律效力；二是规范了电子签名的行为；三是明确了认证机构的法律地位及认证程序，并给认证机构设置了市场准入条件和行政许可的程序；四是规定了电子签名的安全保障措施；五是明确了认证机构行政许可的实施主体是国务院信息产业主管部门。

我国《电子签名法》与其他国家或地区的电子签名方面的立法相比，有许多共性及个性方面的特点。

与国外相关法律相比，我国的《电子签名法》共性特点主要体现在三个方面。一是电子签名技术问题复杂，但法律问题相对简单。与传统商务相比，电子商务本身也是商务，只是载体发生了变化，因此在制定《电子签名法》时着重进行了技术方面的规定，而在法律方面大多数只要采用功能等同于传统法律即可，因此文中有关法律描写的章节较少。这一点与国际上相关的法律十分吻合，国际上许多国家的相关立法在法律方面的篇幅也都很少。二是具有很强的国际统一趋势。电子商务最大的优势就是可以利用全球的网络进行网上交易，这就要求《电子签名法》必须具有国际性。在联合国的努力下，目前很多国家有关数据电文和电子签名的规定大体一致。我国《电子签名法》的基本规定与联合国的《电子商务示范法》也基本一致。三是采取了“技术中立”的立法原则。法律只是规定了作为安全可靠的电子签名所应达到的标准，对于采用何种技术手段法律不做规定，因为信息技术发展日新月异，如果法律过多局限于某项技

术，随着技术的变化就可能失效。我国立法初期名称的不断改变就是为了规避因技术发展可能产生的矛盾。

《电子签名法》的个性特点也主要体现在三个方面。一是体现引导性，而不是强制性。如在电子商务活动或电子政务活动中，可以使用电子签名，也可以不使用电子签名；可以用第三方认证，也可以不用第三方认证。二是体现开放性，而不是封闭性。如虽然从条文规定来看主要适用于电子商务，但又不完全局限于电子商务，电子政务也同样适用。另从技术层面上看，并不局限于使用一种技术。三是条文规定体现的是原则性，而不是具体性。如条文中对“第三方”的界定、对认证机构的条件设置等，都是采用了“原则性”而非“具体性”的处理方式，留下了很大的法律空间。

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》(以下简称《管理办法》)。《管理办法》共分 8 章 43 条。它制定的依据是《电子签名法》的第 25 条，该条规定：国务院信息产业主管部门依照本法制定电子认证服务业的具体管理办法，对电子认证服务提供者依法实施监督管理。

《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。再者，从现实情况看，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，也亟需对它们进行规范。

《管理办法》以电子认证服务机构为主线，围绕电子服务行为规范等方面的内容做出了明确规定，而其他问题暂时不予涉及，目的是为了尽快出台，以保证《电子签名法》的顺利施行。随着电子认证服务的发展，还会陆续制定一些相应的管理办法。

《电子签名法》的通过，标志着我国首部“真正意义上的信息化法律”正式诞生，电子签名将获得与传统手写签名和盖章同等的法律效力，它将对我国电子商务、电子政务的发展起到极其重要的促进作用。

本章小结

本章介绍了电子商务安全技术中的有着特别重要地位的数字签名技术。

数字签名其实是伴随着数字化编码的消息一起发送并与发送的信息有一定逻辑关联的数据项，借助数字签名可以确定消息的发送方，同时还可以确定消息自发出后未被修改过。数字签名机制克服了 MAC 的弱点，可以利用公开密钥技术来建立。基于签字内容可分为对整体消息的签字和对压缩消息的签字。随着计算机网络的发展，过去依赖于手书签名的各种业务都可用这种电子化的数字签名代替，它是实现电子贸易、电子支票、电子货币、电子出版及知识产权保护等系统安全的重要保证。但它不同于模拟的手术签名。

目前的数字签名是建立在公共密钥体制基础上，RSA 签名方法和 EIGamal 数字签名方法是两种基本的数字签名方法，许多数字签名方法都是基于这两种算法。RSA 是可逆的公开密钥加密系统，其数字签名过程中运用了消息的验证模式。而 EIGamal 是一种非确定性的双钥

体制，它对同一明文消息，由于随机参数选择的不同而有不同的签名。

盲签名、多重签名、代理签名、定向签名等特殊的数字签名的应用，是根据电子商务具体应用的需要而形成的。盲签名是应用于需要某人对一个文件签名，而又不让他知道文件的内容。多个用户对同一消息进行签名，这就是多重数字签名问题。代理签名就是原始签名者将自己的签名权委托给可靠的代理人，让代理人代表本人去行使某些权力。定向签名方案仅允许特定的收方对签名进行验证。此外，还有双联签名、团体签名、不可争辩签名等等，它们都是针对某些特殊应用的数字签名方案。

数字签名标准（DSS）提供了一种核查电子传输数据及发送者身份的一种方式。DSS 签名为计算和核实数字签名指定了一个数字签名算法，即 DSA，它是一种单向不可逆的公开密钥系统，其安全性取决于离散对数的计算难度。DSA 的验证过程中对资源的处理要比 RSA 更彻底。

数字证书是一个由使用数字证书的用户群所公认和信任的权威机构（即 CA）签署了其数字签名的信息集合。主要有个人数字证书、服务器证书和开发者证书三种类型。数字证书管理机构包括认证机构 CA 和注册机构 RA。它们负责数字证书的申请、发放、分发以及撤销等相关事宜。公钥基础设施 PKI 是一种利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范，用户可利用 PKI 平台提供的服务进行安全通信。为了使一些认证机构能够验证其他认证机构的身份。需要借助于 CA 间的结构关系，目前有树型层次结构、森林型层次结构和通用结构等三种结构。

国际上第一部电子签名法制定于 1995 年，由美国的犹他州制定。截至目前，世界上已有 60 多个国家和地区制定了相关的法律法规。我国第十届全国人民代表大会常务委员会第十一次会议于 2004 年 8 月 28 日通过《中华人民共和国电子签名法》，自 2005 年 4 月 1 日起施行。

复习题

一、选择题

1．下列对于数字签名要求的说法中，不正确的是（　）

A. 收方能够确认或证实发方的签名，但不能伪造。

B. 发方发出签名的消息送收方后，就不能再否认他所签发的消息。

C. 收方对已收到的签名消息不能否认，即有收到认证。

D. 第三者不可确认收发双方之间的消息传送。

2．在电子商务安全技术中，数字签名技术有着特别重要的地位，以下哪些服务要用到数字签名技术（　）

A. 源鉴别　　B. 完整性服务　　C. 不可否认服务　D. 以上都要用到

3．目前应用最广泛的数字签名是（　）。

A. RSA 签名　　B. DSA 签名　　C. ElGamal 签名　D. 椭圆曲线数字签名

4．A 需要 B 对一个文件签名，而又不想让 B 知道文件的内容，可以用（　）

A. 盲签名　　B. 代理签名　　C. 多重签名　　D. 定向签名

5．需要多个用户对同一消息进行签名和认证的签名是（　）

A. 盲签名　　B. 代理签名　　C. 多重签名　　D. 定向签名

6．某公司的经理需要到外地出差，为了不影响公司的业务，该经理委托他的助手在他出差期间代表他在一些重要文件上签字，可以用（　）

A. 盲签名　　B. 代理签名　　C. 多重签名　　D. 定向签名

7．某病人希望他的医疗记录只有他自己才能够验证，可以用（　）

A. 盲签名　　B. 代理签名　　C. 多重签名　　D. 定向签名

8．某持卡人给商家发送订购信息和自己的付款账户信息，但不愿让商家看到自己的付款账户信息，也不愿让处理商家付款信息的第三方看到订货信息，可以用（　）

A. 双联签名　　B. 团体签名　　C. 多重签名　　D. 不可争辩签名

9．《中华人民共和国电子签名法》自（　）起施行。

A. 2002 年 9 月 25 日　　B. 2003 年 9 月 1 日

C. 2004 年 8 月 28 日　　D. 2005 年 4 月 1 日

10．下列哪种签名方案的验证必须在签名者的帮助下完成（　）

A. 双联签名　　B. 团体签名　　C. 多重签名　　D. 不可争辩签名

二、判断题

1．类似于手写签名，数字签名就是在电子文档上附上电子形式的签名。（　）

2．数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密。（　）

3．对同一明文消息，ElGamal 签名不会由于随机参数选择的不同而有不同的签名。（　）

4．用散列函数进行的 RSA 签名比没有用散列函数进行的 RSA 签名速度要快许多。（　）

5．在强盲签名方案中，签名者不能对消息 m 的拥有者进行追踪。（　）

6．在有序多重签名中，签名者不需对他前面的签名进行验证。（　）

7．在代理多重签名中，一个代理签名可以代表多个原始签名人。（　）

8．使用 MR 型定向签名方案时，接收者收到签名后，可利用签名还原消息。（　）

9．在团体签名方案中，即使出现争议，签名的接收者不能决定是团体内哪一个成员签的名，以免暴露成员的身份。（　）

10．DSA 数字签名的安全性基于数论中大整数分解的困难性。（　）

11．认证机构 CA 和注册机构 RA 都可以发放数字证书。（　）

三、填空题

1．根据数字签名所涉及的通信角色可分为直接数字签名和需仲裁的数字签名。

2．目前数字签名方案所基于的数学难题主要有_____和_____。

3．与《电子签名法》相配套，同样于 2005 年 4 月 1 日实施的还有_____。

4．ElGamal 签名方案的安全性基于_____。

5．盲签名的两个要求是_____。

6．MR 型定向签名方案是具有_____功能的签名方案。

7．多重数字签名方案可以分为两类，_____和_____。

8．电子签名立法主要特点有_____、_____、_____。

9．《中华人民共和国电子签名法》自_____起施行。

10.《中华人民共和国电子签名法》共分_____章_____条。
11．数字证书的类型有_____、_____、_____。
12．常用的数字证书分发方法有_____和_____。

四、名词解释题

1．数字签名
2．确定性数字签名
3．散列函数
4．数字摘要
5．盲签名
6．代理签名
7．定向签名
8．多重签名
9．不可争辩签名
10．DSS
11．数字证书
12．PKI
13．交叉认证数字证书

五、简答题

1．什么是数字签名？数字签名应满足哪些要求？
2．简述数字签名与手写签名的区别。
3．简述利用散列函数的 RSA 数字签名过程。
4．简述 ElGamal 算法的签名及验证过程。
5．强盲签名和弱盲签名的区别？
6．什么是多重签名？多重签名有哪几类？他们有什么区别？
7．什么是双联签名？其基本原理是什么？
8．团体签名需要具有哪些特性？
9．什么是不可争辩签名？它有哪些应用？
10．我国《电子签名法》与其他国家或地区的电子签名方面的立法相比，有哪些特点？
11．简述如何利用数字证书实现信息安全。
12．数字证书格式中包含哪些内容？

六、应用题

某个人写了一份遗嘱需要多个律师签名，以保障遗嘱的合法性和可认证性，但不想让任何律师知道。利用你所学的知识，你觉得此人可以使用什么技术？