面向21世纪高职规划教材

俞立平　主编

电子商务认证

机械工业出版社
CHINA MACHINE PRESS

面向21世纪高职规划教材

电子商务认证

主　编　俞立平
副主编　薛庆根　洪　伟　夏德峰
主　审　周曙东

机械工业出版社

本书系统地介绍了电子商务认证理论和实务内容。首先是电子商务认证原理，其次是数字证书的申请，包括单位数字证书、个人数字证书、代码签名证书、服务器证书等，第三是数字证书的应用，包括安全电子邮件、电子支付、电子合同、代码签名认证、服务器认证。此外，还介绍了部分电子商务认证案例及电子商务认证的相关法律。

本书理论联系实际，偏实务操作，基本都能在互联网上实现，再结合案例分析，便于掌握电子商务认证的全貌，同时能进行电子商务认证的实务操作。

本书可作为各高等院校管理类、信息类、计算机类专业的教材，也适合广大电子商务、电子政务从业人员及相关人士使用。本书赠送电子教案，联系邮件 Wangyx@mail. machineinfo. gov. cn。

图书在版编目（CIP）数据

电子商务认证/俞立平主编. —北京：机械工业出版社，2005.4

面向 21 世纪高职规划教材

ISBN 7-111-16384-2

Ⅰ. 电… Ⅱ. 俞… Ⅲ. 电子商务—认证—高等学校：技术学校—教材 Ⅳ. F713.36

中国版本图书馆 CIP 数据核字（2005）第 025260 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：王玉鑫 版式设计：霍永明 责任校对：刘志文
封面设计：陈 沛 责任印制：洪汉军

北京原创阳光印业有限公司·新华书店北京发行所发行

2005 年 5 月第 1 版 第 1 次印刷
1000mm×1400mm B5·8.375 印张·325 千字
定价：22.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68326294
封面无防伪标均为盗版

前　言

21 世纪是一个以数字化、网络化与信息化为特征，以网络通信为核心的信息时代，随着我国加入 WTO，经济全球化已经成为现实。电子商务作为 21 世纪的主要经济增长方式，给各国和世界经济带来巨大的变革，产生深远的影响。电子商务正以其无可比拟的优势和不可逆转的趋势，改变了商务活动的运作模式，对企业的经营方式、支付手段和组织形式提出了强有力的挑战，并给社会经济的各个方面带来根本性的变革。如何保证网上信息安全及交易者身份的认证，已成为发展电子商务的重要环节，网络信息安全和网上信用问题已经成为电子政务、电子商务发展的瓶颈。

在电子商务认证领域，除了一些纯理论和技术书籍外，却没有一本专门的适用于普通商务人员的著作，本书就是在这样的背景下构思和完成的。全书介绍了电子商务认证的原理，电子商务认证的具体内容，包括单位数字证书、个人数字证书、安全电子邮件、电子支付、电子合同、代码签名认证、虚拟专用网与无线认证，此外，还介绍了部分电子商务认证案例及电子商务认证的相关法律。全书理论联系实际，偏实务操作，基本都能在互联网上实现，再结合案例分析，便于掌握电子商务认证的全貌。

俞立平编写了本书的第 1、2、9 章；薛庆根编写了第 5、10 章、洪伟编写了第 7、8 章；夏德峰编写了第 4、6 章；朱鹭编写了第 3 章，俞立平负责全书的统稿。

本书在编写过程中，参考了同行相关资料及有关网站，在此表示感谢。本书的出版得到了江苏省广播电视大学的大力支持，我的导师周曙东教授在百忙中抽出时间为本书审稿，李雪松、周胜、张泰、张运华、婧飞、陈宝兰、胡冰川等同志在本书的编写过程中提供了无私帮助和支持，在此一并致以诚挚的谢意。

由于编者水平有限，书中难免存在一些不妥之处，恳请广大读者和专家不吝赐教，电子信箱：chinayangzhou@yahoo.com.cn。

编　者

2005 年 3 月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章　电子商务认证概述

全球经济发展正在进入信息经济时代，知识经济初见端倪。作为 21 世纪的主要经济增长方式—— 电子商务，给各国和世界经济带来巨大的变革，产生深远的影响。电子商务通过大幅度降低交易成本，增加贸易机会，简化贸易流程，提高贸易效率；电子商务提高生产力，改善物流系统，并推动企业和国民经济结构的改革。对电子商务的关注和投入可以发展新兴产业，创造就业机会，推动国家和全球经济的发展。电子商务是一个新兴市场，而且是一种替代传统商务活动的新形式。它有可能彻底改变贸易活动的本质，形成一套全新的贸易活动框架。但如何保证互联网上信息传输的安全及交易者身份的认证，是发展电子商务的重要环节。

随着我国社会信息化程度的提高，网络信息安全和网上信用问题已经成为电子政务、电子商务发展的瓶颈。数字证书被誉为“网络身份证”，可以提供身份认证、角色授权、数字签名和数据加密等功能，可以广泛应用于网络上的商务活动和政务活动。

认证在电子政务方面的应用有办公信息系统、政府网站以及报税、报关、审批、统计、公证、政府采购、证照审领等网上办事项目，在这些项目的应用中嵌入数字证书，使之成为确保电子政务信息安全的一项重要措施。经济领域，要在网上支付、电子合同、信息查询等方面嵌入数字证书，促进金融信息化、电子商务、企业信息化和社会信用体系的建设。

1.1　电子商务与信息安全

1.1.1　电子商务安全的现状

在互联网环境中开展电子商务，客户、商家、银行等诸多参与者都会担心自己的利益能否真正得到保障。因此国际组织、各国政府以及研究机构都在致力于互联网安全问题的研究，期望逐步把网上的世界变得有序、可信、可靠。只有保证了电子商务的安全，才能够吸引更多的社会公众投身电子商务、应用电子商务、发展电子商务，才能使电子商务健康地生存、高速地发展。

运作在互联网上的电子商务，每天都在进行数以百万次计的各类交易。由于互联网的高度开放性与电子商务所要求的保密性是矛盾的，而互联网本身又没有完整的网络安全体制，因此基于互联网的电子商务安全无疑会受到严重威胁。就目前而

言，电子商务交易的安全性问题已是实现电子商务的关键所在。

在电子商务的发展过程中，各产业对网络已经出现了高度的依赖性。一旦计算机网络受到攻击就不能正常运作，所以这种高度的依赖性使社会经济变得十分“脆弱”。随着经济信息化进程的加快，计算机网络上黑客的破坏活动也随之猖獗起来。黑客行为已对经济秩序、经济建设、国家信息安全构成严重威胁。黑客组织在互联网上公开网址、信道，提供免费的黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍，因此普通人很容易学到网络攻击方式。黑客的袭击在计算机网络发达的国家尤为严重。目前国际黑客对计算机系统中高度敏感的保密信息的攻击和窃取正在日益上升。人们不难想象，黑客的攻击一旦得逞，轻则篡改删除页面，重则导致网络服务乃至整个商务系统瘫痪，长时间内无法恢复，造成不可估量的损失。

2003 年 1 月 26 日，我国台湾媒体报道称，台湾民众上网或玩网络游戏可能觉得速度迟缓或根本无法连线，这并非自己的计算机有问题，而是因为使用微软服务器资料库 SQL 软件的网站，遭到“DDOS_SQLP1434.A”计算机病毒的封包攻击，造成网路大塞车，使网路传输减缓或服务中断。目前美洲、亚洲地区受害情况严重，欧洲尚在了解中，已有许多企业内部网络都已瘫痪。中国互联网主干网也被迫停顿工作长达两小时之久，该病毒体极其短小，却具有极强的传播性，它利用 Microsoft SQL Server 的漏洞进行传播，通过伪造假地址向服务器发送大量访问请求，以此阻塞网络，造成无法访问。由于 Microsoft SQL Server 在世界范围内使用很普及，因此此次病毒攻击导致全球范围内的互联网瘫痪，在中国 80%以上网民受此次全球性病毒袭击影响而不能上网，很多企业的服务器被此病毒感染引起网络瘫痪。美国、泰国、日本、韩国、马来西亚、菲律宾和印度等国家的互联网也受到严重影响。这是继红色代码、尼姆达、求职信病毒后又一起极速病毒传播案例。

全球黑客大赛 2003.7.6 对不少网站进行了攻击，但损失仅限于那些名不见经传缺少安全措施的小型网站。这次黑客大赛在格林威治时间早上 6 点过后迅速开始，几分钟之后就有 300 次网站攻击事件发生，共有 500 余家小型网站被黑，有趣的是，给这次黑客大赛记分的网站也被黑了。

2004 年 9 月，一个每秒钟能感染 20 台计算机的高危病毒——“斯文（Worm. Swen）”在互联网上肆虐传播。这个病毒会实时自动统计已被感染计算机的数量，目前全球被感染计算机台数已达 100 多万台，该病毒具有非常大的迷惑性。此外，该病毒还会关闭一些老版本的反病毒软件与防火墙，使计算机用户的安全防护失效，最终将造成网络严重堵塞。随后不久，震荡波病毒更是横扫天下，感染上万台计算机，强行关机，使你根本无法工作。

电子商务系统在防不胜防的破坏性活动面前，有时会显得软弱无力，谁都无法预测将会受到什么样的挑战。信息安全漏洞难以堵塞，一方面是由于缺乏统一的信息安全标准、密码算法，协议在安全与效率之间难以两全；另一方面，则是由于大

多数管理者对网络安全不甚了解。另外信息犯罪属跨国界的高技术犯罪，要用现有的法律来有效地防范十分困难，现有的科技手段也难以侦察到计算机恐怖分子的行踪，罪犯只需要一台计算机、一条电话线、一个调制解调器就能远距离作案。

在电子商务交易中，商家、客户和银行等各参与方是通过开放的互联网连接在一起的，相互之间的信息传递也要通过互联网来进行，这一变化使交易的风险性和不确定性加大，从而对网络传输过程中数据的安全和保密提出了更高的要求，尤其对于电子商务支付中涉及到的敏感数据，则更需确保其万无一失。

电子商务的安全性是由计算机的安全性，特别是计算机网络的安全性发展而来的。电子商务对网络及应用系统提出了许多安全要求，一方面科学家很难开发出对保障网络安全普遍有效的技术，另一方面又缺乏足以保证这些手段得到实施的社会环境。因此安全问题是电子商务系统所要解决的核心问题。只有建立起科学、合理的安全体系结构，才能保证电子商务交易的全面安全实施。

计算机安全问题基本可以分为两大类：黑客和计算机病毒。

1.1.2 电子商务安全的要素

电子商务安全是一个复杂的系统问题，在使用电子商务的过程中会涉及到以下几个有关安全方面的要素。

（1）可靠性　可靠性是指电子商务系统的可靠程度，是指为防止由于计算机失效、程序错误、传输错误、硬件故障、系统软件错误、计算机病毒和自然灾害等所产生的潜在威胁，采取了一系列的控制和预防措施来防止数据信息资源不受到破坏的可靠程度。

（2）机密性　机密性是指交易过程中必须保证信息不会泄露给非授权的人或实体。电子商务的交易信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来保守机密的；而电子商务则建立在一个较为开放的网络环境上，商业保密就成为电子商务全面推广应用的重要屏障。因此要预防非法的信息存取和信息在传输过程中被非法窃取，确保只有合法用户才能看到数据，防止泄密事件。

（3）完整性　完整性是指数据在输入、输出和传输过程中，要求能保证数据的一致性，防止数据被非授权建立、修改和破坏。电子商务简化了贸易过程，减少了人为的干预，但同时也带来了需要维护商业信息完整、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信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息不相同。信息的完整性将影响到贸易各方的交易和经营策略，保持这种完整性是电子商务应用的基础。

（4）有效性　电子商务以电子形式取代了纸张，那么如何保证这种电子形式

贸易信息为交易各方共同认可是开展电子商务的前提。电子商务作为一种新的贸易形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。一旦签订交易后，这项交易就应受到保护，以防止被篡改或伪造。交易的有效性在其价格、期限及数量作为协议一部分时尤为重要，这就要求制定相应的法律规范保护交易的有效性。2004 年 8 月 28 日，全国人大通过了《中华人民共和国电子签名法》，首次以法律的形式确认了数字签名、电子合同的法律效力。

（5）不可抵赖性　电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是所期望的贸易方这一问题，则是保证电子商务顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易交易所的书面文件上的手写签名或印章来鉴别贸易伙伴，确定合同、契约、交易的可靠性，并预防抵赖行为的发生。这也就是人们常说的“白纸黑字”。一旦交易开展后便不可撤销，交易中的任何一方都不得否认其在该交易中的作为。在电子商务方式下，通过手写签名和印章进行双方的鉴别已是不可能的了。因此要求在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识，使原发送方在发送数据后不能抵赖；接收方在接收数据后也不能抵赖。

1.2 信息加密概述

随着计算机联网的逐步实现，计算机信息的保密问题显得越来越重要。数据保密变换或密码技术，是对计算机信息进行保护的最实用和最可靠的方法。

密码学是一门古老而深奥的学科，它对一般人来说是陌生的，因为长期以来，它只在很少的范围内，如军事、外交、情报等部门使用。计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。随着计算机网络和计算机通信技术的发展，计算机密码学得到前所未有的重视并迅速普及和发展起来。在国外，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

密码是实现秘密通信的主要手段，是隐蔽语言、文字、图像的特种符号。凡是用特种符号按照通信双方约定的方法把电文的原形隐蔽起来，不为第三者所识别的通信方式称为密码通信。在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能了解信息的内容，从而保证信息传输的安全。

任何一个加密系统至少包括下面四个组成部分：

1）未加密的报文，也称明文。

2）加密后的报文，也称密文。

3）加密解密设备或算法。

4）加密解密的密钥。

发送方用加密密钥，通过加密设备或算法，将信息加密后发送出去。接收方在收到密文后，用解密密钥将密文解密，恢复为明文。如果传输中有人窃取，他只能得到无法理解的密文，从而对信息起到保密作用。

1.2.1 密码的分类

从不同的角度根据不同的标准，可以把密码分成若干类。

（1）按应用技术或历史发展阶段划分类

1）手工密码。以手工完成加密作业，或者以简单器具辅助操作的密码，叫作手工密码。第一次世界大战前主要是这种加密形式。

2）机械密码。以机械密码机或电动密码机来完成加、解密作业的密码，叫作机械密码。这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。

3）电子机内乱密码。通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱数，因为其制乱是在加、解密过程中完成的而不需预先制作，所以称为电子机内乱密码。从 20 世纪 50 年代末期出现到 70 年代被广泛应用。

4）计算机密码。是以计算机软件编程进行算法加密为特点，适用于计算机数据保护和网络通信等广泛用途的密码。

（2）按保密程度划分类

1）理论上保密的密码。不管获取多少密文和有多大的计算能力，对明文始终不能得到惟一解的密码，叫作理论上保密的密码，也叫理论不可破的密码。如客观随机一次一密的密码就属于这种。

2）实际上保密的密码。在理论上可破，但在现有客观条件下，无法通过计算来确定惟一解的密码，叫作实际上保密的密码。

3）不保密的密码。在获取一定数量的密文后可以得到惟一解的密码，叫做不保密密码。如早期单表代替密码，后来的多表代替密码，以及明文加少量密钥等密码，现在都成为不保密的密码。

（3）按密钥方式划分类

1）对称式密码。收发双方使用相同密钥的密码，叫作对称式密码。传统的密码都属此类。

2）非对称式密码。收发双方使用不同密钥的密码，叫作非对称式密码。如现代密码中的公共密钥密码就属此类。

3）散列编码。对要加密的原文用一定的算法生成一个摘要，这个摘要对原文而言是惟一的，如果原文被改动，则新生成的摘要肯定不同，一般用来防止对原文的非法修改。

（4）按明文形态划分类

此为试读，需要完整PDF请访问：www.ertongbook.com

1）模拟型密码。用以加密模拟信息。如对动态范围之内，连续变化的语音信号加密的密码，叫作模拟式密码。

2）数字型密码。用于加密数字信息。对两个离散电平构成0、1二进制关系的电报信息加密的密码叫作数字型密码。

（5）按编制原理划分类　可分为移位、代替和置换三种以及它们的组合形式。古今中外的密码，不论其形态多么繁杂，变化多么巧妙，都是按照这三种基本原理编制出来的。移位、代替和置换这三种原理在密码编制和使用中相互结合，灵活应用。

1.2.2 加密的优势与加密强度

1）加密提供以下四种服务，见表1-1。

表1-1 加密提供的服务

服务	解　　释
数据保密性	这是使用加密的通常的原因。通过小心使用数学算法，你可以保证只有你打算接收的人才能查看它
数据完整性	对需要更安全的场合来说数据保密是不够的。数据仍能够被非法破解并修改。一种叫HASH的运算方法能确定数据是否被修改过
认证	数字签名提供认证服务，主要通过非对称加密技术实现
不可否定性	数字签名允许用户证明一条信息交换确实发生过。金融组织尤其依赖于这种方式的加密，用于电子货币交易

2）加密强度。加密强度取决于三个主要因素：

首先是算法的强度，包括几个因素，例如，除了尝试所有可能的密钥组合之外的任何方法都不能解密。必须使用工业标准的算法，它们已经被加密学专家测试过无数次，任何一个新的加密方案如果没有成为标准将不能被应用。

第二个因素是密钥的保密性，一个合乎逻辑但有时被忽略了的方面，如果密钥受到损害，没有任何算法能够发挥作用，因此，数据的保密程度直接与密钥的保密程度相关，注意区分密钥和算法，算法不需要保密，被加密的数据是先与密钥共同使用，然后再通过加密算法。

第三个因素是密钥程度，这是最为人所知的一个方面，根据加密和解密的应用程序，密钥的长度是由“位”为单位，在密钥的长度上加上一位则相当于把可能的密钥的总数乘以2，简单地说构成一个任意给定长度的密钥的位的可能组合的个数可以被表示为2的n次方，这儿的n是一个密钥长度，因此，一个40位密钥长度的配方将是2的40次方或1099511627776种可能的不同的密钥，与之形成鲜明对比的是现代计算机的速度。

尽管可能加密的密钥的总数是非常大的，专门的计算机现在可以在不到一天时间内试验许多种密钥的组合，在 1933 年，Michael wiener 研制出一种专门的计算机，专门破译 DES（一种使用 56 位密钥的算法）。在研制的过程中他发现设计所需要的费用是呈直线型的，考虑到他的结果和摩尔效应（计算机的计算能力大约每 18 个月增长一倍）。其实任何密码都能破解而无论它的长度，想象一下这样的密钥利用现代的机器去破解是多么的快速。简单地说，一个人或组织在密钥破解的装备上花的钱越多，则密钥就会被越快地破解，这种断言已经得到证实。曾经有个电子基金组织利用建造的专门计算机在不到三天的时间内破译了一个 64 位基础的密码。

1.2.3 加密技术

1. DES 数据加密标准

数据加密标准（DES）是美国经长时间征集和筛选后，于 1977 年由美国国家标准局颁布的一种加密算法。它主要用于民用敏感信息的加密，后来被国际标准化组织接受作为国际标准。DES 主要采用替换和移位的方法加密。它用 56 位密钥对 64 位二进制数据块进行加密，每次加密可对 64 位的输入数据进行 16 轮编码，经一系列替换和移位后，输入的 64 位原始数据转换成完全不同的 64 位输出数据。DES 算法仅使用最大为 64 位的标准算术和逻辑运算，运算速度快，密钥生产容易，适合于在当前大多数计算机上用软件方法实现，同时也适合于在专用芯片上实现。

它用且只用一个密钥对信息进行加密和解密，由于加密和解密用的是同一密钥，所以发送者和接收者都必须知道密钥。

对称加密方法对信息编码和解码的速度很快，效率也很高，但需要细心保存密钥。如果密钥泄露，以前的所有信息都失去了保密性，致使以后发送者和接收者进行通信时必须使用新的密钥。将新密钥发给授权双方是很困难的，关键是传输新密码的信息必须进行加密，这又要求有另一个新密钥。对称密钥的另一个问题是其规模无法适应互联网这类大环境的要求，想用互联网交换保密信息的每对用户都需要一个密钥，这时密钥组合就会是一个天文数字。如果每两个人要求一个密钥，n 个人彼此之间进行保密通信就需要 n (n–1) /2 个密钥。尽管对称加密在很多情况下都很有效，但也有比较大的局限性。所有各方都必须相互了解，并且完全信任，而且每一方都必须妥善保管一份密钥。如果发送者和接收者处在不同地点，就必须当面或在公共传送系统（电话系统、邮政服务）中无人偷听偷看的情况下交换密钥。在密钥的交换过程中，任何人一旦截获了它，就可用它来读取所有加密消息。

因为密钥必须安全地分发给通信各方，所以对称加密的主要问题就出在密钥的分发上，包括密钥的生成、传输和存放。在网络上进行密钥发布非常麻烦，如果企业有几千个在线顾客，那么密钥的发布就很难满足要求。此外对称加密不适合同以前互不认识的交易方在公共网络上交换消息。例如，企业如果想安全地与在线顾客

交易，每个顾客就都必须有企业分配给它的独特密钥，这个密钥也必须通过独立的安全渠道（如电话）传送给顾客，整个成本很高。所以，由于提供安全密钥管理的难度很大，对称加密也就很难成为电子商务中占主导地位的加密方法。

对称密钥的常用算法是DES，该算法1972年由IBM公司提出，后被国际标准化组织接受，并作为数据加密标准。对称密钥最大的特点是加、解密速度快，所以一般用来加密较长的信息，不足是需要的密钥太多，而且安全性也不够高。

DES主要的应用范围有：

（1）计算机网络通信　对计算机网络通信中的数据提供保护是DES的一项重要应用。但这些被保护的数据一般只限于民用敏感信息，即不在政府确定的保密范围之内的信息。

（2）电子资金传送系统　采用DES的方法加密电子资金传送系统中的信息，可准确、快速地传送数据，并可较好地解决信息安全的问题。

（3）保护用户文件　用户可自选密钥对重要文件加密，防止未授权用户窃密。

（4）用户识别　DES还可用于计算机用户识别系统中。

DES是一种世界公认的较好的加密算法。自它问世以来，成为密码界研究的重点，经受住了许多科学家的研究和破译，在民用密码领域得到了广泛的应用。它曾为全球贸易、金融等非官方部门提供了可靠的通信安全保障。但是任何加密算法都不可能是十全十美的。它的缺点是密钥太短（56位），影响了它的保密强度。此外，由于DES算法完全公开，其安全性完全依赖于对密钥的保护，必须有可靠的信道来分发密钥。如采用信使递送密钥等。因此，它不适合在网络环境下单独使用。

针对它密钥短的问题，科学家又研制了80位的密钥，以及在DES的基础上采用三重DES和双密钥加密的方法。即用两个56位的密钥K1、K2，发送方用K1加密，K2解密，再使用K1加密。接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

2. IDEA国际数据加密算法

国际数据加密算法IDEA是瑞士的著名学者提出的。它在1990年正式公布并在以后得到增强。这种算法是在DES算法的基础上发展出来的，类似于三重DES。发展IDEA也是因为感到DES具有密钥太短等缺点。IDEA的密钥为128位，这么长的密钥在今后若干年内应该是安全的。

类似于DES，IDEA算法也是一种数据块加密算法，它设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。与DES的不同处在于，它采用软件实现和采用硬件实现同样快速。

由于IDEA是在美国之外提出并发展起来的，避开了美国法律上对加密技术的诸多限制，因此，有关IDEA算法和实现技术的书籍都可以自由出版和交流，可极大地促进IDEA的发展和完善。但由于该算法出现的时间不长，针对它的攻击也还

不多，还未经过较长时间的考验。因此，尚不能判断出它的优势和缺陷。

3. Clipper 加密芯片

密码虽然可为私人提供信息保密服务，但是它首先是维护国家利益的工具。正是基于这个出发点，考虑到 DES 算法公开后带来的种种问题，美国国家保密局（NSA）从 1985 年起开始着手制定新的商用数据加密标准，以取代 DES。1990 年开始试用，1993 年正式使用，主要用于通信交换系统中电话、传真和计算机通信信息的安全保护。

新的数据加密标准完全改变了过去的政策，密码算法不再公开，对用户提供加密芯片（Clipper）和硬件设备。新算法的安全性远高于 DES，其密钥量比 DES 多 1000 多万倍。据估算，想破译至少需要 10 亿年。为确保安全，Clipper 芯片由一个公司制造裸片，再由另一公司编程后方可使用。

由于完全是官方的封闭控制，该算法除可提供高强度的密码报密外，还可对保密通信进行监听，以防止不法分子利用保密通信进行非法活动，但这种监听是在法律允许的范围内进行的。官方控制也成为美国民间反对该方案的一个重要原因。

Clipper 芯片主要用于商业活动的计算机通信网。NSA 同时在着手进行政府和军事通信网中数据加密芯片的研究，并作为 Clipper 的换代产品。它除了具有 Clipper 的全部功能外，还将实现美国数字签名标准（DSS）和保密的 HASH 函数标准以及用纯噪声源产生随机数据的算法等。

目前，美国 IBM 笔记本计算机上就使用了该加密芯片，一旦忘记密码，IBM 公司也不能解密，只有更换主机板，其安全是相当可靠的。

4. 公开密钥密码体制

传统的加密方法是加密、解密使用同样的密钥，由发送者和接收者分别保存，在加密和解密时使用，采用这种方法的主要问题是密钥的生成、注入、存储、管理、分发等很复杂，特别是随着用户的增加，密钥的需求量成倍增加。在网络通信中，大量密钥的分配是一个难以解决的问题。

为了解决这个问题，1977 年，麻省理工学院的三位教授（Rivest、Shamir 和 Adleman）发明了 RSA 公开密钥密码系统。他们的发明为敏感信息的交换方式带来了新的途径。在此系统中有一对密码，给别人用的就叫公钥，给自己用的就叫私钥。这两个可以互相并且只能为对方加密或解密，用公钥加密后的密文，只有私钥能解。用私钥加密的密文，也只能用公钥解密。

为提高保密强度，RSA 密钥至少为 512 位长，一般推荐使用 1024 位。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的 DES 或 IDEA 对话密钥加密，然后使用 RSA 密钥加密对话密钥和信息摘要。对方收到信息后，用不同的密钥解密并可核对信息摘要。

例如，张三想发给李四信息，可以从公开渠道取得李四的公钥，然后用李四的公钥对自己要发送的信息加密；由于密钥对是惟一的，信息加密后，只有李四才能用其私钥解密信息后阅读。同样，李四也可向张三发一条私人信息，用张三的公钥对信息加密。张三收到李四的信息后可用自己的私钥解密信息后阅读。一旦信息从服务器下载并解密后，就以明文的形式保存在接收者的计算机上，这时接收者就可以阅读了。

与对称加密相比，非对称加密有若干优点：①在多人之间进行保密信息传输所需的密钥组合数量很小。在 n 个人彼此之间传输保密信息，只需要 n 对密钥，远远小于对称加密系统需要 n (n–1) /2 的要求。②公钥的发布不成问题，它没有特殊的发布要求，可以在网上公开。③非对称加密可实现数字签名。这就意味着将电子文档签名后再发给别人，而签名者无法否认。也就是说，采用非对称加密技术，除签名者外他人无法以电子方式进行签名，而且签名者事后也不能否认曾以电子方式签过文档。

非对称加密系统也有缺点，例如，加密、解密的速度比对称加密的速度慢得多。当商家和顾客在互联网上进行商务活动的时候，加密、解密累积的时间会很多。非对称加密系统并不是要取代对称加密系统，恰恰相反，它们是相互补充的。如可用非对称加密在互联网上传输对称加密系统的私有密钥，从而实现更有效的安全网络传输。

RSA 算法的加密密钥和加密算法分开，使得密钥分配更为方便。它特别符合计算机网络环境。对于网上的大量用户，可以将加密密钥用电话簿的方式印出。如果某用户想与另一用户进行保密通信，只需从公钥簿上查出对方的加密密钥，用它对所传送的信息加密发出即可。对方收到信息后，用仅为自己所知的解密密钥将信息脱密，了解报文的内容。由此可看出，RSA 算法解决了大量网络用户密钥管理的难题。

RSA 并不能替代 DES，它们的优、缺点正好互补。RSA 的密钥很长，加密速度慢，而采用 DES，正好弥补了 RSA 的缺点。即 DES 用于明文加密，RSA 用于 DES 密钥的加密。由于 DES 加密速度快，适合加密较长的报文；而 RSA 可解决 DES 密钥分配的问题。美国的保密增强邮件（PEM）就是采用了 RSA 和 DES 结合的方法，目前已成为 E-Mail 保密通信标准。

非对称加密安全可靠，但加密速度慢，所以一般只适合加密较短的信息，如信用卡号、对称密钥等。

1.2.4 签名

信息鉴别的方法可以使信息接收者确定信息发送者的身份以及信息在传送过程中是否被改动过。如果信息的收发双方对该信息的内容及发送端没有争执的话，

那么只采用鉴别技术也就足够了。鉴别技术可以保证在信息传送过程中对信息内容的任何改动都可以被检测出来，并且能够正确地鉴别出信息发送方的身份。但是，当信息的收发方对信息的内容及发送端产生争执时，只用鉴别技术就不够了。

收方可以伪造一份信息，从中获得非法利益，并且自称该信息是由发送方发过来的。例如，银行通过通信网络传送一张支票，收方就可以对支票数额进行改动，并且声称他已收到了这张支票。利用前面的鉴别技术丝毫也解决不了这个问题，因为鉴别使用了一个收/发双方共享的对称密钥，这样才能使发放产生一个鉴别码而接收方又能对该鉴别码进行校验。但是收方也能对他伪造的信息产生一个合法的鉴别码，这给整个系统带来严重的安全问题。

在许多情况下，特别是商业系统中，通常都利用书面文件来规定契约性的责任，虽然鉴别技术可以完全有效的防止第三者的介入，但是却丝毫不能防止接收者的伪造。问题的另一方面是发送方可能是不诚实的，由于他发送的信息变得对他很不利，而要逃避责任，那么发送方就可能谎称他从未发过这个信息。在整个争执过程中，第三方也无法分辨哪种情况是真实的。

为了解决上述问题，就必须利用另外一种安全技术—— 数字签名。签名必须达到如下效果：在信息通信的过程中，接收方能够对公正的第三方（可以是双方事前统一委托其解决某一问题或某一争执的仲裁者，如法院或公证机构）证明其收到的报文内容是真实的，而且确实是由那个发送方发过来的，同时签名还必须保证发送方发送后不能根据自己的利益否认他所发送过的报文，而收方也不能根据自己的利益来伪造报文或签名。

对于数字签名的产生过程来说，必须有足够的信息才能对报文和签名进行验证，没有足够的信息就会给伪造或否认报文提供可乘之机。但是收发双方用来产生与校验的签名的信息不能完全相同，因为一旦接收方能够用发送方用来产生签名的相同信息（算法和参数）来证实报文和签名，那么收方同样也能够用它来伪造报文和签名。所以签名产生者与签名证实者之间的相同信息绝对不能太多。如果发送方事后担心接收方否认接收到了他所发送的报文，那么发送方应能够请求获得报文证明，也就是说由接收方对发送方提供收到报文的证据。例如，如果甲方把报文发送给乙方，那么乙方就要向甲方发送一份签了名的报文证明收到了，由于这份报文有乙方的签名，所以乙方是不能抵赖他所收到的报文的。

随着信息经济和知识经济的迅猛发展，无纸办公彻底改变了过去手工操作的各种不便，显得更安全、更有效、更迅速、更简洁、更方便。数字签名以其独特的优势适应了这种发展，在无纸办公中占有十分重要的地位。例如，对公司内部有下级呈给上级请求批阅的公文在以往只需领导大笔一挥签名盖章，以个人的笔迹来证明其真实性。但手写的文件签名非常容易伪造。除此之外，签名者还可以否认签名，宣称它是伪造的。但在无纸办公年代，计算机网络中传送的电子公文又如何盖章

此为试读，需要完整PDF请访问：www.ertongbook.com