第一章　电子商务概述

1.1 引　　言

当今世界，数字经济(Digital Economy）的两大组成部分：电子商务（Electronic Commerce,简称 EC)和信息技术(Information Technology ,简称 IT)正以惊人的速度发展,信息技术的发展以及它给我们生活方式带来的影响是几年前所不可预见的，甚至我们在一年前作出的种种估计或预测，在今天看来都是保守的。生存、发展、需求和利益是数字经济全球化的重要因素。

随着以计算机网络为核心的信息技术的飞速发展， Internet 的普及应用，使得电子商务已成为网络技术应用一个崭新的发展方向。电子商务不仅给社会提供了无限的商机，也改变着传统的企业经营管理模式，同时也对我们的日常生活和工作的方方面面产生不同程度的影响。网上交易、网上支付、网上交流以及在线支付以其高效益、简化管理、全球性等特点日益受到各国政府和企业界的重视。新一代电子商务正在改变企业经营的面貌，正逐步渗透进我们的生活。这里买主有了广大的新视野，在网上可以从数以万计的供应商中，借助搜索引擎，选取中意的商品或服务。卖方可以在网上建立网页（Home Page）这些网页可以随设立者的目的，提供各种各样的功用，可以有最简单的商品广告，可以有文字、图像、声音说明、性能示范等高度互动的多媒体商业活动。在我国， 1998 年末，上海书城网上书店开业，人们只要在浏览器中键入 www.bookmail.com.cn 就可以实现在上海书城的网上购书活动。 1999 年 3月 9 日，全国最大的国有零售书店——北京图书大厦网上书店正式开业，用户在网上便可以浏览到图书大厦所经营的 16 万种图书。

直观地看，电子商务只是把传统的商务活动移植到计算机网络上，实现商务电子化。然而，电子商务决不是表面看上去那么简单，它是一个复杂的系统工程，涉及信息安全、支付环境、物流体系、资本运作、信息基础设施、法律政策等多方面的内容，它们组成了电子商务的宏观环境，任何一个环节处理得不好，都不可避免地制约或阻碍电子商务的正常发展。由此可以看出，在现阶段，电子商务发展面临许多问题，有技术的，也有非技术的。

本书以电子商务的安全为主题，重点讨论电子商务系统所面临的安全问题以及相应的安全技术解决方案。

安全是电子商务的生命。在电子商务开始逐步普及的今天，无论是加入到电子商务的企业、商家，还是在网上购物的一般消费者，都无一例外地关注它的安全问题。例如，为确保电子商务的成功，企业和商家必须能够得到可靠的信用信息来确保支付，而一般消费者则要求他们的信用信息不会落入第三方手中，避免自身利益受到损害。安全问题威胁着交易中每一方的利益，客户由此产生的疑虑会影响到交易的成败，甚至会影响电子商务

的进一步普及和推广。“电子商务，安全先行”已成为业界的一种共识。

1.2 电子商务

在涉及电子商务的各种文献中，几乎无一例外要对电子商务的概念进行定义，尽管电子商务的定义已经出现了不少，但至今也没有出现一个标准的电子商务定义，也许将来也不会有，原因就在于随着信息技术不断发展，电子商务的内涵也会不断丰富。其实对电子商务的概念如何描述并不是关键的，关键在于把握电子商务特性、电子商务与传统商务的区别以及电子商务赖以存在和发展的基础。

在今天看来，从前的一些电子商务系统，包括现在仍然存在的一些电子商务系统，只不过是完成了商务活动的电子化作业，并不具备一个完善的电子商务系统的特征。这些系统缺少电子商务赖以生存的安全技术和支撑环境，安全性、公平性得不到保障，难以有效地防止诸如交易抵赖、交易诈骗等事件的发生。

在数字经济的时代里，电子商务就是在信息安全技术的保障下，利用计算机网络技术实现可跨地区的商业贸易活动过程的电子化、自动化。

图 1.1 是电子商务的结构示意图。

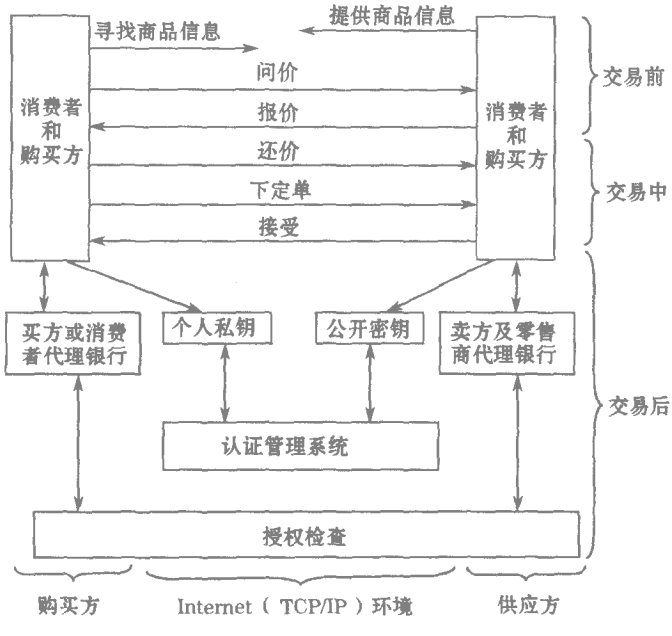

图 1.1 电子商务的结构示意图

1.2.1 电子商务的发展历程

电子商务的发展经历了三个阶段：

第一阶段：即初始电子商务，这个阶段的电子商务不能算是严格意义上的电子商务，主要表现为网上黄页、机构上网以及虚拟主机，其主要特征是网上信息发布。

第二阶段：即简单电子商务，它在初始电子商务基础上提供了互动式信息交换，其主

要特征为：初始电子商务＋网上目录、网上订货……

第三阶段：即完整电子商务，这是电子商务的最高境界，它不再是仅仅用来进行信息发布，而是帮助企业打破时空限制，实现在线交易和在线支付，其主要特征为：简单电子商务＋网上结算、配送……

图 1.2 表示出电子商务发展的三个阶段及相互关系。

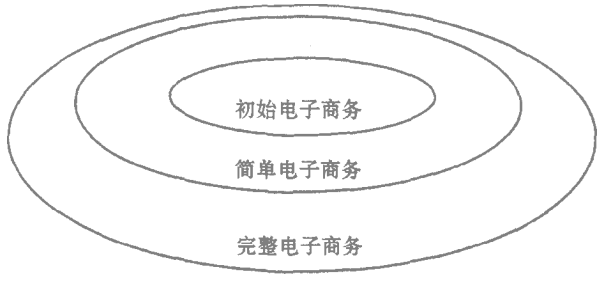

图 1.2　电子商务的发展历程

1.2.2　电子商务的模式

一个系统的安全性要求与系统的模式和应用环境等多方面因素密切相关，因此，下面简单介绍电子商务的模式，以期能更好地对电子商务的安全需求作出深入的分析。

从电子商务的参与对象上分析，电子商务的模式主要包括：

◆ 企业⇔企业(B2B)；

◆ 企业⇔消费者 B2C)；

◆ 消费者⇔消费者(C2C)。

企业与企业之间的电子商务可以使企业减少采购时间，减少库存开销，并形成虚拟的策略联盟，加强企业间的技术合作。在所有的电子商务模式中，B2B 的发展潜力最大。从近期的形式上看，它的发展势头较猛，特别是在国际商贸领域，具有广阔的前景。目前，中国出口商品网(www. chinaproducts. com) 已开通此项业务，由北京师范大学和教育部基础教育课程教材发展中心共同组建的中国基础教育网 (www. cbe21. com) 也将建设大规模的 B2B 网上教学用品采购系统，以降低教育部门的采购成本。

企业与消费者之间的电子商务可以使企业形成独特的产品，扩大市场，为消费者提供超越时空的“ AAA” 式服务，即在任何时间(Anytime)、任何地点(Anywhere) 以任何方式 (Anyhow) 为消费者提供全天候的服务。B2C 模式在一段时间内曾被炒作得很厉害。从方便性、实用性上看，B2C 模式发展的前景也是较为乐观的，但是，在我国发展 B2C 模式目前还有一定阻力，其制约因素包括：配套的物流体系、安全支付环境发展相对滞后等，而且，价格上和传统商务相比也没有什么优势，虽然所有这些都应该只是暂时的。

消费者与消费者之间电子商务的典型应用是消费者之间竞价购物，其中一个最为著名的例子是网上在线拍卖站点 ebay(www. ebay. com) ，这是一个在网上提供信息中介，吸引用户拍卖、竞买的新型商务模式，它的出现以及所呈现的发展势态，确实令许多业界人士称奇。目前 ebay 公司的注册用户以达 800 万，1999 年上半年其股票市值突破了 300 亿美元。雅宝竞价交易网 (www. yabuy. com) 是我国 C2C 模式电子商务的一个突出代表。

然而，应该看到，在我国，大众的购物心理和习惯、相关法律保障不健全、安全支付不完善等问题是近一段时间内制约 C2C 电子商务模式发展的主要因素。

1.2.3 电子商务系统的业务范围

电子商务的应用十分广泛，按商务形式划分，电子商务主要包括：

- 邮购零售：零售商接收基于数字或传统目录的电子订单及支付，并配送实物商品；
- 网上金融服务：金融服务电子化，如家庭银行、股票交易等；
- 网上信息产品销售：与邮购零售类似，但商品主要是受版权保护的数字化信息产品，如计算机软件、电子图书、数字视听产品等；
- 电子商厦：这是一个将众多服务提供者组织起来的虚拟商厦，其服务范围涵盖了从为主机上的内容提供目录服务到记费服务；
- 合同签定：双方或多方交换一份合同的签名备份；
- 在线交易：提供商品的目录服务，并通过网络完成订购及支付；
- 在线信息服务：在网络上提供有偿信息服务，如金融资讯等；
- 网上拍卖：通过网络进行商品或服务的竞价销售；
- 预订：通过客户的预订来为客户提供服务，如预订新闻服务等；
- 彩票销售：通过网络进行数字化的各类彩票的销售、兑奖；
- 旅游服务：提供旅游信息服务和旅游支付业务。

在电子商务的这些业务中，目前呈现较好发展态势的主要包括图书、计算机软件、CD 等。受“触摸式”传统购买观念的影响，通过网上销售的商品类型以那些无须当面挑选的产品为主。当然，我们并没有穷尽所有可能的电子商务应用，因为，需求是发展的最大驱动力，各种形式的电子商务业务将会随着人们需求的发展而层出不穷。

1.2.4 电子商务与传统商务的比较

传统商务与电子商务相比有许多相同点，如它们都以商务为其核心内容，并以利益为原生驱动力，在形式上是很相似的。以购物为例，图 1.3 给出了现实生活中顾客进超市购物的流程，图 1.4、图 1.5 则描述了通过 Internet 进行购物的流程，在图 1.4 的流程中，支付是非在线进行的，而图 1.5 的流程中支付是在线进行的。

尽管传统商务与电子商务在形式上具有很强的相似性，但是，从安全与信任角度看，二者有着本质的不同。在传统商务中，交易的双方基本是面对面的，因此，交易过程中的安全性和相互信任关系是比较容易建立的。

在电子商务活动中，交易双方的联系是通过网络进行的。客户和商家之间一般都不存在预先建立的商务关系，因此，他们之间没有相互信任关系：在送货之前，商家会希望得到付款的某些保证；而客户在付款之前则更希望商家能对所送商品的质量、规格等属性方面作出具体保证。在目前的大部分电子商务系统中，这两个方面的要求并没有得到很充分的满足。由于 Internet 的开放性和不安全性，使得参与电子商务的主体的利益受到威胁。后面会对电子商务所面临的威胁以及造成这些威胁的原因进行深入分析。

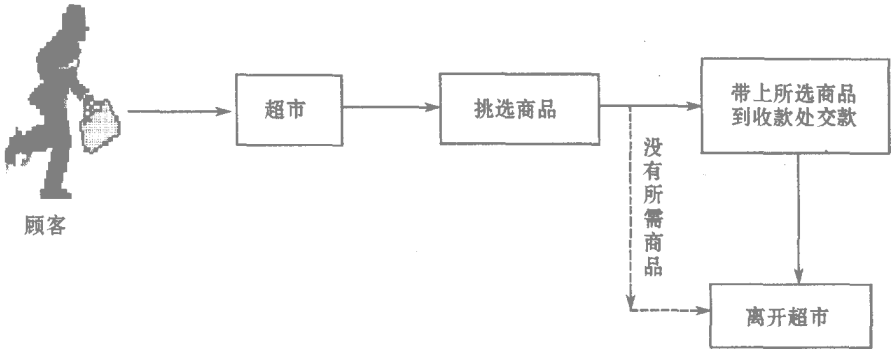

图 1.3 现实生活中顾客进超市购物流程图

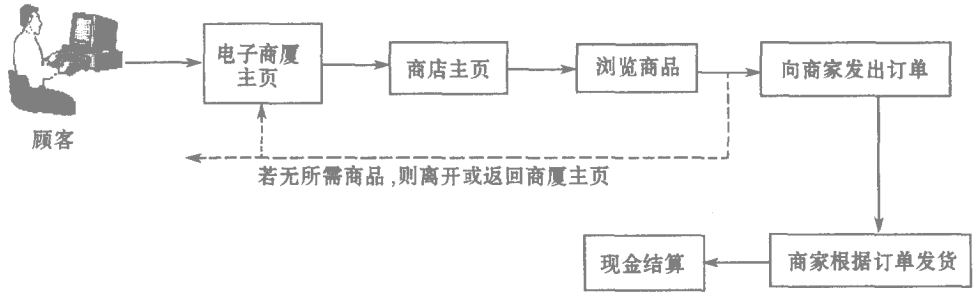

图 1.4 非在线支付的 Internet 购物流程

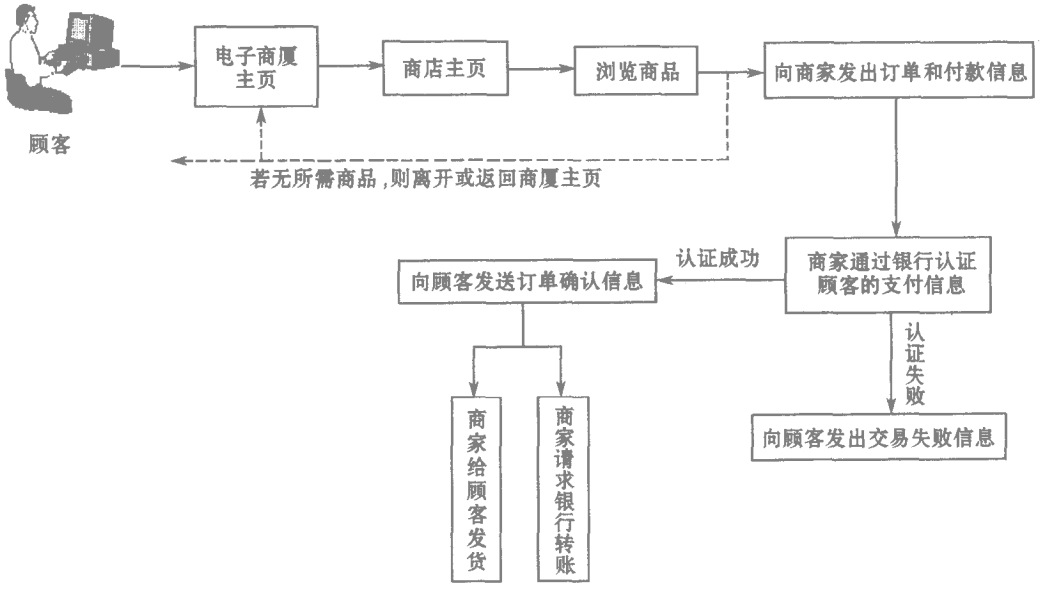

图 1.5 在线支付的 Internet 购物流程

1.2.5 电子商务的特征

从上面的比较可以看出，电子商务和传统商务相比有如下特征：

普遍性：电子商务作为一种新型的交易方式，将生产企业、流通企业以及消费者和政府带入了一个网络经济、数字化生活的新天地；

方便性：在电子商务环境中，人们不再受地域的限制，客户能以非常简捷的方式完成过去较为繁杂的商务活动，如通过网络银行能够全天候地存取资金、查询信息等，同时使得企业对客户的服务质量可以大大提高；

整体性：电子商务能够规范事务处理的工作流程，将人工操作和电子信息处理集成为一个不可分割的整体，这样不仅能提高人力和物力的利用，也可以提高系统运行的严密性；

安全性：在电子商务中，安全性是一个至关重要的核心问题，它要求网络能提供一种端到端的安全解决方案,如加密机制、签名机制、安全管理、存取控制、防火墙、防病毒保护等等，这与传统的商务活动有着很大的不同；

协调性：商务活动本身是一种协调过程，它需要客户与公司内部、生产商、批发商、零售商间的协调，在电子商务环境中，它更要求银行、配送中心、通信部门、技术服务等多个部门的通力协作，往往电子商务的全过程是一气呵成的。

1.3 电子商务的发展状况及趋势

全球电子商务强劲增长的动力，可以归纳为四项因素：

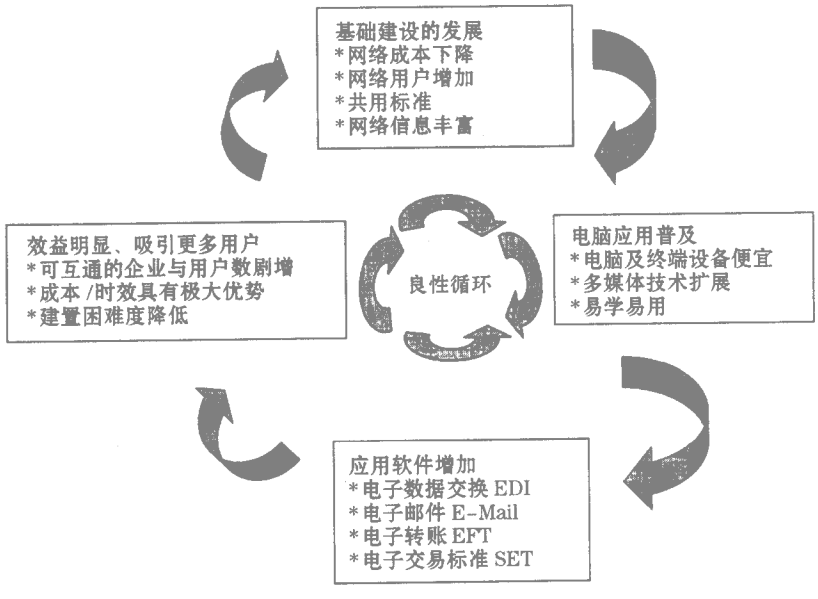

图 1.6 电子商务成长的动力

第一，世界各国竞相推动国家信息网络基础建设，使网络费用不断下降，用户大幅度增加，网上信息资源日益丰富。

第二，由于网上可用信息资源增多，导致更多人买电脑上网。

第三，上网用户增多，网络应用软件有广大买主，鼓励了网络应用软件的开发。

第四，上网人数增多，为电子商务活动开辟了赢利空间，为企业竞争提供了新利器，遂激励了国家信息网络基础建设的发展。

以上四项因素构成良性循环，使电子商务得以持续加速成长，如图 1.6 所示。

1.3.1 全球电子商务发展趋势

全球经济一体化是世界经济发展的主要趋势与重要特征。作为全球经济一体化的产物和重要推动力，电子商务的应用和推广给社会、经济的发展带来了极大的效益，将成为全球经济的最大增长点之一。发达国家纷纷制定政策，发展中国家也正在加紧制定总体发展战略，大力促进电子商务在国民经济各个领域的应用，以求赢得新的竞争优势。

据统计，全球互联网用户到 2000 年 6 月已经达到 2.6 亿以上，预计今后四年内全球上网人数将增至 10 亿，平均每个月增加 100 万户。网上销售方面，1998 年全球销售额达 500 亿美元，比 1997 年增长近 20 倍。全球 B2B 电子商务交易额预计将从 2000 年的 3360 亿美元增至 2005 年的 6.3 兆亿美元，整个经济中 B2B 电子商务所占比例将从目前的 3% 增至 42% ，其中计算机和电信业正成为最大的 B2B 电子商务产业，到 2005 年将有 1 兆亿美元的市场销售额。研究表明，未来数年，亚太 B2B 电子商务市场交易额将从 1999 年的 92 亿美元增长到 2004 年的 9958 亿美元，B2B 交易网站将会成为市场主导。电子商务潜在的巨大发展空间不言而喻。

目前世界范围的电子商务立法工作也正处于一个探索和实验的研究阶段。从 1996 年 5 月联合国制定通过《电子商务示范法》到 1997 年 4 月欧盟出台《欧洲电子商务倡议书》，以及 1997 年 7 月 1 日美国发布《全球电子商务政策框架白皮书》提出发展全球电子商务的五项基本指导原则与九个国际协作领域等等，世界各国纷纷规划 制定电子商务发展的法案、政策和框架，以促进电子商务的发展和应用。

1.3.2 中国电子商务总体情况和特点

一、总体情况

我国电子商务是在国家公共通信网络的基础上，以国家金关工程为代表并以外经贸管理服务为重要内容的电子商务工程逐步发展起来的。我国政府相继实施了“金桥”、“金卡”、“金关”等一系列金字工程，为我国电子商务的发展做了良好的铺垫。

截止 2000 年，我国电子商务网站已达 1100 余家，电子商务交易额 1999 年为人民币 1.8 亿元，其中 B2C 交易额为 1.44 亿元，比 1998 年增长一倍以上， 2000 年则达到 4 亿元，增长态势强劲。从行业应用看，证券公司 金融结算机构 民航票务中心 信用卡发放等领域均已成功进入电子商务领域，并进行了大量可靠的交易，这些为电子商务的发展奠定了基础，也积累了丰富的经验。目前我国信息产业总规模已超过 1.4 万亿元人民币，电信业务平均增长率为 33% ，信息产品制造业平均增长率已超过 30% 。中国电子商务正由起步迈入繁荣阶段。

二、发展特点

第一，理性加强，发展战略开始转变。中国电子商务经历了从疯狂到理性的过程，整个行业目前正在进行实质的变化。很多企业正悄然改变原有发展战略，开始寻求新的商业模式，并注重从注意力经济向购买力经济转变。

第二，传统产业涉足电子商务。众多传统产业认识到互联网的商业价值和电子商务前景，纷纷涉足电子商务并显示出勃勃生机。

第三，网络建设发展迅速，大众化程度明显提高。从 1999 年开始，网站数量增长迅速，上网门坎不断降低，逐渐贴近大众化。

三、基础设施

我国电子商务的基础设施建设取得了很大的成绩，国内主干网带宽有了较大的扩展，个人和企业上网费用已经开始下调，网民和企业对网络环境的要求已经从速度和价格等因素提高到保障服务质量，网络服务开始进入具体和务实的发展阶段。

1999 年，我国国际线路总容量为 351M，2000 年，国际线路总容量达到 1234M，增长了 3 倍多。IP 电话出口带宽总量达 56M。2000 年一季度，信息产业部已组织实施国际出入口带宽扩容工作。

1999 年底，光缆总长度为 100 多万公里，局用程控交换机总容量为 1.6 亿门，建成全国性计算机系统 108 个，与 70 个国家和地区建立了直达线路，与 59 个国家和地区的 108 个移动通信网络开通了国际漫游。

2000 年 3 月，各级政府已申请域名 2400 个，其中 720 个政府部门以 Web 服务器向社会提供服务，利用公用网组建的全国性计算机信息系统达到 86 个。1999 年 3 月和 10 月，电信资费作出重大调整，上网费用有较大程度下降。

四、网络连接

1994 年 9 月，中国公用计算机互联网（ChinaNET）启动。同年 10 月，中国教育和科研网（CerNET）启动。1995 年 1 月，中国电信开始向社会提供互联网接入服务。1995 年 4 月，中国科学院启动百所联网工程，在此基础上发展形成中国科技网（CstNET）。1996 年 9 月，中国金桥信息网（ChinaGBN）向社会提供互联网接入服务。1997 年，中国公用计算机互联网、中国科技网、中国教育和科研计算机网、中国信息网实现了互通。

五、电子商务模式

我国电子商务模式趋向多样化，目前主要有企业对企业（B2B）企业对消费者（B2C）等。

1.3.3 中国电子商务发展的对策

我国电子商务与国外有较大差距，应制定长远规划，分步、分阶段实施电子商务，主要应注意以下几个方面。

建立电子商务框架：由于互联网的全球性特点，不能采用传统的各国独立的方式来发展。应认真研究我国发展电子商务的对策，提出对我国有利的“游戏规则”，积极参与电子商务问题的国际谈判，参与对话，形成电子商务的国际框架。

突出重点，由点带面：目前我国尚处于电子商务发展的初期，在具体实施上应分步进行。首先在比较适合电子商务发挥长处的领域中推行电子商务，如银行、民航、证券等，在

此基础上带动其它的领域。其次，对经济比较发达、信息化程度相对较高、对电子商务有需求和有效益的地区，应不失时机的发展各种方式的电子商务，发挥其示范效应，以便向其它地区推广普及。第三，采取在电子商务和传统商务的结合中逐步扩大电子商务比重的做法。

加强标准制定和安全技术研究，加快法律法规建设：组织银行、信息产业、税务、海关、法律等有关部门集中解决电子支付、安全保密、法律认可等电子商务急需解决的问题，并进行标准制定。尽快建立发展我国信息产业的法律环境和政策环境，并在实践中逐步加以完善。

推动企业信息化进程：企业信息化程度对电子商务的发展有很大影响，要制定发展规划，推动企业信息化进程。

普及电子商务常识、提高电子商务意识：目前人们的电子商务意识还很淡薄，对计算机和网络掌握的知识不够。让更多的人认识计算机、认识网络、了解电子商务是发展电子商务的前提和基础，要加强相关人才的培养。

1.4 电子商务对社会经济的影响

随着电子商务魅力的日渐显露,虚拟企业、虚拟银行、网络营销、网上购物、网上支付、网络广告等一大批前所未闻的新词汇正在为人们所熟悉和认同，这些词汇同时也从另一个侧面反映了电子商务正在对社会和经济产生的影响。

电子商务将改变商务活动的方式：传统的商务活动最典型的情景就是“推销员满天飞”“采购员遍地跑”“说破了嘴、跑断了腿”消费者在商场中筋疲力尽地寻找自己所需要的商品。现在，通过互联网只要动动手就可以了，人们可以进入网上商场浏览、采购各类产品，而且还能得到在线服务；商家们可以在网上与客户联系，利用网络进行货款结算服务；政府还可以方便地进行电子招标、政府采购等。

电子商务将改变人们的消费方式：网上购物的最大特征是消费者的主导性，购物意愿掌握在消费者手中；同时消费者还能以一种轻松自由的自我服务方式来完成交易，消费者主权可以在网络购物中充分体现出来。

电子商务将改变企业的生产方式：由于电子商务是一种快捷、方便的购物手段，消费者的个性化、特殊化需要可以完全通过网络展示在生产厂商面前，为了取悦顾客，突出产品的设计风格，制造业中的许多企业纷纷发展和普及电子商务，如美国福特汽车公司在1998年的3月份将分布在全世界的12万个电脑工作站与公司的内部网连接起来，并将全世界的1.5万个经销商纳入内部网。福特公司的最终目的是实现能够按照用户的不同要求，做到按需供应汽车。

电子商务将对传统行业带来一场革命：电子商务是在商务活动的全过程中，通过人与电子通信方式的结合，极大地提高商务活动的效率，减少不必要的中间环节，传统的制造业籍此进入小批量、多品种的时代，“零库存”成为可能，传统的零售业和批发业开创了“无店铺”“网上营销”的新模式；各种在线服务为传统服务业提供了全新的服务方式。

电子商务将带来一个全新的金融业：由于在线电子支付是电子商务的关键环节，也是电子商务得以顺利发展的基础条件，随着电子商务在电子交易环节上的突破，网上银行、

银行卡支付网络、银行电子支付系统以及电子支票、电子现金等服务，将传统的金融业带入一个全新的领域。1995 年 10 月，全球第一家网上银行“安全第一网络银行”(Security First Network Bank)在美国诞生，这家银行没有建筑物，没有地址，营业厅就是首页画面，员工只有 10 人,与总资产超过 2000 亿美元的美国花旗银行相比,“安全第一网络银行”简直是微不足道，但与花旗银行不同的是，该银行所有交易都通过互联网进行，1996 年存款金额达到 1400 万美元,到 1999 年已达到 4 亿美元。

电子商务将转变政府的行为：政府承担着大量的社会、经济、文化的管理和服务的功能，尤其作为“看得见的手”，在调节市场经济运行，防止市场失灵带来的不足方面有着很大的作用。在电子商务时代，当企业应用电子商务进行生产经营，银行是金融电子化，以及消费者实现网上消费的同时，将同样对政府管理行为提出新的要求，电子政府或称网上政府，将随着电子商务发展而成为一个重要的社会角色。

总而言之，作为一种商务活动过程，电子商务将带来一场史无前例的革命。其对社会经济的影响会远远超过商务的本身，除了上述这些影响外，它还将对就业、法律制度以及文化教育等带来巨大的影响。电子商务会将人类真正带入信息社会。

1.5 电子商务所面临的问题

电子商务的发展前景无疑是非常远大的，但是鉴于我国起步较晚，信息化和网络化程度不高等原因，要在全国顺利普及，还有很多问题需要解决。

1.5.1 网络基础设施建设问题

要想实现真正实时的网上交易，要求网络有非常快的响应速度和较高的带宽，这必须由硬件提供对高速网络的支持。而我国由于经济实力和技术方面的原因等，网络的基础设施建设还比较缓慢和滞后，已建成的网络其质量离电子商务的要求相距甚远。另一方面，上网用户少，网络利用率低，致使网络资源大量闲置和浪费，投资效益低，严重制约着网络的进一步发展。同时，与银行、税务等十几个部门的联网尚未实现。因此，如何加大基础设施建设的力度，提高投资效益，改变网络通信方面的落后面貌，应是促进电子商务应用普及的首要问题。

1.5.2 安全问题

安全问题是企业应用电子商务最担心的问题，而如何保障电子商务活动的安全，将一直是电子商务的核心研究领域。作为一个安全的电子商务系统，首先必须具有一个安全、可靠的通信网络，以保证交易信息安全、迅速地传递；其次必须保证数据库服务器绝对安全，防止黑客闯入网络盗取信息。对于中国来说，网络产品几乎都是“舶来品”，本身就隐藏着不安全隐患，加之受技术、人为等因素的影响，不安全因素更显突出。目前，电子签名和认证是网上比较成熟的安全手段，而在我国大多尚处在对 SSL 协议的应用上，在 SET 协议上的应用试验刚刚成功，而要完全实现 SET 协议安全支付，就必须有一个 CA 认证中心，而目前在我国 CA 认证权的归属问题尚未确定，在信息安全保密体制上究竟谁来管理？怎么管理？采取什么有序的管理办法？这些问题亟待解决。图 1.7 是一个安全完整

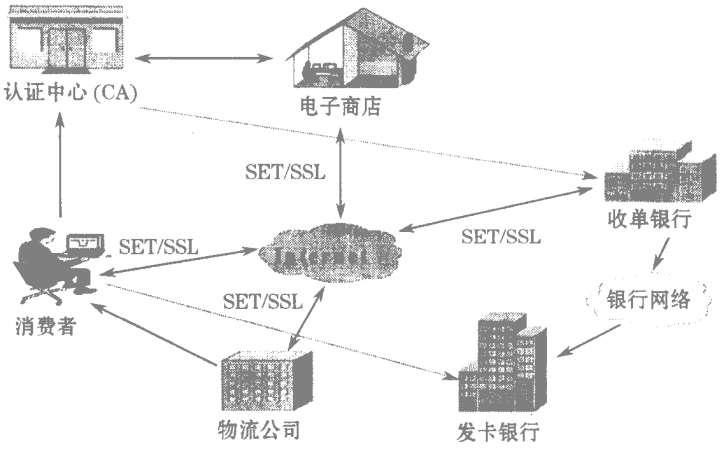

图 1.7　安全完整的电子商务运作环境示意图

的电子商务运作环境示意图。

1.5.3　网上支付问题

电子商务的核心内容是信息的互相沟通和交流，交易双方通过 Internet 进行交流，洽谈确认，最后才能发生交易。这时对于通过电子商务手段完成交易的双方来说，银行等金融机构的介入是必须的，银行所起的作用主要是支持和服务，属于商业行为。但从整个电子商务网络的发展来看，将来要在网络上直接进行交易，就需要通过银行的信用卡等各种方式来完成交易，以及在国际贸易中通过与金融网络的连接来支付和收费。而目前我国各个国有专业银行网络选用的通信平台不统一，不利于各银行间跨行业务的互联、互通和中央银行的金融监管以及宏观调控政策的实施。另外，各行信用卡标准不一样，不能通用，尚不能用信用卡实现网上支付。

1.5.4　电子商务法律问题

电子商务是世界性的经济活动，尽管基于 Internet 的电子商务在世界各国得到迅速发展，但要全面展开电子商务活动，必须建立必要的法律框架。在网络空间中，由于传统的法律不再适用，而各国的法律又互不相同，哪一个国家的法律，也不能作为电子商务的法律依据，因此有必要制定通用的法律，并得到国际间的认可和共同遵守。

一个成功的电子交易必须签订一个双方确认的合同，明确彼此间希望得到的利益及必须承担的义务，只有双方遵守有关电子交易的法律，Internet 电子商务才能发挥效益。在 Internet 上开展电子商务，还面临着一系列诸如税收、国际民事诉讼、电子合同有效性、知识产权、隐私权等法律问题。

为此，必须制定、完善电子商务的法律，才能在 Internet 环境中正常的开展电子商务。

1996 年 12 月，联合国大会以 51/62 号决议通过了《电子商务示范法》(简称示范法)，这是世界上第一个关于电子商务的法律。它的出台，使电子商务的主要法律问题有了可靠依据。1998 年以来，联合国国际贸易法委员会还开始了重点在于数字签名和认证许可的模型及法律的制定工作。强劲的电子商务全球化趋势要求无论哪个国家采纳何种体制

或者法律原则，必须拥有使文件和交易得到国际认可的机制。在电子商务环境中，要求对有关公司、客户和合同的某些信息进行核查，这对于在电子交易中建立信任是必不可少的，尤其是初次交易时更是如此。到目前为止，数字签名技术的使用和有关法律的应用一直是电子市场中关于身份验证和交易认证的中心问题。许多国家（包括美国的许多州）已经通过数字签名和身份认证的法律。

1.5.5 企业计算机应用水平落后、网络意识淡薄

目前我国绝大部分企业正忙于解决吃饭问题，信息部门设在总工程师办公室，大部分企业缺乏计算机，少数企业拥有计算机也主要应用于文字处理和计算，产、供、销、人、财、物等重要资源的管理，大多未实现电子化。信息加工和处理手段落后，信息处理能力仅是世界平均水平的 2.1% ，且仍以提供单纯的技术产品信息为主，不擅长动态信息的跟踪和获取。企业对电子商务的需求非常淡薄， 12 亿人中仅有 210 万网络用户，除去免费用户外，真正交费上网者很少，企业用户还没大量出现。企业的信息化只是在理论界、信息产业界热度很高，而在企业中热度并不高，从而造成经营决策的被动局面。

1.5.6 企业管理水平落后、经营方式陈旧

我国许多企业的管理处于主观、随意的经验管理阶段，而管理程序化、科学化是实现电子商务的基本要求。目前的不规范管理，只能使计算机简单模拟原来手工操作流程，从而加大系统实现的难度，增加投资成本，降低电子商务的投资收益率。电子商务的应用也会因公司的不同而五花八门，不仅不能提高工作效率，相反还会降低原来工作效率。同时，几千年来留下的传统的手工作业的商业模式在人们头脑中根深蒂固，要在现阶段改造这样的商业环境，以适应电子商务产生的新的市场竞争格局，是相当艰巨的。

1.5.7 商家信誉问题

电子商务的应用领域分两类：企业间交易和个人消费者与企业之间的交易。就其发展过程来看，它又必然经历一个从简单的商情查询到网上购物和实现交易的阶段。据调查，1997 年消费者用于购买网上服务和产品的总价值为 32 亿美元，但上网寻找产品信息后再进行离线购物的达 42 亿美元，这说明建立通畅快速的购物网络并不困难，但建立成熟可靠的消费体系和互相信任的市场运作方式，绝不是一蹴而就的事。当传统的购物方式引发的各种纠纷还在“ 3.15 ”消费者权益日频频曝光的环境下，消费者如何信任互不照面的网上交易？在这方面我们与国外的差距，技术手段上的原因是次要的，而人的基本素质却是根本的。

1.6 电子商务主要的安全要素

电子商务发展的核心和关键问题是交易的安全性。由于 Internet 本身的开放性，使网上交易面临了种种危险，也由此提出了相应的安全控制要求。

有效性：电子商务(EC) 以电子形式取代了纸张，那么如何保证这种电子形式的贸易信息的有效性则是开展 EC 的前提。EC 作为贸易的一种形式，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。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、确定的地点是有效的。

机密性：EC 作为贸易的一种手段，其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达到保守机密的目的。EC 是建立在一个较为开放的网络环境上的（尤其 Internet 是更为开放的网络),维护商业机密是 EC 全面推广应用的重要保障。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。

完整性：EC 简化了贸易过程，减少了人为的干预，同时也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的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是 EC 应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。

可靠性／不可抵赖性／鉴别：EC 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进行交易所期望的贸易方这一问题则是保证 EC 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、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。这也就是人们常说的“白纸黑字“。在无纸化的 EC 下，通过手写签名和印章进行贸易方的鉴别已是不可能的。因此，要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。

审查能力：根据机密性和完整性的要求，应对数据审查的结果进行记录。

1.7 电子商务采用的主要安全技术及其标准规范

考虑到安全服务各方面要求的技术方案已经研究出来了，安全服务可在网络上任何一处加以实施。但是，在两个贸易伙伴间进行的 EC,安全服务通常是以‘端到端’形式实施的（即不考虑通信网络及其节点上所实施的安全措施）。所实施安全的等级则是在均衡了潜在的安全危机、采取安全措施的代价及要保护信息的价值等因素后确定的。这里将介绍 EC 应用过程中主要采用的几种安全技术及其相关标准规范。

1.7.1 加密技术

加密技术是 EC 采取的主要安全措施，贸易方可根据需要在信息交换的阶段使用。目前，加密技术分为两类，即对称加密和非对称加密。

1.7.2 密钥管理技术

根据密码体制的不同，密钥管理技术又包括：对称密钥管理、公开密钥管理及数字证书技术。

一、对称密钥管理技术

对称加密是基于共同保守秘密来实现的。采用对称加密技术的贸易双方必须要保证采用的是相同的密钥，要保证彼此密钥的交换是安全可靠的，同时还要设定防止密钥泄密和更改密钥的程序。这样，对称密钥的管理和分发工作将变成一件潜在危险的和繁琐的过程。通过公开密钥加密技术实现对称密钥的管理，使相应的管理变得简单和更加安全，同时还解决了纯对称密钥模式中存在的可靠性问题和鉴别问题。

贸易方可以为每次交换的信息（如每次的 EDI 交换）生成惟一一条对称密钥，并用公开密钥对该密钥进行加密，然后，再将加密后的密钥和用该密钥加密的信息（如 EDI 交换）一起发送给相应的贸易方。由于对每次信息交换都对应生成了惟一的一条密钥，因此各贸易方就不再需要对密钥进行维护和担心密钥的泄露或过期。这种方式的另一优点是即使泄露了一把密钥也只将影响一笔交易，而不会影响到贸易双方之间所有的交易关系。这种方式还提供了贸易伙伴间发布对称密钥的一种安全途径。

二、公开密钥管理／数字证书

贸易伙伴间可以使用数字证书（公开密钥证书）来交换公开密钥。国际电信联盟（ITU）制定的 X.509 标准对数字证书进行了定义，该标准等同于国际标准化组织（ISO）与国际电工委员会（IEC）联合发布的 ISO/IEC 9594—8:195 标准。数字证书通常包含有证书所有者（即贸易方）的惟一标识、证书发布者的惟一标识、证书所有者的公开密钥、证书发布者的数字签名、证书的有效期及证书的序列号等。证书发布者一般称为认证中心（CA），它是贸易各方都信赖的机构。数字证书能够起到标识贸易方的作用，是目前 EC 广泛采用的技术之一。

三、密钥管理相关的标准规范

目前国际有关的标准化机构都着手制定关于密钥管理的技术标准规范。ISO 与 IEC 下属的信息技术委员会（JTC1）已起草了关于密钥管理的国际标准规范。该规范主要由 3 部分组成 第 1 部分是密钥管理框架；第 2 部分是采用对称技术的机制；第 3 部分是采用非对称技术的机制。该规范现已进入到国际标准草案表决阶段，并将很快成为正式的国际标准。

1.7.3 数字签名

数字签名是公钥密码体制的另一类应用。它的主要方式是：报文的发送方利用 Hash 函数，生成报文文本的一个散列值（或报文摘要），发送方用自己的私钥对这个散列值进行加密来形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先用同样的 Hash 函数生成接收到的原始报文的散列值（或报文摘要），接着再用发送方的公开密钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别和不可抵赖性（详细介绍参照 2.1.4 节）。

ISO/IEC JTC1 已在起草有关的国际标准规范。该标准的初步题目是“信息技术——安全技术——带附件的数字签名方案”，它由概述和基于身份的机制两部分构成。

1.7.4 Internet 主要的安全协议 S-HTTP

S-HTTP (安全的超文本传输协议)是对 HTTP 安全特性的扩充，增强了报文的安全性,它是基于 SSL 技术的。该协议为 WWW 的应用提供完整性、鉴别、不可抵赖性及机密性等安全措施。目前，该协议正由 Internet 工程任务组起草 RFC 草案。

1.7.5 UN/EDIFACT 的安全

EDI 是 EC 最重要的组成部分，是国际上广泛采用的自动交换、处理和管理商业信息技术。UN/EDIFACT 报文是惟一的国际通用的 EDI 标准。利用 Internet 进行 EDI 已成为人们日益关注的领域，保证 EDI 的安全成为主要解决的问题。联合国下属的专门从事 UN/EDIFACT 标准研制的组织一UN/ECE/WP4(即贸易简化工作组)于 1990 年成立了安全联合工作组（UN-SJWG）来负责研究 UN/EDIFACT 标准中实施安全的措施。该工作组的工作成果将以 ISO 的标准形式公布。

在 ISO 将要发布的 ISO 9735(即 UN/EDIFACT 语法规则）新版本中包括了描述 UN/EDIFACT 中实施安全措施的 5 个新部分。它们分别是：第 5 部分批式 EDI(可靠性、完整性和不可抵赖性)的安全规则 第 6 部分安全鉴别和确认报文（AUTACK）;第 7 部分批式 EDI(机密性)的安全规则 第 9 部分安全密钥和证书管理报告（KEYMAN）第 10 部分交互式 EDI 的安全规则。

UN/EDIFACT 的安全措施主要是通过集成式和分离式两种途径来实现。集成式的途径是通过在 UN/EDIFACT 报文结构中使用可选择的安全头段和安全尾段来保证报文内容的完整性、报文来源的鉴别和不可抵赖性。

而分离式途径则是通过发送 3 种特殊的 UN/EDIFACT 报文（即 AU TCK、KEY-MAN 和 CIPHER 来达到保障安全的目的。

对于 SSL 协议、安全电子交易规范 SET 和 EDI，将在第二章和第四章详细介绍。

第二章　电子商务的安全基础

2.1　密 码 技 术

密码技术包括密码学与密码分析学两个相辅相成的部分：通信方希望信息保密使用密码，而攻击者则想法破译密码。长久以来，虽然密码技术在谍报、外交和军事等重要部门广泛应用，但鲜为普通人关心和了解。利用密码技术进行的保密通信模型可用图 2.1 说明。

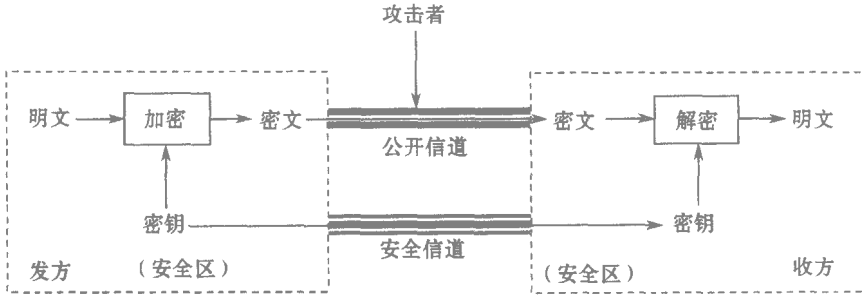

图 2.1　利用密码技术的保密通信模型

随着计算机网络技术的发展及其应用的推广，人们对信息的安全也越来越关注，作为信息安全技术核心的密码技术也得到快速发展，其应用也从传统的加密功能拓展到更广泛的加密、签名与认证、完整性保护等功能，从军事、外交、谍报部门扩展到社会、经济各部门，对于电子商务来说，密码技术已成为其健康、有序发展的一个重要基础。

下面将对用于电子商务的一些密码技术进行简要的介绍，分为对称密码、公钥密码、HASH 函数三部分。

2.1.1　对称密码

对称密码的特征是加、解密双方在加、解密过程中使用相同密钥。它包括序列密码与分组密码两类。在电子商务中广泛使用的是分组密码，主要用于对发送的数据（如交易票据）进行加密保护，只有合法的接受方能够知道数据的内容。国际通用的分组密码算法最典型的是 DES 算法以及其替代算法 AES。

一、DES

目前在金融界广泛使用的数据加密标准（DES），由美国联邦信息处理标准 FIPS46-3 定义，其加密技术是 IBM 公司在 20 世纪 70 年代中期开发的，主要用途是保护商业信息和政府无密级的敏感信息。美国国家标准技术研究协会每隔五年就重新审议 DES 是否继续作为联邦信息处理标准。在 1994 年的时候，NIST 宣布 DES 标准要延续到 1998 年，

1998 年后就不再批准 DES 作为联邦信息处理标准。 DES 算法是迄今为止得到最广泛应用的一种算法,但是,随着近年来计算能力的与日俱增,DES 的密钥较短 (56bit) 的弱点受到了强大的攻击,1998 年 5 月,美国 EFF(Electronic Frontier Foundation) 宣布,他们一台 20 万美元的计算机改装成的专用解密机,用 56 小时就破译了 DES 算法。为了克服 DES 密钥较短的缺点,提出了 3DES 这个变异的加密标准,安全性得到了较大程度的提高,但是,也带来了运算效率降低的负面影响。

客观地说,即使在今天 DES 仍不失为一个优秀的密码算法,因为有这样一个事实是不容否认的:

在 DES 公布 10 多年后,密码研究人员研制出破译 DES 最为有效的几项技术, DES 的设计者们在 DES 的设计之初就已经考虑了。

因此,DES 的不安全不是说它的编码原理不安全了,而是体现在以两个方面,一是密钥太短;另一方面是其设计原则没有公开,有理由怀疑它有陷门。因此, DES 最终退出历史舞台也是一种必然。

二、AES

1997 年 1 月 2 日,美国国家标准技术研究所(NIST) 宣布启动高级加密标准 (AES) (Advanced Ecryption Standard) [http://aes. nist. gov/aes/, http://www. nist. gov/aes]的开发研究计划,并于 1997 年 9 月 12 日正式发出征集算法的公告,算法要求在 1998 年 6 月之前提交。征集公告同时指明了 NIST 的目标,就是要确定一种无密级的、公开透露加密算法的、免费使用的、全世界通用的 AES。算法的最低要求是,必须是采用对称密钥密码实现的分组密码,并支持 128bit 分组长度和 128、192、256bit 密钥长度。

2000 年 10 月 2 日,美国商务部长宣布美国最终推荐的高级加密标准是 Rijndael。开发并提交 Rijndael 算法的是两位比利时密码专家,一位是国际质子世界 (Proton World International)公司的 Joan Daemen 博士,另一位是利文 Katholieke 大学电器工程系的 Vincent Rijmen 博士。

一旦把高级加密标准作为 FIPS 颁布后,该算法就成为美国政府机构保护敏感 (无密级) 信息的正式加密算法。NIST 建议商业和美国的非政府机构接受并使用 AES 和 NIST 的其它密码标准,但不作硬性规定。

在高级加密标准成为正式标准后, NIST 会像对待其它加密标准一样,继续对 Rijndael 进行密码分析,跟踪其发展情况,每隔五年进行一次正式评估。要在充分考虑具体情况的基础上,在适当时间补充完善这一新标准。一旦发生问题需要立即处理, NIST 会当机立断地用其它加密标准代替 Rijndael。从目前的分析上看,除非有了比密钥穷举更有效的攻击,或者未来的科技有了新的发展,否则,AES 的潜在安全期会超过二十年。

对称算法最主要的问题是:由于加、解密双方需要使用相同的密钥,因此在发送、接收数据之前,必须完成密钥的分发。因此,密钥的分发便成了该加密体系中的最薄弱因而风险最大的环节,需要采用相配套的密钥管理机制来确保其安全应用。

2.1.2 公钥密码体制

公钥密码的特征是加、解密密钥不同,发送方与接收方都有自己的公私钥对。对应于传统的加、解密,发送方使用接收方的公开密钥对信息进行加密,接收方使用自己的私钥