第 3 章　电子商务的应用

本章要点

- 网上交易、网上支付的基础知识
- 网上支付工具及网上银行
- 第三方支付平台的概念及特点
- 国内主要的第三方支付平台
- 电子商务的安全及威胁
- 电子商务安全技术
- 文件传输协议 FTP

3.1 网 上 交 易

3.1.1 网上交易概述

1．定义

网上交易是买卖双方利用互联网进行的商品或服务的交易。常见的网上交易主要有：企业间交易、企业和消费者间交易、个人间交易及企业和政府间交易等。

网上交易是信息技术与经济发展相结合的产物，是一种新的交易方式，是电子商务的一种重要模式。开展网上交易有助于提高交易效率，降低交易成本，拉动消费，促进商品和各种生产要素的自由流动及国民经济又好又快的发展。

2．网上交易参与方

网上交易参与方包括网上交易的交易方（即买方和卖方）和网上交易服务提供者。网上交易服务提供者，根据其服务内容可以分为以下两种。

1）网上交易平台服务提供者。从事网上交易平台运营并为买卖双方提供交易服务，如阿里巴巴、淘宝和当当网等。

2）网上交易辅助服务提供者。为优化网上交易环境和促进网上交易，为买卖双方提供身份认证、信用评估、网络广告发布、网络营销、网上支付、物流配送及交易保险等辅助服务，例如第三方支付平台支付宝和财付通等。

3．网上交易参与方注意事项

近年来，国内电子商务发展迅猛，但关于网上交易的相关法规条款还没有形成整套系统，尚需完善。尤其目前的网上交易条款还存在一些模糊区，一些不良卖家趁机钻空子、刷信用或诈骗消费者的情况时有发生，网上交易的“诚信及安全”成了困扰消费者的首要问题。网络安全成为当前各业界十分关注的问题，网络钓鱼、病毒及木马等网络安全隐患的存在给电子商务及网络支付等应用的开展造成了障碍。

（1）认识网上交易的特点

网上交易通过互联网进行信息交流，洽谈、签订合同乃至履行合同，其优点是效率高、成本低。但交易方在了解对方真实身份、信用情况及履约能力等方面有一定难度，存在一定的违约和欺诈风险。交易方应认识网上交易的特点，谨慎交易，积极防范风险，防患于未然。

（2）了解交易对方的真实身份

交易各方在交易前要尽可能多了解对方的真实身份、信用状况及履约能力等信息，可以要求对方告知或向交易服务提供者询问，必要时也可以向有关管理或服务机构查询。

卖方应在适当的时间将自身与交易有关的真实信息告知对方，例如营业执照和特殊业务许可证照的有关信息，实体经营地址和真实有效的联系方式等。如果卖方拒绝提供

基本身份信息，买方要谨慎对待，慎重交易，警惕和防范利用网上交易进行欺诈的行为。

（3）注意支付安全

交易各方如果选择网上支付方式，要通过安全可靠的第三方支付平台进行，及时保存支付信息，增强网上支付的安全意识。交易各方进行网下支付的，要充分考虑货到付款、预付货款等方式的特点，注意资金的使用安全，以防上当受骗。

（4）保存网上交易记录

交易各方可以自行保存各类交易记录，以作为纠纷处理时的证据。贵重商品与重要服务的交易，可以生成必要的书面文件或采取其他合理措施留存交易记录。

3.1.2　网络证券交易

网络证券是电子商务应用较好的领域，主要业务集中在网上证券交易和各种增值服务上，目前已成为证券交易的主要方式。网上交易系统发展速度很快，网上进行的交易平均占比从 2006 年的 40%发展到目前的 70%，最高达到 90%以上。

随着互联网在中国的逐步普及，网上交易已成为投资者使用的主要手段，其交易量已远远超过传统的现场交易。网上证券交易正日益成为全球证券市场交易委托的发展主流，这在很大程度上改变了投资者和证券商的活动方式。中国证券监管层从技术层面看到了市场应用前景，积极支持网上证券交易的发展。网上交易之所以能如此快速的发展，是因为其自身的优势。首先，与其他的电子商务活动相比，网上证券交易有几个特点：一是网上证券交易没有物流环节，大大节约了成本；二是网上证券交易避免了电子商务活动中的直接支付问题，通过交易收费、服务免费的运作方式，证券商以证券交易手续费作为收入来源，这也避免了直接支付带来的网上交易安全性的问题；三是交易的单一性和标准化降低了网上证券交易的复杂程度，这避免了关于外形、质量等方面的顾虑；四是证券公司作为网上证券交易服务提供者是具有专业资格的，其权威性与可靠的信誉度增加了网上证券交易的安全感。其次，网上交易还有无可比拟的便捷性，主要体现在两个方面：一是交易可以与看盘同步进行，这增加了买卖决策的安全性；二是交易过程十分快速，委托的全过程甚至能够简化到鼠标的一次点击。可以说，便捷性适应了证券交易的特性要求。

网络证券交易作为一种新型的证券交易方式，具有委托快捷便利，可视化强，资金网上自助管理及保证金存取方便等特点。它体现出显著的优势：成本低、虚拟性、个性化、服务质量高及融合性强等。目前，证券业的网络交易是在国内开展较早、规模较大、比较成功的金融电子商务。

下面以招商证券网上交易系统为例，简单介绍网上交易的方法。

1．开户

持本人身份证和同名银行存折或银行卡，到招商证券营业部或营业网点均可办理深沪 A、B 股证券账户卡和开立资金账户，同时办理资金存取业务，即将用户银行卡或存折上的钱和保证金账户内的资金互转。

2．网上交易

招商证券提供两种网上交易方式：一种是使用专业版交易软件，另一种是登录招商证券网的“快速交易通道”进行交易。

（1）专业版交易软件

将专业交易软件下载到本地计算机的网上交易方式，其优势是交易速度快，安全性高；具备功能超强的行情分析工具，操作界面友好，支持各种上网代理服务器；稳定性好，可靠性强，能支持交易高峰期高并发流量。如果经常网上交易，建议尽量选择该方式。

登录招商证券网站（http://www.newone.com.cn/），单击导航条中的【软件下载】按钮，进入“下载交易软件”页面，如图 3-1 所示。单击“招商证券网上交易全能版”对应的【下载】按钮，即可下载该软件。

图 3-1　在招商证券网站下载交易软件

将该下载软件安装在自己的计算机中，打开登录界面，输入“牛卡号”、“交易密码”和“验证码”，单击【登录】按钮，即可进入软件，如图 3-2 所示。

图 3-2　登录交易软件

1）银证转账。进行证券交易前，需要将银行存折或卡上的存款划拨到牛卡资金账户上。单击软件主界面左下方的“银证业务”中的【银证转账】按钮，弹出转账的信息，如图 3-3 所示。选择银行并输入“转账金额”，单击【转账】按钮，就可以将银行卡或存折上的钱转入牛卡账户中，转账成功后就可以进行证券交易了。

图 3-3　银证转账

2）查看行情。要快速查找某一只股票的行情，可以直接输入该股票的代码或者拼音简称，按 Enter 键即可，如图 3-4 和图 3-5 所示。

图 3-4　输入股票的代码或者拼音简称

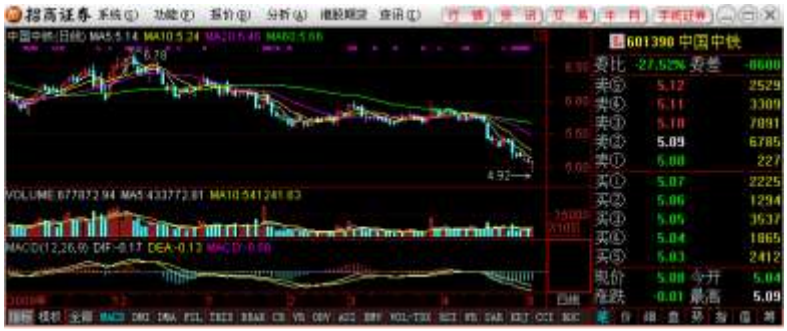

图 3-5　查看股票行情

选择一支股票，按 F10 键即可查看该股票的各股资料，例如最新动态、公司概况及持股情况等信息。

3）进行交易。该软件提供了丰富的交易功能，包含股票业务、开放式基金业务、组合通和 ETF 篮子买卖等多种功能，如图 3-6 所示。

（a）买入

（b）卖出

（c）对买对卖

图 3-6　丰富的交易功能

此外，该软件还为用户提供了很多贴心的服务，如专家在线，用户可以在线咨询专家。短信理财通服务，能为用户提供更及时、更周到的证券咨询服务，该服务项目分两部分，一部分是免费类定制：账户信息提示，包括新股申购提示、新股中签提示及持仓股重大公告等服务项目；另一部分是单项类定制：股票行情和投资资讯，包括定时行情发送、大盘指数报送及股票到价提示等服务项目。

（2）快速交易通道

除了使用专业软件进行操作，还可以直接从招商证券牛网（www.newone.com.cn）登录，不需要下载安装、不受代理服务器限制、能穿越防火墙在局域网内使用。目前招商证券“快速交易通道”能够提供较全的交易服务，包括开放式基金的开户、申购和赎回等功能。缺点是行情分析功能弱，操作时交互性差。

3.2　网 上 支 付

随着 Internet 技术和电子商务的迅速发展，网上支付系统已经成为现代金融领域不可或缺的组成部分。快捷、方便和安全的网上支付给商务活动带来新的改变和发展，电子商务的广阔发展前景吸引了更多资源投入，促使电子支付技术日益成熟和完善，而更为成熟安全的电子支付技术又促进了电子商务的飞速发展。

根据 iResearch 艾瑞咨询推出的《2009－2010 年中国网上支付行业发展报告》统计，2009 年中国网上支付市场规模将达 5766 亿元人民币，相比 2008 年的 2743 亿元增长 110.2%。网上支付交易额连续 5 年增速超 100%。2005～2009 年，这 5 年间交易额规模增长了近 30 倍，如图 3-7 所示。

目前，我国网上支付市场呈快速发展态势，自 2005 年第三方支付交易额年年翻番增长。网上支付已成为互联网上的明星行业，支付宝以 49.8%的市场份额占领军地位，它也成为互联网上令人期待的新星。

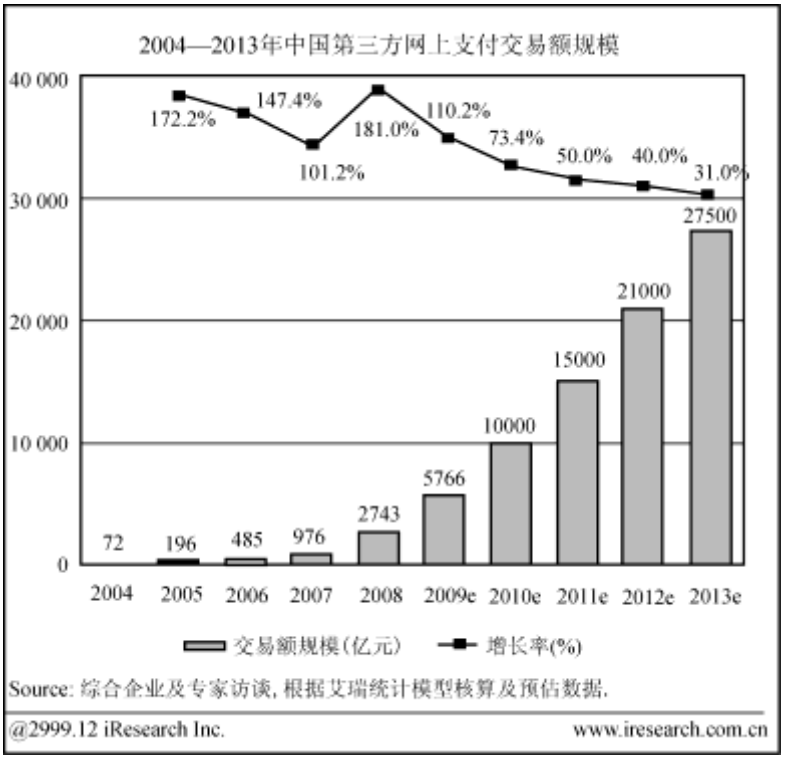

图 3-7　中国第三方网上支付交易额规模

3.2.1　网上支付概述

1．网上支付的概念

网上支付是指客户、商家和网络银行（或第三方支付）之间使用安全电子手段，利用电子现金、银行卡或电子支票等支付工具通过互联网传送到银行或相应的处理机构，从而完成支付的整个过程。参与网上支付活动的主要参与者有买卖双方及银行或第三方支付商，例如支付宝、快钱及财付通等。

2．网上支付系统的构成

网上支付系统主要由 Internet、客户、商家、开户银行、支付网关、银行网络和认证中心等几个元素组成，如图 3-8 所示。

网上支付系统几个主要元素具体含义说明如下。

1）Internet。Internet 是进行电子商务活动的基础，是电子商务网上支付的载体。

2）客户、商家。客户是指与商家有着交易关系并存在未清偿的债权债务关系（一般是债务）的一方，商家则是拥有债权的商品交易的另一方。

3）开户行。网上支付系统涉及客户开户行和商家开户行，分别指客户和商家在其中拥有账户的银行。

4）支付网关。支付网关是 Internet 公用网和银行网络（金融专用网）之间的接口。

5）银行网络。银行网络作为一个金融专用网，是银行内部及银行间进行通信的网络，应具有较高的安全性。

6）认证中心。认证中心又称为数字证书授权（certificate authority，简称 CA）中心，它是法律承认的权威机构，用于对电子商务各参与方（客户、商家、支付网关及网上银行等）进行身份认证，发放数字证书，以保证电子商务交易和支付能安全、可靠地进行。

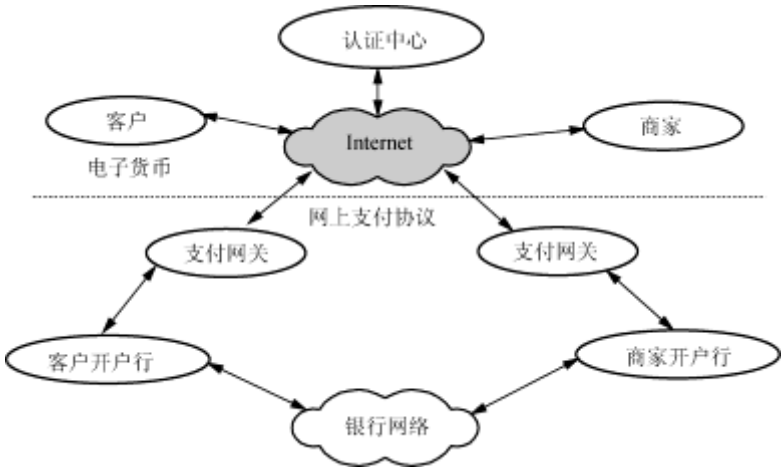

图 3-8　网上支付系统的构成

3．网上支付的种类

广义上，网上支付包括两种方式，一种是直接使用网上银行进行支付，另一种是通过第三方支付平台间接使用网上银行进行支付。狭义上，网上支付是指通过第三方支付平台实现的支付。

3.2.2　网上支付的流程

网上购物的过程与现实生活中的极其类似，网上购物流程示意图如图 3-9 所示。

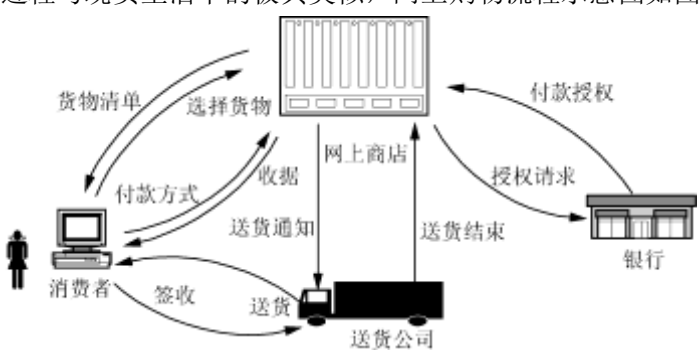

图 3-9　网上购物流程示意图

其具体网上购物流程如下。

1）消费者在电子商务网站的在线商店选定所购买的商品。

2）消费者向商家发出订货单，订货单上需包括购买商品的名称、数量、交货时间和地点等相关信息。

3）通过电子商务服务器与相关在线商店联系，在线商店作出应答，告诉消费者所填订货单的货物单价、应付款数及交货方式等信息是否准确，是否有变化。

4）消费者选择付款方式，确认订单签发付款指令。此时 SET（安全电子交易协议）开始介入。

5）在 SET 中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到消费者的账号信息。

6）在线商店接受订单后，向消费者所在银行请求支付认可。信息通过支付网关到收单银行，再到电子货币发行公司确认。批准交易后，返回确认信息给在线商店。

7）在线商店发送订单确认信息给消费者。消费者端可记录交易日志，以备将来查询。

8）在线商店发送货物或提供服务，并通知收单银行将钱从消费者的账号转移到商店账号。

3.2.3 网上支付工具

随着网络技术和电子商务的快速发展，网上支付工具也越来越多，这些工具可分为 3 大类，一类是电子现金类，如电子现金、电子钱包及电子零钱等；另一类是电子信用卡类，如智能卡、借记卡及电话卡等；还有一类是电子支票类，如电子汇票、电子划款等。这些方式都有其自身的特点和运作模式，适用于不同的交易过程，如表 3-1 所示。

表 3-1 网上支付工具及其相关的信息

支付类型特点	银行卡支付系统	电子现金	电子支票
事先/事后付款	事后付款	事先付款	事后付款
使用对象	银行卡持有人	任何人	在银行有账户者
交易风险	由发卡银行承担，当银行卡号被盗，可取消银行卡	由消费者自行承担电子现金丢失、被盗用或出错的风险	付款方可以止付有问题的付款指令或有问题的支票
交易凭据转换	直接由商户向银行查询持卡人账号	自由转换，不需要留下交易参与者的信息	电子支票或付款指令需要经过“背书”方能转让
在线检查	允许在线或离线检查	在线检查电子现金是否重复使用	以在线检查方式运作
目前普及程度	是在线付款中最普及的形式	电子现金的未来缺乏国际性的金融网络支持	目前缺乏国际性的标准，法律制度有待建立
交易额度	与银行卡额度相同	电子现金的额度通常固定的	和传统支票相同，即不大于支票账户的现有余额
是否支持小额支付	每笔交易成本相对较高，不适合进行小额支付	可进行不同面额的电子现金交易与找零，适合进行小额支付	有些系统允许商户累计付款指令到一定金额再进行支付，这些系统适合进行小额支付
与银行的关系	交易信息中的银行卡号为持卡人在发卡银行的账号	电子现金从银行提取后，就与银行账号没有关系	由银行账号进行付款

1．电子现金支付

电子现金又称为电子货币或数字现金，它把现金数值转换为一系列的加密序列数，通过这些序列数来表示现实中各种金额的币值。电子现金是一种非常重要的电子支付系统，可以被看做是对现实货币的电子或数字模拟以数字信息形式存在，通过互联网流通，但比现实货币更加方便、经济。电子现金支付流程如图 3-10 所示。

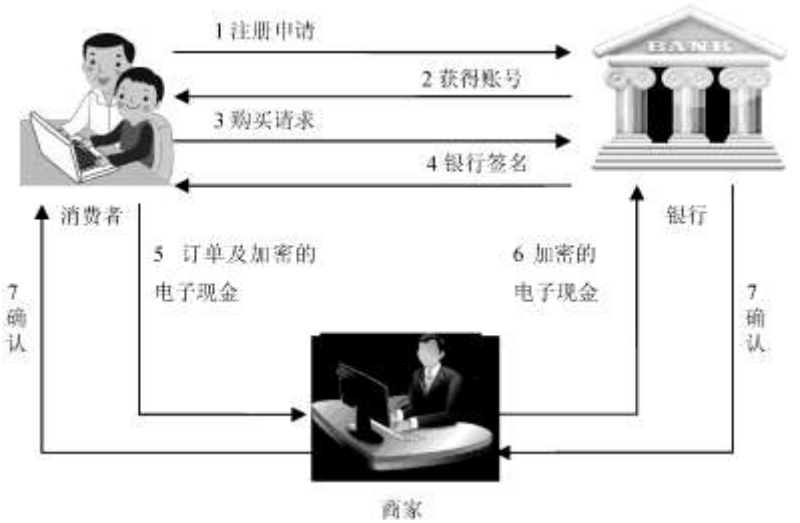

图 3-10　电子现金支付流程示意图

电子现金具体的支付过程可分为 4 个步骤。

1）消费者在有电子现金业务的银行开立电子现金账号，并预先存入现金，购买电子现金证书，这些电子现金就有了可以在商业领域进行流通的价值。

2）消费者使用电子现金终端软件从电子银行下载成包的电子现金到自己的计算机硬盘上备用。

3）消费者与同意使用电子现金的商家洽谈，签订货合同，使用电子现金支付所购商品的费用。

4）接收电子现金的商家与授权的电子现金银行进行结账，银行将消费者购买商品的钱支付给商家。

2．电子信用卡支付

电子信用卡是电子商务活动中常用的支付方式之一，电子信用卡通过网络直接支付。电子信用卡具有快捷、方便的特点，买方可以及时通过发卡机构了解持卡人的信用度，避免欺诈行为的发生。由于使用电子信用卡需要通过公共的 Internet 进行信用卡传输，因此在技术上需要保证传输的安全性和可靠性。利用 SET 协议保证电子信用卡卡号和密码的安全传输，在信用卡进行支付的过程中也需要认证客户、商家及信用卡发放机构的身份，防止抵赖行为的发生。如图 3-11 所示为 SET 信用卡支付流程。

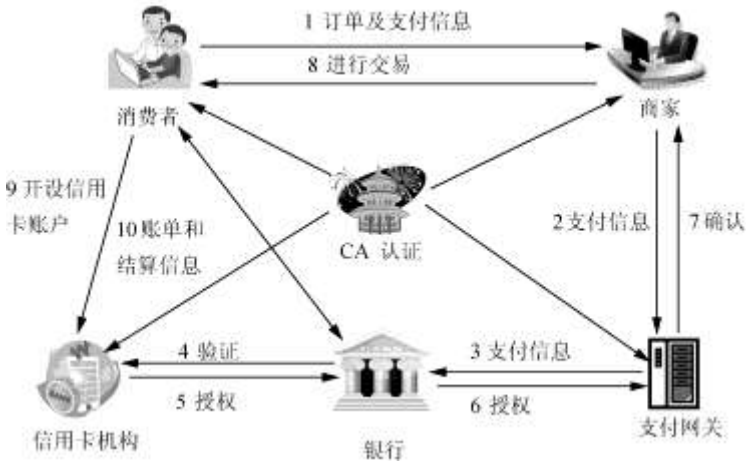

图 3-11　SET 信用卡支付流程示意图

3．电子支票支付

电子支票是一种借鉴纸张支票转移支付的优点，利用数字传递将钱款从一个账户转移到另一个账户的电子付款形式。这种电子支票的支付是在与商户及银行相连的网络上以密码方式传递的，多数使用公用关键字加密签名或个人身份证号码（PIN）代替手写签名。用电子支票支付，事务处理费用较低，而且银行也能为参与电子商务的商户提供标准化的资金信息，故而是最有效率的支付手段。电子支票支付流程如图 3-12 所示。

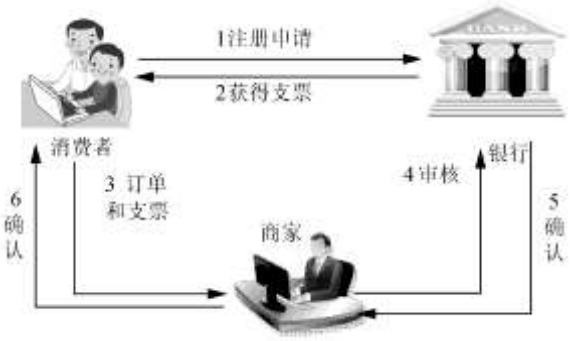

图 3-12　电子支票支付流程示意图

电子支票具体的支付过程可分为 4 个步骤。

1）消费者和商家达成购销协议并选择用电子支票支付。

2）消费者通过网络向商家发出电子支票，同时向银行发出付款通知单。

3）商家通过验证中心对消费者提供的电子支票进行验证，验证无误后将电子支票送交银行索付。

4）银行在商家索付时通过验证中心对消费者提供的电子支票进行验证，验证无误后即向商家兑付或转账。

4．电子钱包支付

电子钱包是电子商务活动中消费者使用的一种支付工具，是在小额购物或购买小商品时常用的新式“钱包”。用电子钱包购物需在电子钱包服务系统中进行，这就需要安装相应的系统。电子钱包软件通常都是免费提供的，可以直接使用与自己银行账户相连接的电子商务服务器上的电子钱包软件，也可以利用 Internet 上的电子钱包软件。

在电子钱包内只能存放电子货币，例如电子现金、电子零钱或电子信用卡等。电子钱包通常在银行里有账户。使用电子钱包时，用户先安装相应的应用软件，在该软件系统中设有电子货币和电子钱包的功能管理模块，称为电子钱包管理器；用户可以用它来改变口令或保密方式等，也可以用它来查看自己银行账号上电子货币收付往来的账目、清单和其他数据。该系统中还提供了一个电子交易记录器，顾客通过查询记录器可以了解自己的购物记录。

3.2.4　网上银行

1．什么是网上银行

网上银行也称为网络银行或在线银行，是指利用 Internet、Intranet 及相关技术处理传统的银行业务和支持电子商务网上支付的新型银行。网上银行通过 Internet 向客户提供开户、销户、查询、对帐、行内转账、跨行转账、信贷、网上证券及投资理财等传统服务项目，使客户可以足不出户就能够安全、便捷地管理活期或定期存款、支票、信用卡及个人投资等。可以说，网上银行就是在 Internet 上的虚拟银行柜台。

2．网上银行的主要特点

网上银行以计算机网络与通信技术为依托，突破传统银行时空的业务模式和便捷的企业与个人的金融支付。网上银行是近几年逐步成熟起来的新一代电子银行，它依托于传统银行业务，并为其带来根本性的变革，同时也拓展了传统的电子银行业务功能，扩大了经营范围，降低了经营成本。与传统银行和传统电子银行相比，网上银行在运行机制和服务功能方面都具有不同的特点。

（1）降低银行经营成本

网上银行主要利用公共网络资源，不需要设置物理的分支机构或营业网点，节省了巨额的场地租金、装修及水电等费用，只需要雇佣少量的工作人员，减少了人工成本，有效地提高了银行的营利能力。

（2）便利性

网上银行业务打破了传统银行业务地域和时间的限制，用户在家里或办公室就能登录银行主页完成开户、转账或存款等手续。这种方便快捷的方式既有利于吸引和保留优质的客户资源，又能主动扩大客户群开辟新的利润来源。

（3）个性化服务

传统银行通过营业网点销售保险、证券和基金等金融产品，其营销目标只能细分到某一类客户群，难以实现详细的、低成本的信息咨询服务。利用互联网和银行支付系统容易满足客户咨询、购买和交易多种金融产品的需求，客户除办理银行业务外，还可以很方便地进行网上买卖股票或债券等，网上银行能够为客户提供更加适合的个性化金融服务。

（4）业务范围更广

电子商务的发展、国民金融意识的增强和国家规范网上行为的法律法规的出台，将保障有更好的网上银行使用环境，这将促使网上银行的业务范围不断拓展，而且将有大量的非金融机构介入并有推出新的网上银行业务。

3．网上银行的支付流程

在电子商务网站上进行网上支付有两种方法：一种是通过第三方支付平台，如支付宝、财付通等，操作比较简单；另一种是与银行协商获得一个支付接口，从而实现网上银行的直接支付。

下面以中国工商银行为例介绍网上银行支付的基本流程。首先要进行网上注册，如图 3-13 所示为网上注册过程。

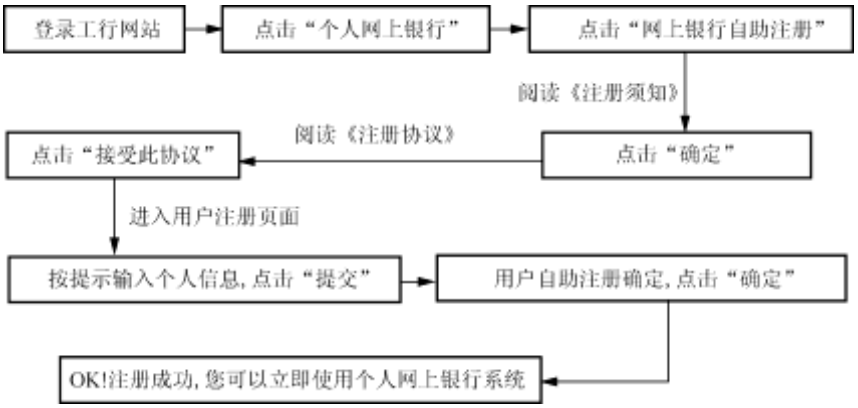

图 3-13　中国工商银行网上银行支付流程示意图

注册成功后，就可以网上购物，其具体过程如下。

1）消费者在电子商务网站浏览商品并下订单。

2）商家向中国工商银行提交订单。

3）消费者确认要使用中国工商银行支付后，将此订单提交给中国工商银行。

4）中国工商银行网银系统接收此订单，对商家和订单进行审核，审核通过后显示支付页面。

5）消费者输入支付卡卡号、支付密码和验证码等。

6）中国工商银行审核持卡人的信息，审核通过后显示确认页面；消费者确认后，中国工商银行进行支付指令处理；处理结束后，给消费者显示交易结果。

3.2.5　第三方支付平台

1．什么是第三方支付平台

第三方支付支付平台是指和国内及国外各大银行签约，并具备一定实力和信誉保障的第三方独立机构提供的交易支持平台。在通过第三方支付平台的交易中，买方选购商品后，使用第三方平台提供的账户进行货款支付，由第三方通知卖家货款到达、进行发货；买方检验物品后，就可以通知第三方付款给卖家，第三方再将款项转至卖家账户。

2．第三方支付平台的特点

第三方支付平台应该具有以下特点。

1）第三方网上支付平台可以支持国内各大银行发行的银行卡和国际信用卡组织发行的信用卡。第三方支付平台大大丰富了网上交易的支付手段，使网上交易渠道更加畅通。

2）第三方支付平台手续费标准统一且结算周期可根据商户需求设定，服务更加人性化。

3）相对于传统的资金划拨交易方式，专业的第三方网上支付平台可以确保商户在后期服务、支付过程中出现问题时能够得到及时解决。在整个交易过程中，都可以对交易双方进行约束和监督，为保证交易成功提供了必要的支持。

4）第三方支付作为中立的一方，具有公信度。一旦发生交易纠纷，第三方支付会对消费者和商家采取双向保护，在交易双方之间进行公平、公正的协调处理，确保双方的合法利益得到最大限度的维护。

5）方便、安全。第三方支付平台提供一系列应用接口程序，将多种银行卡支付方式整合到一个界面上对支付者而言，他所面对的是友好的界面，操作极其简单。交易时，用户将信用卡或银行账户信息仅告知第三方支付平台，大大降低了失密的风险。

3．第三方支付平台介绍

目前，国内的第三方支付平台主要有支付宝（阿里巴巴旗下）、财付通（腾讯公司，腾讯拍拍）、快钱（99bill）、百付宝（百度 C2C）、网易宝（网易旗下），以及首信易支付（首都电子商城网上支付平台）和安付通等。其中用户数量最大的是支付宝和财付通；中国银联旗下的银联电子支付也开始发展第三方支付，其实力也不容小视。据艾瑞报告显示，2009 年中国第三方网上支付平台市场交易额分布如图 3-14 所示。

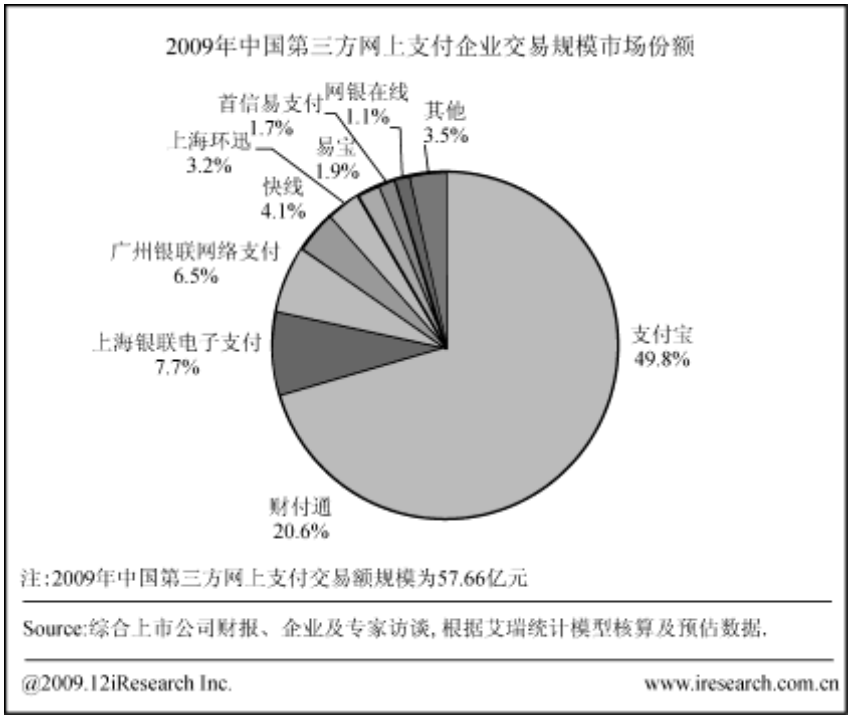

图 3-14　2009 年中国第三方网上支付平台市场交易额分布

（1）支付宝

支付宝是中国最大的第三方支付平台，是全球著名的电子商务公司阿里巴巴旗下的支付网站。其针对网上交易推出安全付款服务，以支付宝为信用中介，在买家确认收到商品前，由支付宝替买卖双方暂时保管货款，确保了买家和卖家双方的利益。

支付宝定位于电子商务支付领域，于 2003 年 10 月首次在淘宝出现。截止到 2008 年 8 月底，日交易额突破 4.5 亿元人民币，日交易突破 200 万笔，用户数首次达到 1 亿，从其出现到积累 1 亿用户共花去了近 5 年时间。但从 1 亿用户增长到 2 亿用户，支付宝仅仅花了 10 个月，而从 2 亿增长到 3 亿，只花了 9 个月。

目前，支付宝已与中国工商银行、中国农业银行、中国建设银行、中国邮政储蓄银行、交通银行、中国银行、招商银行及浦东发展银行等国内多家银行合作。

如图 3-15 所示为支付宝注册流程；如图 3-16 所示为支付宝安全交易流程。

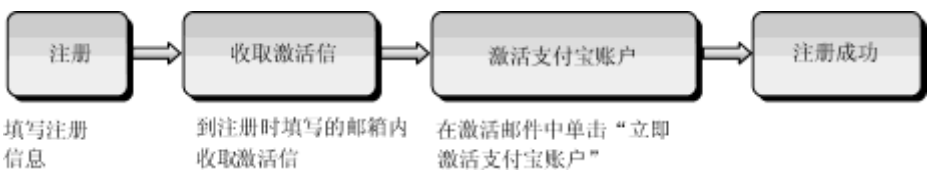

图 3-15　支付宝注册流程示意图

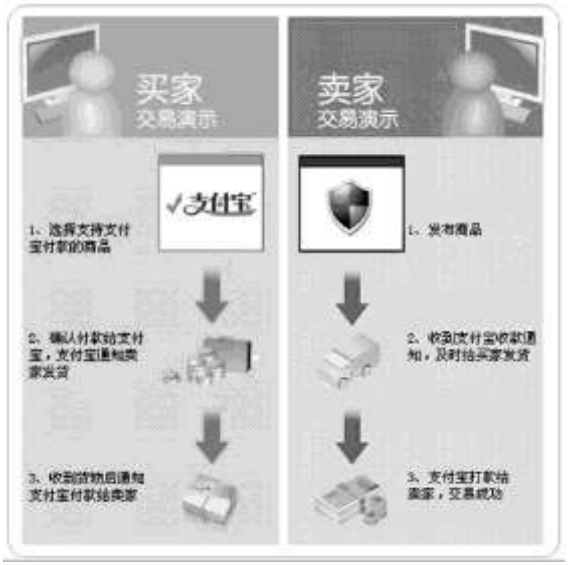

图 3-16　卖家和买家支付宝安全交易流程示意图

买家使用的好处：货款先由支付宝保管，收货满意后才付钱给卖家，安全放心；不必跑银行汇款，网上在线支付，方便简单；付款成功后，卖家立刻发货，快速高效，经济实惠。

卖家使用的好处：无须到银行查账，支付宝即时告知之买家付款情况，省力、省时；账目分明，交易管理帮卖家清晰地记录每一笔交易的详细信息，省心；支付宝认证是卖家信誉的有效体现。

（2）财付通

财付通是腾讯公司创办的中国领先的在线支付平台，致力于为互联网用户和企业提供安全、便捷、专业的在线支付服务。

个人用户注册财付通后，即可在拍拍网及 40 多万家购物网站轻松进行地购物。财付通支持全国各大银行的网银支付，用户也可以先充值到财付通，享受更加便捷的财付通余额支付体验。财付通的提现、收款及付款等配套账户功能让资金使用更灵活。财付通还为广大用户提供了手机充值、游戏充值、信用卡还款及机票专区等特色便民服务，让生活更方便。

针对企业用户，财付通构建全新的综合支付平台，业务覆盖 B2B、B2C 和 C2C 各领域，提供卓越的网上支付及清算服务。此外，还提供了极富特色的 QQ 营销资源支持，与广大商户共享 3 亿腾讯用户资源。

财付通购物流程如图 3-17 所示。

图 3-17　财付通购物流程示意图

3.3 电子商务安全

3.3.1 电子商务安全概述

随着电子商务在全球范围内的迅猛发展，电子商务中的网络安全问题日渐突出。根据中国互联网络信息中心（CNNIC）发布的“中国互联网络发展状况统计”报告，在电子商务方面，52.26%的用户最关心的是交易的安全可靠性。由此可见，解决电子商务中的网络安全和交易安全问题是实现电子商务的关键之所在。

网络安全就是如何保证网络上存储和传输的信息的安全性。但是，由于在互连网设计之初只考虑其方便性、开放性，因此互连网络难免非常脆弱，极易受到黑客的攻击或有组织群体的入侵，系统内部人员的不规范使用和恶意破坏也会使网络信息系统遭到破坏或信息泄露。

1．电子商务的安全问题

电子商务中存在的安全问题主要有以下 4 种类型。

1）冒充用户合法的身份。非法用户盗用合法用户的信息，冒充其身份与他人进行交易，损坏了被冒充的合法用户权益使得交易失去可靠性。

2）破坏网络传输数据的保密性。非法用户通过不正当手段利用数据在网络传输的过程，非法拦截数据并使用而导致合法用户的数据丢失。

3）损害网络传输数据的完整性。非法用户对截获的网络数据进行恶意篡改，例如添加、减少、删除及修改等。

4）恶意攻击网络硬件和软件，导致商务信息传递的丢失与破坏。例如，非法用户利用截获的网络数据包再次发送来攻击对方的计算机。

介于上述存在的威胁，应该在电子商务中实施安全保护措施。安全措施包括有下述几类：

1）保证交易双方身份的真实性：常用的处理技术是身份认证，依赖某个可信赖的机构（如 CA 认证中心）发放证书，并以此识别对方。目的是保证身份的精确性，分辨参与者身份的真伪，防止伪装攻击。

2）保证信息的保密性：保护信息不被泄露或被披露给未经授权的人或组织，常用的处理技术是数据加密和解密，其安全性依赖于使用的算法和密钥长度。常见的加密方法有对称式密钥加密技术（如 DES 算法）和公开密钥加密技术（如 RSA 算法）。

3）保证信息的完整性：常用数据杂凑等技术来实现。通过散列算法来保护数据不被未授权者（非法用户）建立、嵌入、删除、篡改或重放。典型的散列算法为美国国家安全局开发的单向散列算法。

4）保证信息的真实性：常用的处理手段是数字签名技术，目的是为了解决通信双方相互之间可能的欺诈（如发送用户对他所发送信息的否认、接收用户对他已收到信息的否认等），而不是对付未知的攻击者，其基础是公开密钥加密技术。目前，可用的数

字签名算法较多，例如 RSA 数字签名、ELGamal 数字签名等。

5）保证信息的不可否认性：通常要求引入认证中心（CA）进行管理，由 CA 发放密钥，传输的单证及其签名的备份发至 CA 保存作为可能争议的仲裁依据。

6）保证存储信息的安全性：规范内部管理，使用访问控制权限和日志，以及敏感信息的加密存储等。当使用 WWW 服务器支持电子商务活动时，应注意数据的备份和恢复，并采用防火墙技术保护内部网络的安全性。

2．电子商务的安全威胁

电子商务中的安全威胁可分为如下几类。

1）信息的截获和窃取。如果没有采用加密措施或加密强度不够，攻击者可能通过互联网、公共电话网、搭线、电磁波辐射范围内安装截收装置或在数据包通过的网关和路由器上截获数据等方式获取传输的机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析推出有用信息，例如消费者的银行账号、密码及企业的商业机密等。

2）信息的篡改。当攻击者熟悉了网络信息格式以后，通过各种技术方法和手段对网络传输的信息进行中途修改并发往目的地，从而破坏信息的完整性。这种破坏手段主要有 3 个方面：篡改——改变信息流的次序，更改信息的内容，如购买商品的出货地址；删除——删除某个消息或消息的某些部分；插入——在消息中插入一些信息，让接收方读不懂或接收错误的信息。

3）信息假冒。当攻击者掌握了网络信息数据规律或解密了商务信息以后，可以假冒合法用户或发送假冒信息来欺骗其他用户，主要有以下两种方式。

① 伪造电子邮件，虚开网站和商店，给用户发电子邮件，收订货单；伪造大量用户，发电子邮件，穷尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应；伪造用户，发大量的电子邮件，窃取商家的商品信息和用户信用等信息。

② 假冒他人身份，例如冒充领导发布命令、调阅密件；冒充他人消费、栽赃；冒充主机欺骗合法主机及合法用户；冒充网络控制程序，套取或修改使用权限、通行字或密钥等信息；接管合法用户欺骗系统，占用合法用户的资源。

4）交易抵赖。交易抵赖包括多个方面，例如发信者事后否认曾经发送过某条信息或内容；收信者事后否认曾经收到过某条消息或内容；购买者做了订货单不承认；商家卖出的商品因价格差而不承认原有的交易。

适当设置防护措施可以降低或防止来自现实的威胁。在通信安全、计算机安全、物理安全、人事安全、管理安全和媒体安全方面均可采取一定的措施，整个系统的安全取决于系统中最薄弱环节的安全水平，这就需要从系统设计上进行全面的考虑，折中选取。

如何应对安全威胁？电子商务安全是信息安全的上层应用，它包括的技术范围比较广，主要分为网络安全技术和密码技术两大类。其中，密码技术可分为加密、数字签名和认证技术等。

网络安全是电子商务安全的基础，一个完整的电子商务系统应建立在安全的网络基

础设施上。网络安全所涉及的方面有操作系统安全、防火墙技术、虚拟专用网 VPN 技术、各种反黑客技术和漏洞检测技术等，其中最重要的就是防火墙技术。

防火墙是建立在通信技术和信息安全技术上，用于在网络之间建立一个安全屏障，根据指定的策略对网络数据进行过滤、分析和审计，并对各种攻击提供有效的防范。主要用于 Internet 接入和专用网与公用网之间的安全连接。

VPN 也是一项保证网络安全的技术之一，是指在公共网络中建立一个专用网络，数据通过建立好的虚拟安全通道在公共网络中传播。企业只需要租用本地的数据专线连接本地的公众信息网，其各地的分支机构互相之间就可以安全传递信息；同时，企业还可以利用公众信息网的拨号接入设备，让自己的用户拨号到公众信息网上连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处。

3.3.2 电子商务安全技术

1．数据加密技术

加密技术是保证电子商务安全的重要手段，许多密码算法现已成为网络安全和商务信息安全的基础。密码算法利用密钥来对敏感信息进行加密，然后把加密好的数据和密钥（要通过安全方式）发送给接收者，接收者可利用同样的算法和传递来的密钥对数据进行解密获取敏感信息并保证了网络数据的机密性。利用另外一种称为数字签名的密码技术，可同时保证网络数据的完整性和真实性。利用密码技术可以达到对电子商务安全的需求，保证商务交易的机密性、完整性、真实性和不可否认性等。

加密技术包括对称加密和公钥加密，下面对两者分别进行详细介绍。

（1）对称加密技术

对称密钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据，私钥加密算法包括 DES 和 IDEA 等。对称加密技术的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。对称加密技术要求通信双方事先交换密钥，当系统用户多时，例如，在网上购物的环境中，商户需要与成千上万的购物者进行交易，若采用简单的对称密钥加密技术，商户需要管理成千上万的密钥与不同的对象通信，除了存储开销以外，密钥管理是一个几乎不可能解决的问题。另外，双方如何交换密钥？无论是通过传统手段还是通过 Internet，都会遇到密钥传送的安全性问题。网络环境中，密钥通常会经常更换，更为极端的是，每次传送都使用不同的密钥，对称加密技术的密钥管理和发布都是远远无法满足使用要求的。

对称加密技术中加密和解密均采用同一把密钥，而且通信双方必须都要获得这把钥匙并保持钥匙的秘密。这时的密钥称为对称密钥，并且不对外发布，也称为私钥密码。最典型的对称密钥加密算法是美国数据加密标准（data encrypt standard，简称 DES），如图 3-18 所示。

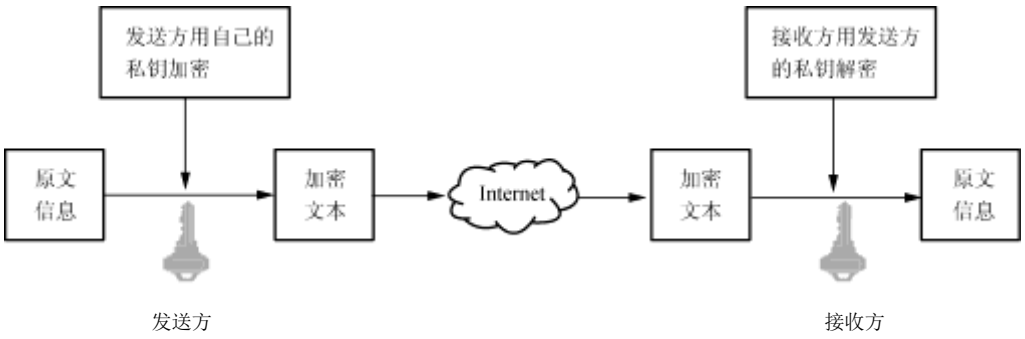

图 3-18　对称加密技术

例如：

明文 a，b，c，d，…，w，x，y，z

密文 D，E，F，G，…，Z，A，B，C（即相差 3 个字符）

若明文为 student，则对应的密文为 VWXGHQW（此时密钥为 3）。由于英文字母中各字母出现的频率早已有人进行过统计，所以根据字母频率表可以很容易对这种代替密码进行破译。

（2）公钥密钥加密技术

公钥密钥加密，又称不对称密钥加密系统，它需要使用一对密钥来分别完成加密和解密操作。其中一个公开发布，称为公开密钥（Public-Key）；另一个由用户自己秘密保存，称为私有密钥（Private-Key）。信息发送者用公开密钥去加密，而信息接收者则用私有密钥去解密。通过数学的手段保证加密过程是一个不可逆过程，即用公钥加密的信息只能是用与该公钥配对的私有密钥才能解密。常用的算法是 RSA、ElGamal 等。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。

为了充分利用公钥密码和对称密码算法的优点克服其缺点，解决每次传送更换密钥的问题，提出混合密码系统，即所谓的电子信封（envelope）技术。发送者自动生成对称密钥，用对称密钥加密发送的信息，将生成的密文连同用接收方的公钥加密后的对称密钥一起传送出去。收信者用其秘密密钥解密被加密的密钥来得到对称密钥，并用它来解密密文。这样保证每次传送都可由发送方选定不同密钥进行，更好地保证了数据通信的安全性。

使用混合密码系统可同时提供机密性保障和存取控制。利用对称加密算法加密大量输入数据可提供机密性保障，然后利用公钥加密对称密钥。如果想使多个接收者都能使用该信息，可以对每一个接收者利用其公钥加密一份对称密钥即可，从而提供存取控制功能。

2．数字签名技术

数字签名技术即进行身份认证的技术。在数字化文档上的数字签名类似于纸张上的手写签名，是不可伪造的。接收者能够验证文档确实来自签名者，并且签名后文档没有

被修改过，从而保证信息的真实性和完整性。在指挥自动化系统中，数字签名技术可安全地用于传送作战指挥命令和文件。

完善的签名应满足以下 3 个条件。

1）签名者事后不能抵赖自己的签名。

2）任何其他人不能伪造签名。

3）如果当事人双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。

数字签名是通过一个单向函数对要传送的报文进行处理后，得到的用以认证报文来源并核实报文是否发生变化的一个字母数字串。

在传统的商业系统中，通常都利用书面文件的亲笔签名或印章来规定契约的责任，在电子商务中，传送的文件是通过电子签名证明当事人身份与数据真实性的。数据加密是保护数据的最基本方法，但也只能防止第三者获得真实数据。电子签名则可以解决否认、伪造、篡改及冒充等问题，其具体要求是发送者事后不能否认发送的报文签名、接收者能够核实发送者发送的报文签名、接收者不能伪造发送者的报文签名、接收者不能对发送者的报文进行部分篡改及网络中的某一用户不能冒充另一用户作为发送者或接收者。

数字签名的算法很多，其中 HASH 签名是应用较为广泛的一种。数字签名中常用的就是散列（HASH）函数，也称消息摘要（message digest）、哈希函数或杂凑函数等，其输入为一个可变长度串，返回一个固定长度串，该串被称为输入的散列值（消息摘要）。日常生活中，通常通过对某一文档进行签名来保证文档的真实有效性，可以对签字方进行约束，防止其抵赖行为，并把文档与签名同时发送以作为日后查证的依据。在网络环境中，可以用电子数字签名作为模拟，从而为电子商务提供不可否认服务。

把 HASH 函数和公钥算法结合起来，可以在提供数据完整性的同时保证数据的真实性。完整性保证传输的数据没有被修改，而真实性则保证是由确定的合法者产生的 HASH，而不是由其他人假冒。把这两种机制结合起来就可以产生所谓的数字签名（digital signature）。

将报文按双方约定的 HASH 算法计算得到一个固定位数的报文摘要值。在数学上，保证只要改动报文的任何一位，重新计算出的报文摘要就会与原先值不符。这样就保证了报文的不可更改性。然后把该报文的摘要值用发送者的私人密钥加密，将该密文同原报文一起发送给接收者所产生的报文即称数字签名。

接收方收到数字签名后，用同样的 HASH 算法对报文计算摘要值，然后与用发送者的公开密钥进行解密解开的报文摘要值相比较，如相等，则说明报文确实来自发送者，因为只有用发送者的签名私钥加密的信息才能用发送者的公钥解开，从而保证了数据的真实性。

在安全性方面，数字签名相对于手写签名具有的好处：数字签名不仅与签名者的私有密钥有关，而且与报文的内容有关，因此不能将签名者对一份报文的签名复制到另一份报文上，同时也能防止篡改报文的内容。

3．数字证书

对数字签名和公开密钥加密技术来说，都会面临公开密钥的分发问题，即如何把一个用户的公钥以一种安全可靠的方式发送给需要的另一方。解决这个问题的关键在于，要求管理这些公钥的系统必须是值得信赖的。在这样的系统中，如果 Alice 想要给 Bob 发送一些加密数据，Alice 需要知道 Bob 的公开密钥；如果 Bob 想要检验 Alice 发来的文档的数字签名，Bob 需要知道 Alice 的公开密钥。因此，必须有一项技术来解决公钥与合法拥有者身份的绑定问题。假设有一个人自称某一个公钥是自己的，必须有一定的措施和技术来对其进行验证。

数字证书是解决这一问题的有效方法。它通常是一个签名文档，标记特定对象的公开密钥。电子证书由一个认证中心（CA）签发，认证中心类似于现实生活中公证人的角色，它具有权威性，是一个普遍可信的第三方。当通信双方都信任同一个 CA 时，两者就可以得到对方的公开密钥并能进行秘密通信、签名和检验。

证书机构 CA（certification authority）是一个可信的第三方实体，其主要职责是保证用户的真实性。本质上，CA 的作用同政府机关的护照颁发机构类似，用于证实公民是否是其所宣称的那样（正确身份），而信任这个国家护照颁发机构的其他国家则信任该公民，认为其护照是可信的，这也是第三方信任一个很好的实例。

同护照类似，网络用户的电子身份（electronic identity）是由 CA 来发布的，也就是说他是被 CA 所信任的，该电子身份就称为数字证书。因此，所有信任 CA 的其他用户同样也信任该用户。护照颁发机构和证书机构 CA 都是由策略和物理元素构成的。在护照颁发机构，有一套由政府确定的政策来判定哪些人可信任为公民，以及护照的颁发过程。

实行网上安全支付是顺利开展电子商务的前提，建立安全的认证体系（CA）则是电子商务的中心环节，建立 CA 的目的是加强电子证书和密钥的管理工作，增强网络交易各方的相互信任，提高网上购物和网上交易的安全，控制交易的风险，从而推动电子商务的发展。

为了推动电子商务的发展，首先要确定网上参与交易的各方（例如持卡消费户、商户、收单银行的支付网关等）的身份，相应的电子证书（digital certificate，简称 DC）就代表他们的身份，由权威的、公正的认证机构管理。各级认证机构按照根认证机构（Root CA），品牌认证机构（Brand CA），以及持卡人（holder card）、商户（merchant）或收单银行（acquirer）的支付网关认证机构（payment gateway CA）由上而下按层次结构建立。

电子商务安全认证机构 CA 的基本功能如下。

1）生成和保管符合安全认证协议要求的公私密钥、数字证书及其数字签名。

2）对电子证书和数字签名进行验证。

3）对电子证书进行管理，重点是证书的撤销管理，同时追求实施自动管理（非手工管理）。

4）建立应用接口，特别是支付接口。CA 是否具有支付接口是能否支持电子商务的

关键。

4．安全交易协议

在电子商务过程中，买卖双方是通过网络来联系的，因而建立交易双方的安全和信任关系是相当困难的，这使得电子商务交易双方都面临不同的安全威胁。而电子商务的主要特征是在线支付，为了加强电子商务交易的安全性，需要采用数据加密和身份认证技术，以便于营造一种可信赖的电子交易环境。目前有两种安全支付协议被采用，即安全套接层 SSL 协议和安全电子交易 SET 协议。

（1）安全套接层协议

安全套接层（secure sockets layer，简称 SSL）协议是 Netscape 公司于 1995 年推出的一种安全通信协议。SSL 提供了两台计算机之间的安全连接，对计算机的整个会话进行了加密，从而保证了信息传输的安全，实现浏览器与 Web 服务器之间的安全通信，在 Internet 上广泛应用于处理与金融有关的敏感信息。

SSL 协议是一种保护 Web 通信的工业标准，能够对信用卡和个人信息及电子商务提供较强的加密保护。SSL 连接是保密的，对于每个连接都有一个唯一的会话密钥，采用对称密码体制（如 DES、RC4 等）来加密数据；SSL 连接是可靠的，消息的传输采用 MAC 算法（如 MD5、SHA 等）进行完整性检验；SSL 对端实体的鉴别采用非对称密码体制（如 RSA、DSS 等）进行认证。

SSL 协议提供的服务是数据和服务器的合法认证，使得用户和服务器能够确信数据将被发送到正确的客户机和服务器上。客户机和服务器都有各自的识别号，由公开密钥编排。SSL 协议要求在握手交换数据中做数字认证，以此来确保用户的合法性，加密数据以便隐藏被传送的数据。SSL 协议采用的加密技术既有对称密钥，也有公开密钥。具体来说，就是客户机与服务器交换数据前，先交换 SSL 初始握手信息。在 SSL 握手信息中采用了各种加密技术，以保证数据的机密性，防止非法用户破译，维护数据的完整性。SSL 协议采用 HASH 函数和机密共享的方法，提供完整性信息的服务来建立客户机与服务器之间的安全通道，使经过处理的业务在传输过程中能够完整、准确地到达目的地。

（2）安全电子交易协议

安全电子交易（secure electronic transaction，简称 SET）协议是 1996 年由 Visa（维萨）与 MasterCard（万事达）两大国际信用卡公司联合制订的安全电子交易规范。它提供了消费者、商家和银行之间的认证，确保网上交易的保密性、数据的完整性、交易的不可否认性和交易的身份认证，保证在开放网络环境下使用信用卡进行在线购物的安全。

SET 协议中采用数据加密过程的特点：交易参与者的身份鉴别采用数字证书的方式来完成，数字证书的格式一般采用 X.509 国际标准；交易的不可否认性用数字签名的方

式来实现，由于数字签名是由发送方的私钥产生，而发送方的私钥只有他本人知道，所以发送方不能对其发送过的交易数据进行抵赖；由于非对称加密算法的运算速度慢，所以要和对称加密算法联合使用，用对称加密算法来加密数据，用数字信封来交换对称密钥。

SET 协议的数据交换过程，如图 3-19 所示。

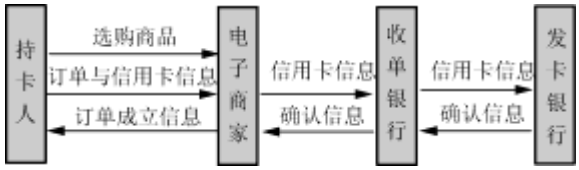

图 3-19　SET 协议的数据交换过程示意图

SET 协议的购物系统由持卡人、商家、支付网关、收单行和发卡行 5 个部分组成，这 5 个部分之间的数据交换过程如下。

1）持卡人决定购买，向商家发出购买请求。

2）商家返回商家证书等信息。

3）持卡人验证商家身份，将定购信息和支付信息安全地传送给商家，但支付信息对商家来说是不可见的（用银行公钥加密）。

4）商家验证支付网关身份，把支付信息传给支付网关，要求验证持卡人的支付信息是否有效。

5）支付网关验证商家身份，通过传统的银行网络到发卡银行验证持卡人的支付信息是否有效，并把结果返回给商家。

6）商家将信息返回给持卡人，按照订单信息送货。

7）商家定期向支付网关发送要求支付的信息，支付网关通知发卡行划账，并把结果返回给商家，交易结束。

SET 的运作流程如图 3-20 所示。

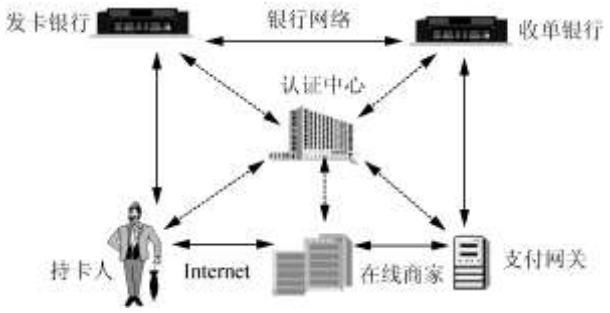

图 3-20　SET 的运作流程

SET 动作的具体流程如下。

1）客户进入网络商家订购商品，并填写订购数量和送货日期等信息。

2）客户准备结账，这时计算机中具有 SET 规格的“电子钱包”软件自动启动，并将信用卡信息连同订单信息分别加密后传送给商家。

3）商家收到该订单及信用卡信息后，将信用卡信息原封不动地传给收单银行以检查信用卡是否有效。

4）收单银行向发卡银行确认该信用卡数据无误后，发出信息通知商家可以接下此笔订单。

5）到了结账日，客户会接到发卡银行的信用账单，而商家则可以拿信用卡授权码向收单银行划款。

SSL 协议和 SET 协议的差别主要表现在以下几个方面。

1）SSL 协议已被浏览器和 Web 服务器内置，无须安装专门软件；而 SET 协议中客户端须安装专门的电子钱包软件，在商家服务器和银行网络上也需安装相应的软件。

2）安全性是网上交易中最关键的问题。SET 协议由于采用了公钥加密、信息摘要和数字签名技术可以确保信息的保密性、可鉴别性、完整性和不可否认性，且 SET 协议采用了双重签名来保证参与交易活动的各方信息相互隔离，使商家只能看到持卡人的订购数据，而银行只能取得持卡人的信用卡信息。SSL 协议虽也采用了公钥加密、信息摘要和 MAC 检测，可以提供保密性、完整性和一定程度的身份鉴别功能，但缺乏一套完整的认证体系，不能提供完备的防抵赖功能。因此，SET 的安全性远比 SSL 的高。

3.4 文件传输协议 FTP

3.4.1 FTP 概述

FTP 是 file transfer protocol（文件传输协议）的英文简称，而中文简称为“文传协议”，是用于 Internet 上控制文件双向传输的。同时，它也是一个应用程序（application）。用户可以通过它把自己的 PC 与世界各地所有运行 FTP 的服务器相连，并可以访问服务器上的大量程序和信息。FTP 的主要作用就是让用户连接一个远程计算机（这些计算机上运行着 FTP 服务器程序），查看远程计算机有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件传送到远程计算机去。

在 FTP 的使用过程中，用户经常遇到两个概念：“下载”（download）和“上传”（upload）。其中，“下载”文件就是从远程主机复制文件至自己的计算机上；“上传”文件就是将文件从自己的计算机中复制至远程主机上。用 Internet 语言来说，用户可通过客户机程序向（从）远程主机上传（下载）文件。

使用 FTP 时必须先登录，在远程主机上获得相应的权限以后才可下载或上传文件。也就是说，要想同哪一台计算机互传文件，就必须具有哪一台计算机的适当授权。换言之，除非有用户 ID 和口令，否则无法传送文件。这种情况违背了 Internet 的开放性，Internet 上的 FTP 主机何止千万，不可能要求每个用户在每一台主机上都拥有账号。匿名 FTP

就是为解决这个问题而产生的。

匿名 FTP 是这样一种机制，用户可通过它连接到远程主机上并从其上面下载文件，而无须成为其注册用户。系统管理员建立了一个特殊的用户 ID，名为 anonymous，这样 Internet 上的任何人在任何地方都可使用该用户 ID。

通过 FTP 程序连接匿名 FTP 主机的方式同连接普通 FTP 主机的方式差不多，只是在要求提供用户标识 ID 时必须输入 anonymous，该用户 ID 的口令可以是任意的字符串。习惯上，用自己的 E-mail 地址作为口令，使系统维护程序能够记录下来谁在存取这些文件。

CuteFTP 是一款商业级 FTP 客户端程序，其加强的文件传输系统能够完全满足各种用户的应用需求。文件通过构建于 SSL 或 SSH 2 安全认证的客户机/服务器系统进行传输，同时也为 VPN、WAN、Extranet 开发管理人员提供了最经济的解决方案，使企业不再需要为了一套安全的数据传输系统而破费。此外，专业版的 CuteFTP 8.2 还提供了 Sophisticated Scripting（经典脚本）、目录同步、自动排程、同时多站点连接、多协议支持（FTP、SFTP、HTTP、HTTPS）、智能覆盖及整合的 HTML 编辑器等功能，是一款出色并且更加快速的文件传输系统。

3.4.2　实训：FTP 的应用

下载 CuteFTP Pro 8.3，软件下载后为一个.rar 格式的压缩文件。其安装比较简单，只需要依次单击【下一步】按钮，CuteFTP Pro 8.3 安装起始画面（对某些功能和工具可以进行安装选择）如图 3-21 所示，CuteFTP Pro 8.3 含有简体中文语言包，通过执行【工具】|【全局选项】命令可以进行语言设置。

（a）起始界面　　（b）选择组件

图 3-21　安装向导

试用版期限为 30 天，主界面默认显示了本地驱动器（目录）、站点管理器、队列及日志 4 大窗口，如图 3-22 所示。

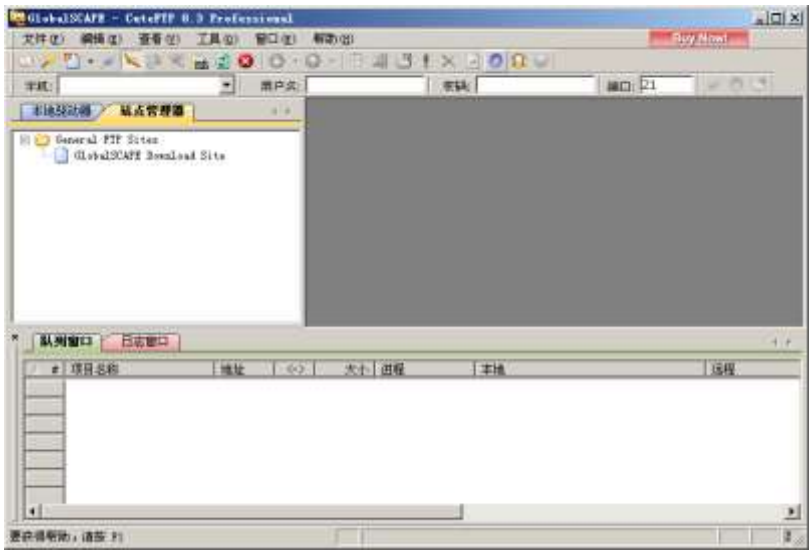

图 3-22　CuteFTP 主界面

1．站点设置

要使用 FTP 工具来上传（下载）文件，首先必须要设定好 FTP 服务器的网址（IP 地址）、授权访问的用户名及密码。

通过执行【文件】|【新建】|【FTP 站点】命令或者 Ctrl+N 键，用户可以对远程的 FTP 服务器进行具体的设置。

1）按照如图 3-23 所示的界面，在常规选项卡中输入标签内容，然后再分别输入主机地址（即 FTP 服务器所拥有的 IP 地址）、用户名和密码。

2）在【类型】选项卡有一项端口号（21），对于端口号，在没有特别要求的情况下就使用默认值，不必再进行任何改变。

3）在【动作】选项卡设置远程及本地文件夹（目录），远程文件夹其实就是连上 FTP 服务器后默认打开的目录；而本地文件夹就是每次进入 FTP 软件后默认显示的本地文件目录。

图 3-23　CuteFTP 站点设置界面

2．连接上传

通过上面的设置后，就可以连接到 FTP 服务器上传文件了。用户可以通过在站点管理器窗口中双击要连接的 FTP 服务器，也可以选择要连接的 FTP 服务器单击工具栏的【连接】图标。连接后，便可选择目录或文件进行上传或下载了。

用户不仅可以传输单个文件，而且还可以传输多个文件甚至整个目录，CuteFTP 主

要提供了 5 种方法。

1）选中所要传输的文件或目录，直接拖动到目的主机中。

2）在选中所要传输的文件或目录后，单击鼠标右键选择【传输】命令。

3）双击想要传输的文件（但先要在参数选择中进行设置）。

4）选中所要传输的文件或目录后，单击工具栏上的【上传】按钮；

5）将选中的文件或文件夹拖放到队列窗口中，然后通过单击鼠标右键选择相应的菜单命令进行传输。使用传输队列最大的好处是可以随时加入或删除传输的文件，并且对于需要经常更新的内容，允许用户把它们放到队列中保存下来，每次传输文件时还可以通过执行【工具】|【队列】|【载入并保存队列】|【载入队列】命令调出以前保存的队列进行文件传输，如图 3-24 所示。要注意的是，不同的文件上传到不同目录时，必须先将该目录打开后再添加要上传的文件到队列中。

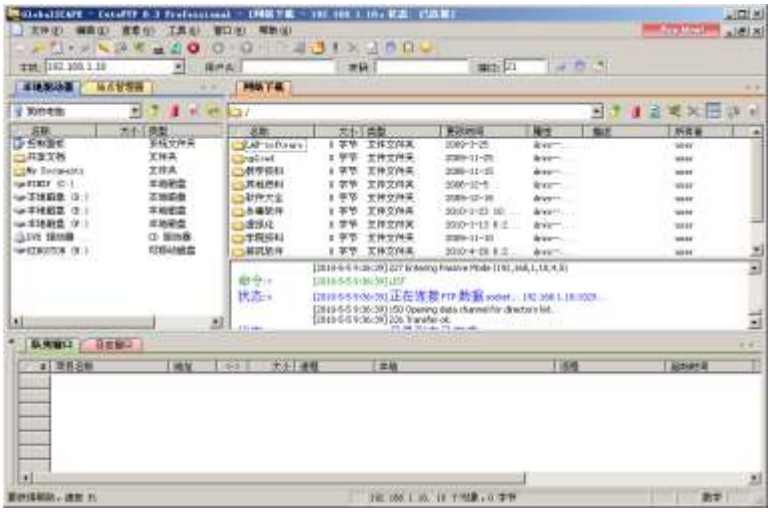

图 3-24　CuteFTP 连接后传输界面

3．其他功能及设置

（1）快速连接

快速连接就是不需通过站点设置，直接输入 IP 地址、用户名及密码进行连接，如图 3-25 所示。

图 3-25　CuteFTP 快速连接界面

它适合用在需要临时连接的站点，并且快速连接信息会被保存，如果下次还想使用，就可以直接选择进行连接，非常方便。通过快速连接工具栏输入相关信息，单击【连接】按钮即可。

（2）站点导入导出

站点导入就是将以前版本的站点信息或其他 FTP 软件的站点信息导入进来，而不需

要再进行重复的设置，这给广大用户节省了时间，也减少了麻烦。通过执行【工具】|【站点管理器】|【导入/导出 FTP 站点】命令，即可进行站点导入及导出，如图 3-26 和图 3-27 所示。

图 3-26 CuteFTP 站点导入

图 3-27 CuteFTP 站点导出（支持两种格式导出文本）

（3）密码保护

密码保护，顾名思义就是对站点管理器的数据信息进行加密，给数据安全提供保障，并且在以后的每次启动时都会出现密码提示窗口。但要注意的是，在设置密码后如果忘记密码，CuteFTP 将创建一个新的站点管理器，同时备份被锁定的站点管理器。通过执行【工具】|【站点管理器】|【安全】|【加密站点管理器数据】命令，即可设置密码，如图 3-28 所示。

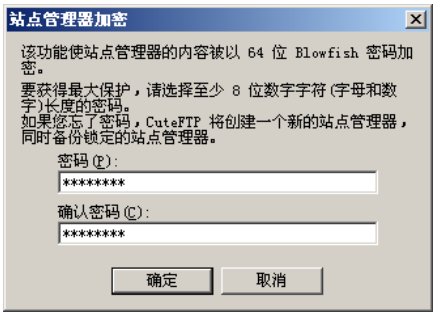

图 3-28 CuteFTP 密码设置界面

（4）队列管理

队列管理就是对所传输的文件及目录进行的一些功能设置，包括队列的保存、载入、清除、恢复和传输等，可以说是比较重要的功能。通过执行【工具】|【队列】命令，即可进行队列的相关操作，如图 3-29 所示。

（5）文件夹工具（比较及同步）

文件夹内容比较就是对两台不同计算机上相关目录下的内容进行比较，然后把不相同的内容使用不同的颜色分别显示出来，而文件夹内容同步就是让本地和远程的文件结构保持一致（共有 3 种方向），这对于保持版本一致性是非常有用的。通过执行【工具】|

【文件夹工具】命令，即可进行相关的操作，如图 3-30 所示。

图 3-29　CuteFTP 队列管理功能

图 3-30　CuteFTP 文件夹内容比较

（6）远程站点对传

远程站点对传就是在两台远程 FTP 服务器之间直接传送文件，省去了很多中间环节。通过执行菜单命令【文件】|【下载高级】|【站点对传到】命令，选择要对传的站点即可，如图 3-31 所示。但要注意的是，不是所有的 FTP 服务器都支持此功能，并且传输速度比较慢，不一定能够成功。

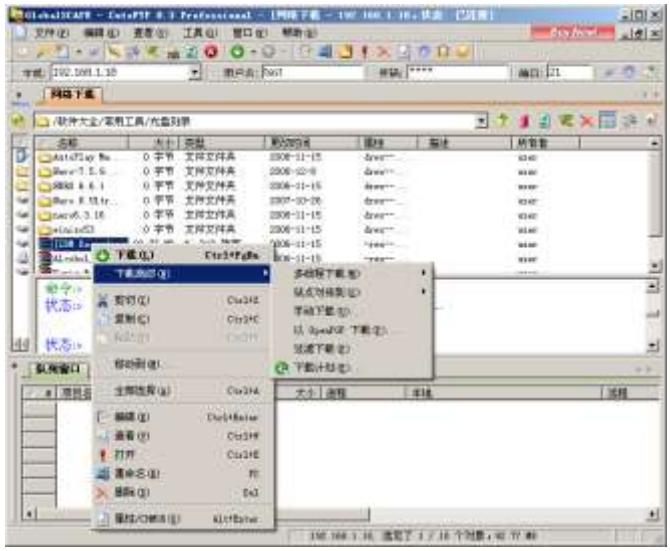

图 3-31　CuteFTP 远程站点对传

连接上目标站点后，基本上准备工作已经完成。下面要做的就是如何进行文件的上传和下载。

文件的上传和下载很简单。连接到服务器以后，CuteFTP 的窗口被分成左、右两个窗格。左边的窗格用于显示本地硬盘的文件列表，右边的窗格用于显示远程目标站点上的文件列表。文件列表的显示方式和 Windows 资源管理器的完全一样。

上传和下载都可以通过拖曳文件（或者文件夹）的图标来实现。例如，将左侧窗格中的文件拖动到右侧窗格中，就可以上传文件；将右侧窗格中的文件拖到左侧窗格中，就可以下载文件。

首先实现文件上传。选中本地的文件，单击鼠标右键，在弹出的快捷菜单中选择【上传命令】，如图 3-32 所示。

上传完毕以后，左边本地目录窗口和右边远程目录窗口中会有相同的文件出现，表明已经上传成功，如图 3-33 所示。

图 3-32　上传文件

图 3-33　上传成功

同时，CuteFTP 还提供高级上传功能，包括多线程上传、手动上传等，如图 3-34 所示。

下载文件。成功登录 FTP 服务器后，选中想要下载的文件，单击鼠标右键，在弹出的快捷菜单中选择【下载】命令（见图 3-35），同时在下载队列窗口中可以看到文件正在下载，如图 3-36 所示。

图 3-34　高级上传功能

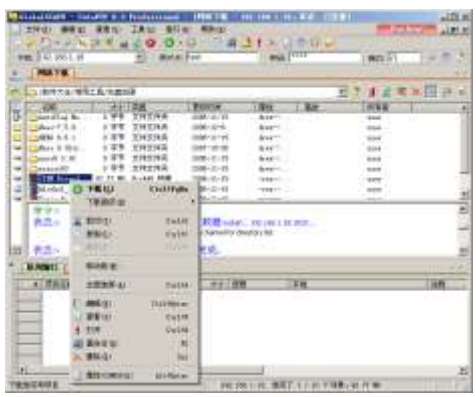

图 3-36　下载文件

图 3-36　文件正在下载

同时，CuteFTP 还提供高级下载功能，包括多线程下载、手动下载及过滤下载等，如图 3-37 所示。

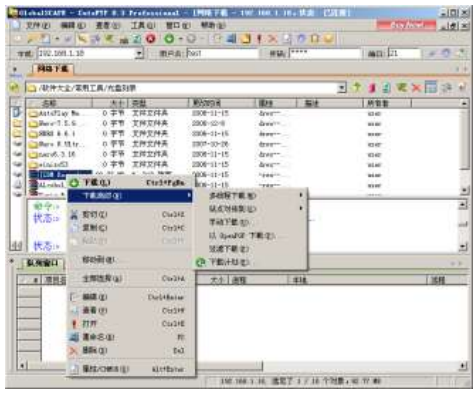

图 3-37　高级下载功能

教 学 小 结

通过本章的学习，能够了解网上交易及网上支付的基本概念和流程，掌握各种网上支付工具的使用方法，了解网上银行的特点及支付过程，目前国内主要的第三方支付平台的现状及交易流程，能够独立分析电子商务存在的安全问题，并能够理解数据加密、数字签名、数字证书等安全技术的原理及应用，掌握文件传输协议的原理及用途，能够使用 CuteFTP 软件轻松完成文件的上传和下载任务。

习　　题

一、单项选择题

1. 计算机的安全问题可以分为（　　）。
   A. 实体的安全性、运行环境的安全性和信息的可靠性
   B. 实体的安全性、运行环境的安全性和信息的安全性
   C. 实体的可靠性、运行环境的安全性和信息的安全性
   D. 实体的安全性、运行环境的可靠性和信息的安全性

2．计算机安全通常表现在（　　）方面。

A．计算机系统的安全保护和对计算机身份的确定

B．计算机系统的数字证书和对计算机犯罪的防范打击

C．计算机系统的安全保护和对计算机犯罪的防范打击

D．计算机系统的密码保护和对计算机犯罪的防范打击

3．利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家机密、经济情报或商业秘密等是属于（　　）。

A．直接以计算机信息系统为犯罪对象的犯罪

B．直接以计算机信息系统进行经济犯罪

C．以计算机为犯罪工具实施金融诈骗

D．以计算机为犯罪工具实施其他犯罪

4.（　　）是对用户的身份进行鉴别和识别，对用户利用资源的权限和范围进行核查，是数据保护的前沿屏障。

A．多媒体数据存取　　B．存取控制

C．身份认证　　D．数据库存取控制

5．使用密钥将密文数据还原成明文数据，称为（　　）。

A．解码　　B．编译　　C．加密　　D．解密

6．数据库存取控制对数据库信息按存取属性划分的授权分为允许或禁止运行，允许或禁止阅读，允许或禁止写入，允许或禁止修改，以及（　　）。

A．允许或禁止拆分　　B．允许或禁止清除

C．允许或禁止合并　　D．允许或禁止添加

7. 实体安全技术的环境保护要求对计算机房采取防火、防水、防尘、防震和（　　）。

A．防盗窃　　B．防鼠害　　C．防静电　　D．防病毒

8．使用密钥将明文数据变换成密文数据，称为（　　）。

A．数据加密　　B．数据解密　　C．调制　　D．解调

9．防火墙的组成部分包括服务访问政策、包过滤、应用网关和（　　）。

A．验证工具　　B．硬件狗　　C．隔离工具　　D．软件识别

10．身份认证的目的是确定系统或网络的访问者是否为（　　）。

A．网站会员　　B．合法用户　　C．合法顾客　　D．后还管理

11．下列（　　）不是计算机犯罪区别于传统的盗窃、抢劫等犯罪的特征。

A．不易侦查　　B．不易觉察　　C．隐蔽性　　D．公开性

12．考虑公用网上支付信息的流动规则及其安全保护，是（　　）的责任。

A．支付工具　　B．支付方式　　C．支付协议　　D．支付手段

13．电子现金是一种以（　　）形式流通的货币。

A．数据　　B．十进制　　C．实物　　D．资金

14．电子资金的划拨依据是虚拟银行与（　　）之间所订立的协议

A．认证中心　　B．网络交易客户 C．网络交易中心 D．商家

15．在电子商务条件下，下列选项中（　　）不属于买方应当承担的义务。

A．按照网络交易规定方式支付价款

B．按照合同规定的时间、地点运输标的物

C．对标的物的质量承担担保责任

D．对标的物验收

16．买方不履行合同义务，包括买方不安合同规定支付货款和不按规定收取货物。在这种情况下，卖方可选择相应救济方法，以下方法无效的是（　　）。

A．要求买方支付价款、收取货物或履行其他义务，并为此可以规定一段合理额外的延长期限，以便买方履行义务

B．解除合同　　C．减少支付价款

D．损害赔偿，要求买方支付合同价格与转售价之间的差额

17．CA 的中文含义是（　　）。

A．电子中心　　B．认证中心　　C．银行中心　　D．信息中心

18．CA 数字证书中不包含的信息有（　　）。

A．CA 的数字签名　　B．证书申请者的个人信息

C．证书申请者的私钥　　D．证书申请者的公钥信息

19．数字签名可以解决（　　）。

A．数据被泄露　　B．数据被篡改

C．未经授权擅自访问　　D．冒名发送数据或发送后抵赖

20．实现在线交易，最重要的是解决交易中的（　　）问题。

A．信誉　　B．安全　　C．法律　　D．同步

21．（　　）用来确认电子商务活动中各自的身份，实现网上安全的信息交换与安全交易。

A．CA 中心　　B．网上银行　　C．网上工商局　　D．网上公安局

二、是非题

1．网上支付是通过虚拟银行的电子资金划拨来完成的，实现这一过程涉及网络银行与网络交易客户之间的协议、网络银行与网站之间的合作协议、网络银行与网站之间的法律关系、网络银行与网站之间的安全保障问题。（　　）

2．身份认证的唯一方法是使用 IC 卡。（　　）

3．计算机安全控制的技术手段包括实体的安全性、运行环境的安全性和信息的安全性。（　　）

4．电子合同与传统合同有很大的区别，突出表现在商品信息、电子签名的有效性、合同证据、电子合同收到与合同成立地点等方面的问题。（　　）

5．资料汇编的基本要求是系统、完整、安全、及时。（　　）

6．资料汇编的基本要求是系统、完整、简明、集中。（　　）

7．身份注册类网上单证主要以表格形式出现，用于各网站收集用户信息和确认用

户身份。（　　）

8．中国银行推出的网上支付服务——“支付网上行”支持的信用卡包括长城借记卡和长城国际信用卡。（　　）

9．在对收集到的众多资料进行审查判别其真伪时，常采用的方法是专题审查。（　　）

10．因为在网上收集到的数据常有某些回复的资料不完整的情况，所以要进行数据的审查。（　　）

三、实践题

选择任意一家银行进行网上支付，并写出整个支付流程。