**模块1**

**一、名词解释**

电子交易：电子交易就是指在网上进行买卖交易。

电子支付：所谓电子支付（Electronic Payment）是指进行电子商务交易的当事人（包括消费者、厂商和金融机构）使用安全手段和密码技术通过电子信息化手段进行的货币支付和资金流转。

计算机病毒：计算机病毒是编制者在[计算机程序](http://baike.baidu.com/view/178184.htm)中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组[计算机指令](http://baike.baidu.com/view/786118.htm)或者程序代码。

黑客攻击：利用计算机的安全漏洞，入侵计算机系统的行为。黑客的破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的[数据](http://baike.baidu.com/view/38752.htm)为目的。

网络安全漏洞：[系统安全漏洞](http://baike.baidu.com/view/5555774.htm)是指可以用来对系统安全造成危害，系统本身具有的，或设置上存在的缺陷。漏洞主要是因为设计和实施中出现错误所致，造成信息完整性、可获得性和保密性受损。错误通常在[软件](http://baike.baidu.com/view/37.htm)中，也存在于各个信息系统层，从协议规格到设计到物理硬件。

**二、选择题**

1．下面哪个不是电子支付的“全能化”的“3A服务”。（D ）

A．Anytime B．Anywhere C．Anyhow D．Anyone

2．（ B ）是[公钥基础设施](http://baike.baidu.com/view/641671.htm" \t "_blank)的简称。

A．SET B．PKI C．EDI D．Intranet

3．电子支付的特征不包括哪些？（ A ）

A．通过现金的方式进行款项支付。

B．工作环境是基于互联网开放的系统平台。

C．使用的是最先进的通信手段，对软件、硬件设施的要求很高。

D．具有方便、快捷、高效、经济的优势。

4．.以下哪些问题会涉及资金的安全？（ D ）

A．黑客入侵 B．内部作案 C．密码泄露 D．以上都是

5．电子商务系统必须保证具有十分可靠的安全保密技术，必须保证网络安全（ C ）。

A．不可修改性  B．信息的稳定性  C．交易者身份的确定性  D．数据的可靠性

6．信息的完整性是指（ D ）。

A．信息不被他人所接收  B．信息内容不被指定以外的人所知悉

C．信息不被篡改 D．信息在传递过程中未经任何改动

**三、简答题**

1．与传统交易相比电子交易有哪些优势？

与传统交易方式相比，电子交易具有以下的优点：

①电子交易超越了传统商务的四大障碍：地域障碍、时间障碍、价格信息对比障碍和更换供货商的障碍。电子交易的实施可使厂商真正提供24小时不间断服务和全天候营业，方便客户和优化服务，客户可以足不出户、随心所欲地浏览网页和订货，并具有更多的选择余地。

②厂商可以根据客户浏览网页的习惯掌握客户的喜好和消费模式，有助于调整产品结构、生产和进货规划，同时厂商的直销、广告、宣传和市场调查可以不受地理位置的限制。

③降低企业内部人与人之间的互动成本。

④减少中间流通环节，实现零库存，降低成本，从而可使用户和厂商双双得利，也有利于遏制假货的出现。借助于因特网的覆盖范围和众多的用户，实现信息流通，扩大产品销路和选择低价质优的原料。

⑤减少交通费用，减缓交通压力，节省差旅费用。

2．与传统的支付方式相比，电子支付具有哪些优势？

与传统的支付方式相比，电子支付具有以下优势：

①电子支付适应了整个社会向信息化、数字化发展的趋势。电子支付是通过网络以先进安全的数字流转技术完成信息传输；而传统的交易支付方式则以传统的通信媒介通过现金、票据、银行兑汇等物理实体完成，无法满足信息社会高效、便捷的商务活动的需求。

②电子支付的工作环境是基于开放的系统平台（如互联网），而传统的交易支付方式则在较为封闭的系统中运行（如某银行的各分行之间）。工作环境的开放性使得商家加入电子支付系统更加方便快捷，没有障碍；而开放性带来的普遍性也使得消费者可以随时随地进行消费支付活动。

③电子支付是跨时空的电子化支付，能够真正实现全球7天24小时的服务保证。交易方只要有一台能够上网的PC机或者手机，就可以足不出户，在很短的时间内完成整个支付过程。

④电子支付有助于降低交易成本，最终为消费者带来更低的价格。传统的支付系统要求银行、分行、银行职员、自动取款机及相应的电子交易系统来管理现金和转账，成本非常高。而电子支付只需现有的技术设施、互联网和现有的计算机（手机）系统就可以，而且只需要少数系统维护人员。电子支付的交易效率较高，从而加快了资金周转速度，降低了企业的资金成本。

3．电子支付的流程包括哪些内容？

基于互联网平台的电子支付的基本流程如图1-3所示。根据工作流程图，可将整个电子支付工作程序分为下面七个步骤：

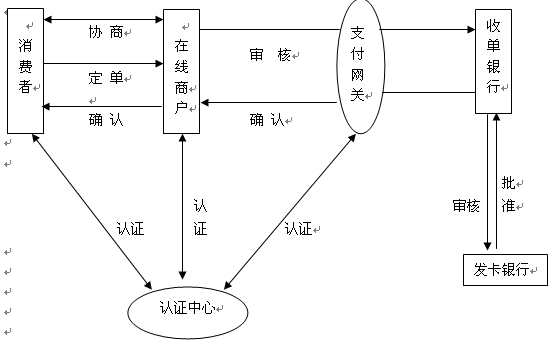


图1-3 基于Internet平台的电子支付的一般流程

① 消费者利用自己的PC机通过因特网选定所要购买的物品，并在[计算机](http://www.chinatat.com/jsj/)上输入定货单，定货单上需包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。

② 通过[电子商务](http://www.chinatat.com/dianzishangwushi/)服务器与有关在线商店联系，在线商店作出应答，告诉消费者所填定货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。

③ 消费者选择付款方式，如信用卡、电子钱包、电子现金、电子支票或网络银行账号等，确认定单，签发付款指令。此时SET（Secure Electronic Transaction称之为[安全电子交易协议](http://baike.baidu.com/view/1102909.htm" \t "_blank)）开始介入。

④ 在SET中，消费者必须对定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。

⑤ 在线商店接受定单后，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。

⑥ 在线商店发送定单确认信息给消费者。消费者端软件可记录交易日志，以备将来查询。

⑦ 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，或通知发卡银行请求支付。

4．电子商务面临的威胁有哪些？

（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，获取输入的机密信息，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，如消费者的银行账号、密码以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三个方面。

①篡改：改变信息流的次序，更改信息的内容，如篡改购买商品的出货地址等。

②删除：删除某个消息或消息的某些部分，比如一些淘宝店铺雇佣黑客删除差评，误导消费者。

③插入：在消息中插入一些信息，让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，收定货单；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，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、密钥等信息；接管合法用户，欺骗系统，占用合法用户的资源。由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨清真伪。

（4）恶意破坏

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入网络内部，其后果是非常严重的。

（5）交易抵赖

交易抵赖包括多个方面，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：购买者做了定货单不承认；商家卖出的商品因价格差而不承认原有的交易。

5．密码技术具体包括哪些？

它主要包括加密、签名认证和密钥管理三大技术。

①加密技术是保证电子商务安全的重要手段。所谓加密就是使用数学方法来重新组织数据，使得除了合法的接收者外，任何其他人要想恢复原先的“报文”或读懂变化后的“报文”是非常困难的。许多密码算法现已成为网络安全和商务信息安全的基础。密码算法利用密秘密钥（secret keys）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，从而获取敏感信息并保证了网络数据的机密性。

②密钥管理技术。密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁以及保密等内容。其中分配和存储是最棘手的问题。密钥管理不仅影响系统的安全性，而且涉及到系统的可靠性、有效性和经济性。在用密码技术保护的现代信息系统的安全性主要取决于对密钥的保护，而不是对算法或硬件本身的保护，即密码算法的安全性完全寓于密钥之中。

③数字签名。数字签名（Digital Signature）是公开密钥加密技术的一种应用，是指用发送方的私有密钥加密报文摘要，然后将其与原始的信息附加在一起，合称为数字签名。通过数字签名能够实现对原始报文的鉴别与验证，保证报文的完整性、权威性和发送者对所发报文的不可抵赖性。数字签名机制提供了一种鉴别方法，保证了网络数据的完整性和真实性。普遍用于银行、电子贸易等，以解决伪造、抵赖、冒充、篡改等问题。

④安全协议。安全协议是许多分布式系统安全的基础，是电子商务系统运行的安全通信标准。目前国际上流行的电子商务所采用的协议主要包括以下4个方面。

一是电子支付协议。电子支付作为电子商务中最重要的内容，目前已经出现了很多的电子支付协议。根据人们在现实生活中常见的有基于卡的支付协议、基于支票的支付协议和基于现金的支付协议。著名的有：First Virtual、SSL、SET、iKP、NetBill、E-Cash等。

二是安全HTTP（S—HTTP）协议。

三是安全电子邮件协议（如PEM、S/MIME等）。

四是用于公对公交易的Internet EDI（UN/EDIFACT）等。

⑤PKI技术。PKI是利用公钥算法原理和技术为网上通信提供通用安全服务的基础设施。它为电子商务、电子政务、网上银行证券等提供一整套安全基础平台。

密钥管理是电子商务安全业务中共同存在的问题，为解决在Internet上开展电子商务的安全问题，世界各国在经多年研究后，初步形成了一套完整的解决方案。PKI采用证书管理公钥，即结合x．509标准中的鉴别框架来实现密钥管理，通过CA把用户的公钥及其他标识信息捆绑在一起，在Internet上验证用户的身份，保证网上数据的保密性和完整性。

PKI的核心元素是数字证书，其核心执行者是认证机构。有关数字证书服务的应用，实施是广泛开展电子商务的基本前提，电子商务的深入开展离不开数字证书技术和认证机构的正确督导。

6．电子支付面临哪些安全威胁？

电子支付面临的安全问题主要表现在：

①计算机病毒。计算机病毒是编制者在[计算机程序](http://baike.baidu.com/view/178184.htm)中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组[计算机指令](http://baike.baidu.com/view/786118.htm)或者程序代码。计算机中毒后，可能会导致[正常](http://baike.baidu.com/view/491091.htm)的程序无法运行，把计算机内的文件删除或受到不同程度的损坏。通常表现为：增、删、改、移。中毒的计算机很有可能无法正常完成电子商务活动，或者无法进行正常的电子支付。

②黑客攻击。利用计算机的安全漏洞，入侵计算机系统的行为。黑客的破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的[数据](http://baike.baidu.com/view/38752.htm)为目的。在利益的驱使之下，入侵者在网上获取用户信息，将账单转嫁到目标[主机](http://baike.baidu.com/view/23880.htm)上，设立钓鱼网站，对用户进行诈骗。

③系统安全漏洞。[系统安全漏洞](http://baike.baidu.com/view/5555774.htm)是指可以用来对系统安全造成危害，系统本身具有的，或设置上存在的缺陷。漏洞主要是因为设计和实施中出现错误所致，造成信息完整性、可获得性和保密性受损。错误通常在[软件](http://baike.baidu.com/view/37.htm)中，也存在于各个信息系统层，从协议规格到设计到物理硬件。系统在安全方面存在漏洞，非法网站、病毒和非法插件会通过这个漏[洞入](http://www.baike.com/wiki/%E6%B4%9E%E5%85%A5)侵系统，会破坏系统的安全性，给电子支付带来巨大的威胁。

**四、论述题**

1．试论述电子支付安全的重要作用。

电子支付作为新型的支付方式，已经对电子商务和金融发展产生重大影响。这些影响主要表现在以下几个方面：

一是电子支付的发展能够提高电子商务和金融运行效率，节约交易成本，促进经济发展；二是电子支付为电子商务的发展提供了广阔的前景，有利于缓解并最终解决电子商务中的支付瓶颈问题；三是电子支付突破时空的限制，丰富了支付手段，促进金融创新改革和发展；四是电子支付方便了日常生活支付需要，有利于培养健康文明的支付习惯；五是电子支付将对货币政策，主要是对货币的基本定义、货币发行方式、货币流通速度和货币乘数等方面产生一定影响；六是电子支付工具特别是信用卡的使用将促进消费信贷发展，培育社会信用体系建设。