Chapter 5

第5章　电子商务交易安全

学习要点

- 电子商务安全体系；
- 电子商务安全控制要素；
- 电子商务安全管理；
- 数据加密技术；
- 数据签名技术；
- 数字证书；
- 电子商务安全交易协议。

5.1　电子商务安全概述

5.1.1　电子商务的安全问题

在传统交易过程中，买卖双方是面对面的，因此很容易保证交易过程的安全性和建立起信任关系。但在电子商务过程中，买卖双方是通过网络来联系的，甚至彼此可能远隔千山万水，也可能近在咫尺，因而建立交易双方的安全和信任关系相当困难。电子商务交易双方（卖方和买方）都面临不同的安全问题。

1. 卖方面临的问题

对卖方而言，面临的安全威胁主要有以下几个方面：

（1）中央系统安全性被破坏。入侵者假冒成合法用户来改变用户数据（如商品送达地址）、解除用户订单或生成虚假订单、盗用客户资料。

（2）竞争对手检索商品递送状况。恶意竞争者以他人的名义来订购商品，从而了解有关商品的递送状况和货物的库存情况。

（3）被他人假冒而损害公司的信誉。不诚实的人建立与卖方服务器名字相同的另一个服务器来假冒卖方。

（4）买方提交订单后不付款。

（5）获取他人的机密数据。比如，某人想要了解另一人在卖方处的信誉时，他以另一人的名字向卖方订购昂贵的商品，然后观察卖方的行动。假如卖方认可该订单，则说明被观察者的信誉高；否则，则说明被观察者的信誉不高。

2. 买方面临的问题

对买方而言，面临的安全问题主要有以下几个方面：

(1) 付款后不能收到商品。在要求客户付款后，卖方中的内部人员不将订单和钱转发给执行部门，因而使客户不能收到商品。

(2) 机密性丧失。客户有可能将秘密的个人数据或自己的身份数据(如账号、口令等)发送给冒充卖方的机构，这些信息也可能会在传递过程中被窃取。

(3) 拒绝服务。攻击者可能向卖方的服务器发送大量的虚假订单来穷竭它的资源，从而使合法用户不能得到正常的服务。

3. 信息传输问题

信息传输问题是指在进行网上交易时，因传输的信息失真或者信息被非法地窃取、篡改和丢失，而导致网上交易的不必要损失。从技术上看，网上交易的信息传输问题主要来自以下几个方面：

(1) 冒名偷窃。如“黑客”为了获取重要的商业秘密、资源和信息，常常采用源 IP 地址欺骗攻击。

(2) 篡改数据。攻击者未经授权进入网络交易系统，使用非法手段，删除、修改、重发某些重要信息，破坏数据的完整性，损害他人的经济利益，或干扰对方的正确决策，造成网上交易的信息传输问题。

(3) 信息丢失。交易信息的丢失，可能有三种情况：一是因为线路问题造成信息丢失；二是因为安全措施不当而丢失信息；三是在不同的操作平台上转换操作不当而丢失信息。

(4) 信息传递过程中的破坏。信息在网络上传递时，要经过多个环节和渠道。由于计算机技术发展迅速，原有的病毒防范技术、加密技术、防火墙技术等始终存在着被新技术攻击的可能性。计算机病毒的侵袭、“黑客”非法侵入、线路窃听等很容易使重要数据在传递过程中泄露，威胁电子商务交易的安全。此外，各种外界的物理性干扰，如通信线路质量较差、地理位置复杂、自然灾害等，都可能影响到数据的真实性和完整性。

(5) 虚假信息。从买卖双方自身的角度观察，网上交易中的信息传输问题还可能来源于用户以合法身份进入系统后，买卖双方都可能在网上发布虚假的供求信息，或以过期的信息冒充现在的信息，以骗取对方的钱款或货物。现在还没有很好地解决信息鉴别的办法。

4. 信用问题

信用问题主要来自以下三个方面：

(1) 来自买方的信用问题。对于个人买方来说，可能在网络上使用信用卡进行支付时恶意透支，或使用伪造的信用卡骗取卖方的货物；对于集团购买者来说，存在拖延货款的可能，卖方需要为此承担风险。

(2) 来自卖方的信用风险。卖方不能按质、按量、按时寄送买方购买的货物，或者不能完全履行与集团购买者签订的合同，造成买方的风险。

(3) 买卖双方都存在抵赖的情况。

传统交易时，交易双方可以直接面对面地进行交易，信用风险比较容易控制。由于网上交易时，物流与资金流在空间上和时间上是分离的，因此如果没有信用保证，网上交易是很难进行的。再加上网上交易一般是跨越时空的，交易双方很难面对面地交流，信用的风险就很难控制。这就要求网上交易双方必须有良好的信用，而且有一套有效的信用机制降低信

用风险。

5.1.2 电子商务安全体系

由于电子商务是在开放的网上进行的贸易,支付信息、订货信息、谈判信息、机密的商务往来文件等大量商务信息在计算机系统中存放、传输和处理,所以,其安全问题引起了广泛的重视。计算机诈骗、计算机病毒等造成的商务信息被窃、篡改和破坏,以及机器失效、程序错误、误操作、传输错误等造成的信息失误或失效,都严重地危害着电子商务系统的安全。因此,保证商务信息的安全是进行电子商务的前提。

电子商务系统是一个计算机系统,其安全性是一个系统的概念,不仅与计算机系统结构有关,还与电子商务应用的环境、人员素质和社会因素有关。它包括电子商务系统的硬件安全、软件安全、运行安全和电子商务安全立法。

1. 电子商务系统硬件安全

硬件安全是指保护计算机系统硬件(包括外部设备)的安全,保证其自身的可靠性和为系统提供基本安全机制。

2. 电子商务系统软件安全

软件安全是指保护软件和数据不被篡改、破坏和非法复制。系统软件安全的目标是使计算机系统逻辑上安全,主要是使系统中信息的存取、处理和传输满足系统安全策略的要求。

3. 电子商务系统运行安全

运行安全是指保护系统能连续和正常地运行。

4. 电子商务安全立法

电子商务安全立法是对电子商务犯罪的约束,它是利用国家机器,通过安全立法,体现与犯罪斗争的国家意志。

综上所述,电子商务安全是一个复杂的系统问题。电子商务安全立法与电子商务应用的环境、人员素质、社会有关,基本上不属于技术上的系统设计问题,而硬件安全是目前硬件技术水平能够解决的问题。鉴于现代计算机系统软件的庞大和复杂性,软件安全成为电子商务系统安全的关键问题。有关电子商务涉及的硬件、软件及网络安全可以参考有关的资料,本章仅讨论在电子商务交易过程中文件及信息传输的特殊安全问题。

与传统交易不同的是,网上交易的信息传输问题更为严重。传统交易中的信息传递和保存主要通过有形的单证进行,信息接触面比较窄,容易受到保护和控制。即使在信息传递过程中出现丢失、篡改等情况时,也可以通过留下的痕迹查找出现偏差的原因。而在在网上传递的信息,是在开放的网络上进行的,与信息的接触面比较多,而且信息被篡改时可以不留下痕迹,因此在网上交易时面临的信息传输问题比传统交易更为严重。

网上信息传输主要涉及信息传输的保密性、交易文件的完整性、信息的不可否认性及身份的真实性。

5.1.3 电子商务的安全控制要求

1. 信息传输的保密性

信息的保密性是指信息在传输过程或存储中不被他人窃取。因此,信息需要加密以及在必要的节点上设置防火墙。例如,信用卡号在网上传输时,如果非持卡人从网上拦截并知道了该号码,他也可以用这个号码在网上购物。因此,必须对要保密的信息进行加密,然后再放到网上传输。

2. 交易文件的完整性

信息的完整性是从信息传输和存储两个方面来看的。在存储时,要防止非法篡改和破坏网站上的信息。在传输过程中,接收端收到的信息与发送的信息完全一样,说明在传输过程中信息没有遭到破坏。尽管信息在传输过程中被加了密,能保证第三方看不到真正的信息,但并不能保证信息不被修改。例如,如果发送的信用卡号码是 9856,接收端收到的却是 9894,这样,信息的完整性就遭到了破坏。

3. 信息的不可否认性

信息的不可否认性是指信息的发送方不能否认已发送的信息,接收方不能否认已收到的信息。由于商情的千变万化,交易达成后是不能否认的,否则,必然会损害一方的利益。例如,买方向卖方订购石油,订货时世界市场的价格较低,收到订单时价格上涨了,如果卖方否认收到的订单的时间,甚至否认收到订单,那么买方就会受到损失。再例如,买方在网上买了书,不能说没有买,谎称发出的订单不是自己的。

4. 交易者身份的真实性

交易者身份的真实性是指在虚拟市场中确定交易者的实际身份。网上交易的双方很可能素昧平生,相隔千里。要使交易成功首先要能确认对方的身份,对商家要考虑客户端不能是骗子,而客户也会担心网上的商店不是一个玩弄欺诈的黑店。因此能方便而可靠地确认对方身份是交易的前提。对于为顾客或用户开展服务的银行、信用卡公司和销售商店,为了做到安全、保密、可靠地开展服务活动,都要进行身份认证的工作。对有关的销售商店来说,它们对顾客所用的信用卡的号码是不知道的,商店只能把信用卡的确认工作完全交给银行来完成。银行和信用卡公司可以采用各种保密与识别方法,确认顾客的身份是否合法,同时还要防止发生拒付款问题以及确认订货和订货收据信息等。

5.1.4 电子商务安全管理

电子商务安全管理关键是要落实到制度上。这些制度包括保密制度、系统维护制度、数据备份制度和病毒定期清理制度等。

1. 保密制度

信息的安全级别一般分为三级。

(1) 绝密级:此部分网址、密码不在因特网上公开,只限高层管理人员掌握。如公司经营状况报告、订货或出货价格、公司发展规划等。

(2) 机密级：此部分只限公司中层管理人员以上使用。如公司日常管理情况、会议通知等。

(3) 秘密级：此部分在因特网上公开，供消费者浏览，但必须保护程序，防止黑客侵入。如公司简介、新产品介绍及订货方式等。

2. 网络系统的日常维护制度

1) 硬件的日常管理和维护

用户通过自己的互联网参与电子商务，其日常管理和维护非常重要，特别是对那些运行关键任务的企业内部网，如银行、邮电、税务等。

网管人员必须建立系统档案，其内容应包括设备型号、生产厂家、配置参数、安装时间、安装地点、IP 地址、上网目录和内容等。对于服务器和客户机还应记录内存、硬盘容量和型号、终端型号及数量、多用户卡型号、操作系统名、数据库名等。这些内容可存于小型数据库，以方便查询和管理。

对于网络设备，一般都有相应的网管软件，可以做到对网络拓扑结构的自动识别、显示和管理，网络系统节点配置与管理系统故障诊断等，还可以进行网络系统调优、负载平衡等。对于不可管设备，应通过手工操作来检查状态，做到定期检查和随机抽查相结合，以便及时准确地掌握网络的运行状况，一旦有故障发生能及时处理。

对于内部线路，应尽可能采用结构化布线。虽然采用布线系统在初期会增加投资，但可大大降低网络故障率，有故障时也易排除。

2) 软件的日常维护和管理

对于支撑软件，一般需进行定期清理日志文件、临时文件，定期执行整理文件系统，检测服务器上的活动状态和用户注册数，处理运行中的死机情况。

对于应用软件主要是版本控制。设置一台安装服务器，当远程客户机软件需要更新时，可从网络上远程安装。注意选择网络负载较低时进行，以免影响网络的正常运行。

3) 数据备份制度

定期、完整、真实、准确地将数据转储到不可更改的介质上，并要求集中和异地保存，保存期限至少两年，保证系统发生故障时能够快速恢复。重要数据的存储应采用只读式数据记录设备，备份的数据必须指定专人负责保管；数据保管员必须对备份数据进行规范的登记管理，备份数据保管地点应有防火、防热、防潮、防尘、防磁、防盗设施等。

4) 用户管理

每个系统都设置了若干角色，用户管理等任务就是添加或者删除用户和用户组号。如添加一个用户，需先在客户机上添加用户并分配组号，然后在服务器数据库上添加用户并分配组号，最后分配该用户的访问权限。

3. 病毒防范制度

病毒对网络交易的顺利进行和交易数据的妥善保存构成严重的威胁，因此必须做到如下几点：

(1) 给电脑安装防病毒软件。防病毒软件有两种：一是单机版防病毒软件，另一种是联机版防病毒软件。联机版防毒软件能够在病毒入侵之前，及时阻止病毒侵入。

(2) 不打开陌生的电子邮件。电子邮件传播病毒的关键是附件，最好不要在进行网络交易时打开。

(3) 认真执行病毒定期清理制度。许多病毒都有潜伏期,定期清理制度可以清除处于潜伏期的病毒,防止病毒突然爆发。

(4) 控制权限。将网络系统中易感染病毒的文件属性、权限加以限制,对各终端用户允许只读权限,断绝病毒入侵的渠道。

(5) 高度警惕网络陷阱。对非常诱人的广告和免费使用的承诺,应保持高度警惕。

4. 应急措施

在计算机灾难事件发生时,利用应急计划辅助软件和应急设施排除灾难和故障,保障计算机继续运行。灾难事件包括由自然灾害直接导致的系统不能运行;因发电厂事故、信息服务商的问题导致的系统非正常运行;计算机本身所发生的数据丢失等灾难。其恢复工作包括硬件恢复和数据恢复。一般来讲,数据的恢复更为重要,目前运用的数据恢复技术主要是瞬时复制技术、远程磁盘镜像技术和数据库恢复技术。

1) 瞬时复制技术

瞬时复制技术就是使计算机在某一灾难时刻自动复制数据的技术。现有一种瞬时复制技术是通过使用磁盘镜像技术来复制数据。它利用空白磁盘和每一个数据磁盘相连,将数据复制到空白磁盘。在复制进行过程中,为保证数据的一致性,使用数据的应用程序被暂时挂起。当复制完成时,瞬时复制磁盘与数据磁盘脱离连接,应用程序继续运行。瞬时复制的备份数据可以典型地用来产生磁带备份或用做远程恢复节点的基本数据。

目前,许多系统厂商、存储设备供应商和软件开发商已利用这一技术开发了多种瞬时复制产品。

2) 远程磁盘镜像技术

远程磁盘镜像技术是在远程备份中心提供主数据中心的磁盘镜像。这种技术最主要的优点是可以把数据中心磁盘中的数据复制到远程备份中心,而无须考虑数据在磁盘上是如何组织的。系统管理员仅需要确定哪些磁盘需要备份到远程备份中心,存储在这些磁盘上的数据会被自动地备份到远程备份中心,这对应用系统的安全非常有利。

3) 数据库恢复技术

数据库恢复技术是产生和维护一份或多份数据库数据的复制。数据库复制技术为用户提供了更大的灵活性。数据库管理员可以准确地选择哪些数据可以被复制到哪些地方。对于那些在日常应用中经常使用大量联机数据的用户,可以选择少量最为关键的数据。复制服务器比磁盘镜像更加灵活,支持对数据的多个复制。

数据库复制技术提供了非常灵活的手段,可在灾难发生后恢复应用数据,但还不是完整的解决方案,必须考虑其他方法作为补充。因为数据库复制技术不能复制非数据库格式的数据,一些应用系统的主要数据存储于数据库中,但通常也使用大量的常规文件。对于一些非常重要的数据或从数据库生成的数据,通常存放在文件中,有些应用系统的数据不能转换成数据库数据,配置文件、批量控制文件、应用程序的镜像和其他的管理文件通常不以数据库格式存储。所以,将数据库复制技术与远程磁盘镜像技术配合使用,常常可以获得更好的效果。

5. 浏览器安全设置

Internet Explorer 是使用最广泛的浏览器,它使用方便,功能强大,但由于它支持 JavaScript 脚本和 Active X 控件等元素,使得在利用它浏览网页时存在很多安全隐患。这

里简单介绍一下 Internet Explorer 的安全配置手段,但注意利用网页进行攻击是很难防范的,没有特别有效的方法,而且安全的配置都是以失去很多功能为代价的。

1) 管理 Cookies 的技巧

在 IE 6.0 中,打开 IE 的"工具"菜单的"Internet 属性"中的"隐私"选项卡,可以管理 Cookies。

Cookies 有六个安全级别,分别是"阻止所有 Cookies""高""中高""中""低""接受所有 Cookies"(默认级别为"中"),分别对应从严到松的 Cookies 策略,可根据需要方便地进行设定。

通过 IE 6.0 的 Cookies 策略,就能个性化地设定浏览网页时的 Cookies 规则,更好地保护自己的信息,增加使用 IE 的安全性。例如,在默认级别"中"时,IE 允许网站将 Cookies 放入你的电脑,但拒绝第三方的操作。

2) 禁用或限制使用 Java、Java 小程序脚本、Active X 控件和插件

互联网上经常使用 Java、Java Applet、Active X 编写的脚本,它们可能会获取用户的用户标识、IP 地址和口令等信息,影响系统的安全。因此应对 Java、Java 小程序脚本、Active X 控件和插件的使用进行限制。

选中 IE "工具"菜单的"Internet 属性"中的"安全"选项卡,在这里 Internet Explorer 将 Internet 划分为四个区域,分别是 Internet、本地 Intranet、受信任的站点和受限制的站点。用户可以将网站分配到具有适当安全级的区域。通过"自定义级别"对不同的区域设置不同的安全级别。

安全级别包括"Active X 控件和插件""Microsoft VM""脚本""下载""用户验证"以及其他六项,每一项均可展开进行详细配置,对于一些不安全或不太安全的控件或插件以及下载操作,应该予以禁止、限制或至少要进行提示。

例如,在设置 Script Active X controls marked safe for Scripting(对标记为可安全执行 Active X 控件执行脚本)项的时候,可根据信任级别来选择允许、禁止或是提示,默认情况为允许。

3) 调整自动完成功能的设置

默认条件下,用户在第一次使用 Web 地址、表单、表单的用户名和密码后(如果同意保存密码),在下一次再想进入同样的 Web 页及输入密码时,只需输入开头部分,后面的就会自动完成,给用户带来了便利,但同时也带来了安全问题。

可以通过调整"自动完成"功能的设置来解决该问题。可以做到只选择针对 Web 地址、表单和密码使用"自动完成"功能,也可以只在某些地方使用此功能,还可以清除任何项目的历史记录。为了安全起见,防止泄露自己的一些信息,应该定期清除历史记录。

EC 聚焦——网络黑客

某年 2 月 7 日至 9 日,短短三天时间内,美国几大主要网站遭受不明黑客攻击,其中包括著名的电子商务网站 eBay 和 Amazon。在黑客开始所谓"拒绝服务"式的攻击后,Amazon 站点容纳顾客的能力急剧下降。数分钟后访客数量只有平时同一时段访客数量的

1.5%，大约一小时后，Amazon网站才恢复正常。Buy.com的一台服务器在两三个小时内速度减慢，而E-Trade则瘫痪了三个小时。据统计，三天来黑客袭击各大网站所造成的直接或间接经济损失高达数十亿美元以上。

信息风险对电子商务的损害是双重的，它不仅给商务网站造成了巨大的经济损失，而且更为严重的是降低了消费者和风险投资机构对电子商务的信心，从而影响到电子商务的长期发展。信息安全已成为制约电子商务发展的瓶颈之一。已从事或准备从事电子商务的企业不得不面对这样一个严峻的事实。

5.2 电子商务安全技术

5.2.1 数据加密技术

1. 加密和解密

加密技术目的是为了防止合法接收者之外的人获取信息系统中的机密信息，是实现信息保密性的一种重要的手段。所谓信息加密技术，就是采用数学方法对原始信息（通常称为“明文”）进行再组织，使得加密后在网络上公开传输的内容对于非法接收者来说成为无意义的文字（加密后的信息通常称为“密文”）。通过解密过程得到原始数据（即“明文”）。加密和解密过程依靠两个元素，缺一不可，这就是算法和密钥。算法是加密或解密的一步一步的过程。在这个过程中需要一串数字，这个数字就是密钥。

由此可见，在加密和解密的过程中，都要涉及信息（明文、密文）、密钥（加密密钥、解密密钥）和算法（加密算法、解密算法）这三项内容。

密钥是用于加、解密的一些特殊信息，它是控制明文与密文之间变换的关键，它可以是数字、词汇或语句。密钥分为加密密钥和解密密钥，完成加密和解密的算法称为密码体制，传统的密码体制所用的加密密钥和解密密钥相同，形成了对称式密钥加密技术。在一些新体制中，加密密钥和解密密钥不同，形成非对称式密码加密技术，即公开密钥加密技术。

2. 密码系统的构成

密码系统的一般构成如图5-1所示。

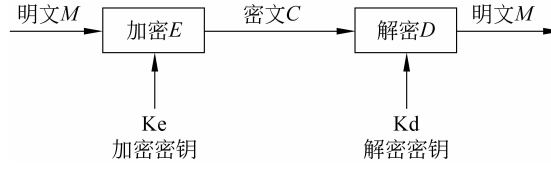

图5-1 密码系统的构成

密码系统的工作过程是，发送方用加密密钥Ke和加密算法E，对明文M加密，得到的密文$C=E(\mathrm{Ke},M)$，传输密文C。接收方用解密密钥Kd（与加密密钥Ke成对）和解密算法D，对密文解密，得到原来的明文$M=D(\mathrm{Kd},C)$。

对于不知道Kd的第三者，由密文C破解出明文M（解密），在实际上几乎是不可能的。

密码系统使用的密码体制，按密钥的形式可以分为两类：通用密钥密码体制和公开密钥体制。

3. 通用密钥密码体制

所谓通用密钥密码体制，就是加密密钥 Ke 和解密密钥 Kd 是通用的，即发送方和接收方使用同样密钥的密码体制，也称为“传统密码体制”。通用密钥密码体制可采用各种不同的算法，构成各种不同类型的密钥，例如，人类历史上最古老的“恺撒密码”算法，是在古罗马时代使用的密码方式。由于无论是何种语言的文字，恺撒密码都可以通过编码与二进制数字串对应，所以经过加密的文字仍然可变换成二进制数字串，不影响数据通信的实现。现以英语为例，用一个简单的实例说明使用恺撒密码方式的通用密钥密码体制的原理。

以英语为例，恺撒密码的原理是：对于明文的各个字母，根据它在 26 个英文字母表中的排列位置，按某个固定间隔 n 变换字母，即得到对应的密文。这个固定间隔的数字 n 就是加密密钥，也是解密密钥。

例如英文单词：cryptography 是明文，使用密钥 $n=4$，加密过程如图 5-2 所示。

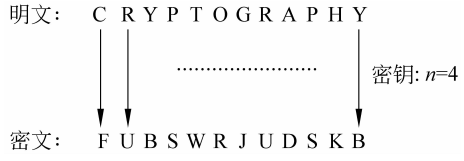

图 5-2　恺撒密码

说明如下：明文的第一个字母 C 在字母表中的位置设为 1，以 4 为间隔，往后第四个字母是 F，把 C 置换为 F；同样，明文中的第二个字母 R 的位置设为 1，往后第四个字母是 U，把 R 置换为 U；以此类推，直到把明文中的字母置换完毕，即得到密文。密文是意思不明的文章，即使第三者得到也毫无意义。通信的对方得到密文之后，用同样的密钥 $n=4$，对密文的每个字母，按往前间隔 4 得到的字母进行置换的原则，即可解密得到明文。

恺撒密码方式的密钥只有 26 种，只要知道了算法，最多将密钥变换 26 次做试验，即可破解密码。因此，恺撒密码的安全性依赖于算法的保密性，是最原始的密码技术，但是，其原理为现代高级密码技术奠定了基础。其后出现的一些算法与恺撒密码大同小异，直到 17 世纪，近代数学的发展成就应用于密码学，才使密码技术有了突破性进步，例如出现了多表式密码、转置式密码等。下面用一个简单的实例说明多表式密码的算法。

简单的多表式密码的例子如图 5-3 所示。

说明如下：本例中密钥字串与明文同样长度(也可不同长度)，明文中每一个字母往后移动的间隔，与它在密钥字串中对应的字母本身在字母表中的位置有关。本例中，明文的第一个字母 H，对应密钥字串的第一个字母 E，E 在字母表中的位置是 5，则 H 往后第五个字母是 L，因此将 H 置换为 L。以此类推，明文每个字母置换时，移动的间隔不同。

以恺撒密码为代表的单字符换字方式，若根据明文中字符出现的频率的统计特性，是比较容易破解的，例如，普通的英语文章中使用频率高的字母依次是：E，T，A，O，I，N，…的顺序。多表式密码，正是为了克服上述缺点而开发的密码技术。本例中，密钥使用字符串 ENGLANDEN，明文置换为密文的间隔是依次变化的。而且，密钥字串越长，明文中字符的频率分布特性在密文中越不明显，根据频率分布破解密码的可能性越小。如果，使用与明文

同样长度的密钥字串，而且限定只能使用一次，那么，理论上破解密码将是不可能的。但是，这种情况下密钥的管理和传递也随之更困难。

通用密钥密码体制用于公众通信网时，每对通信对象的密钥不同，必须用不被第三者知道的方式，事先通知对方。通用密钥密码体制如图 5-3 所示。

	H O W A R E Y O U	…	明文
+)	E N G L A N D E N	…	密钥字串
	L B C L R R B S H	…	密文

图 5-3 通用密钥密码体制

随着通信对象的增加，公众通信网上的密码使用者，必须保存所有通信对象的大量的密钥。这种大量密钥的分配和保存，是通用密钥密码体制存在的最大问题。

目前得到广泛应用的通用密钥密码体制的典型代表是 DES 算法。DES 是由“转置”方式和“换字”方式合成的通用密钥算法，它先将明文(或密文)按 64 位分组，再逐组将 64 位的明文(或密文)，用 56 位(另有 8 位奇偶校验位，共 64 位)的密钥，经过各种复杂的计算和变换，生成 64 位的密文(或明文)，该算法属于分组密码算法。

DES 算法可以由一块集成电路实现加密和解密功能。该算法是对二进制数字化信息加密及解密的算法，是通常数据通信中用计算机对通信数据加密保护时使用的算法。DES 算法在 1977 年作为数字化信息的加密标准，由美国商业部国家标准局制定标准，称为“数据加密标准”，并以“联邦信息处理标准公告”的名称于 1977 年 1 月 15 日正式公布。使用该标准，可以简单地生成 DES 密码。

4. 公开密钥密码体制

公开密钥密码体制的加密密钥 Ke 与解密密钥 Kd 不同，只有解密密钥是保密的，称为私人密钥(private key)，而加密密钥完全公开，称为公共密钥(public key)。该系统也称为“非对称密码体制”。当然，对于从加密密钥破解出解密密钥的过程必须设计得足够复杂，以至于难以实施。

使用该系统，可以解决通用密钥系统密钥管理的问题，即对应于各个使用者的加密密钥(公共密钥)是公开的，可以像电话簿一样，存储于文件中，文件保存在密钥中心。如图 5-4 所示，各使用者只需保存一个只有自己使用的解密密钥(私人密钥)，因此，解决了密钥管理问题。通过公众通信网，与众多非特定的通信对象通信时，为了保密，使用公开密钥密码体制，显然有极大的优越性。

使用该体制时，例如，与 X 秘密通信时，可以用 X 的公共密钥 Kex 生成密文 $C=E(\mathrm{Kex},M)$，传输给 X，X 收到密文后，用只有自己知道的私人密钥，即保密的解密密钥 Kdx，计算出明文 $M=D(\mathrm{Kdx},C)$，用这种公开密钥密码体制，可以与任何对象秘密通信。

公开密钥密码体制的另一个优点是可以确认发送方的身份，即具有“数字签名”的功能。例如，接收方 Y 想在通信文上署名时，可以用自己的私人密钥 Kdy 生成署名文 $V=D(\mathrm{KdY},M)$，然后，将 V 和自己的姓名 NY 一起传输给对方。发送方从姓名 NY 检索出 Y 的公共密钥 Key，计算 $M=E(\mathrm{Key},V)$，如果复原的 M 文是有意义的信息，则可确认 Y 是合法的授信者，并确认通信途中未发生篡改信息的事件。利用 Internet 通信时，具有数字证书