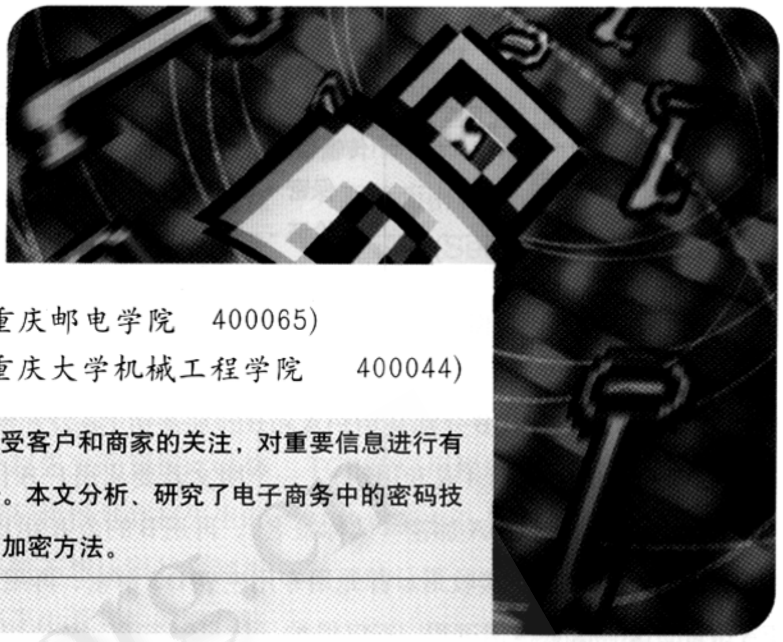
基于电子商务的信息密码技术



陈 勇 （重庆邮电学院 400065）
刘焕淋 （重庆大学机械工程学院 400044）

摘要 随着电子商务的发展，其重要信息的安全也倍受客户和商家的关注，对重要信息进行有效加密已成为保护客户和商家的重要措施之一。本文分析、研究了电子商务中的密码技术特点，探讨了在电子商务中保证数据安全的加密方法。

关键词 电子商务 信息安全 密码技术

1 前言

电子商务是利用公共信息通信网进行商贸活动的总称[1]，其组成及环境如图1，它包括客户、网上商店、支付网关、认证中心和通信平台—因特网。

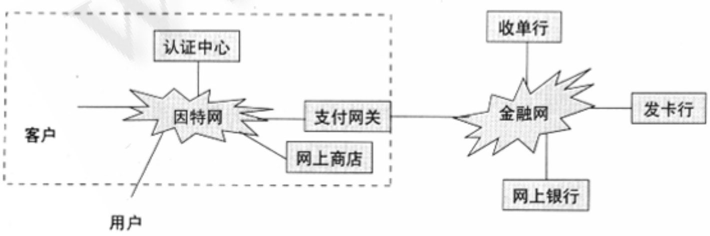


图 1 电子商务的组成环境

电子商务与传统商贸活动最大的不同是：一方面，电子商务中购销双方不可见，相互间对身份真实性存有疑虑；另一方面，电子商务所含的信息流、资金流都是网上进行的，需通过不安全的因特网环境。

因此，在电子商务中，安全性是必须考虑和解决的核心问题[1]。在网上进行电子商务活动的核心问题就是安全性问题。数据加密技术、数据签名技术和数据指纹技术是保证电子商务的数据传输安全、数据完整性、有效的身份验证、交易的不可抵赖特点的重要手段。密码技术是确保信息安全保密的最常用技术，它可以把某些重用信息或数据从一个可理解的明文形式变换成一种错乱（即加密）的不可理解的密文形式后，在线路上传送或在数据库中存储，用户再将密文还原成明文(即解密)。因此，密码技术在电子商务中起着非常重要的作用。

2 密码技术一般原理

在电子商务中，获得广泛应用的现代密码体制有两大类，即单钥密码体制和双钥密码体制 [2] [3] [4]。

单钥密码体制是指信息的发送方和接收方共享一把密钥。在现代网络通信条件下，该体制的一个关键问题是如何将密钥安全可靠地分配给通信的对方，并进行密钥管理。如图2所示。

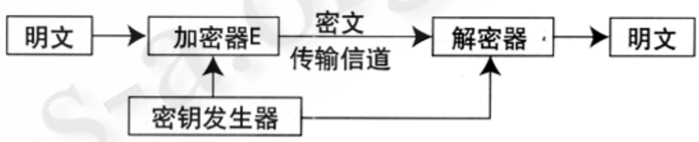


图 2 单密钥体制的加密与解密

由图2可知，单钥密码体制在实际应用中除了要设计出满足安全性要求的加密算法外，还必须解决好密码的产生、分配、传输、存储和销毁等多方面问题。因为电子商务中通信对象的多元性导致了一个用户必须拥有多个不同对象的密钥，方可安全可靠地进行通信。

双钥密码体制，其最大特点是采用两个密钥将加密、解密分开。在双钥体制下，每个用户都拥有两把密钥A和B，一个公开，一个自己专用，公开密钥可以公开得到，用于确认数字签名、信息加密；而私钥为使用者自己拥有，用于创建数字签名、信息解密。

当使用用户专用密钥加密，而用该用户公开密钥解密时，则可实现一个被加密的消息可被多个用户解读；当使用用户公开密钥加密，而由该用户专用密钥解密时，则可

实现传输的信息只被一个用户解读。前者常被用于数字签名，后者则常用于保密通信。

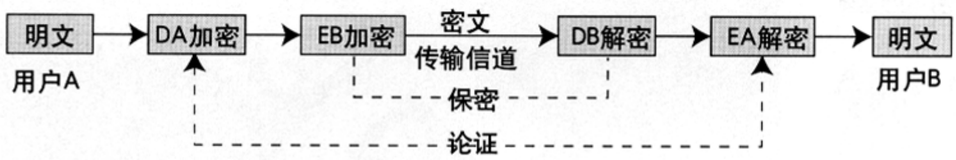


图 3 双密钥体制的加密和解密

在图3中，EA和EB分别是用户A和B的加密钥（或公开钥），DA和DB分别是A和B的解密钥（或专用钥）。一个明文若要从用户A传输到用户B，先要用A的专用密钥DA加密（又称签名），再用B的公开钥EB加密，然后传送到接收方B；B在接收后，首先用专用密钥DB解密，再用A的公开密钥EA认证。这一信息传递过程，不仅保护了信息的安全，又使接收方B对信息的发送方A确信无疑。

3 密码算法的分类

信息密码体制的两大类别基本涵盖了常用的加密算法，分为单钥密码和双钥密码，如下表所示。

密码分类表

单钥密码			双钥密码
古典密码	流密码	分组密码背	RSA，DSA，
换位密码 移位密码 乘积密码 同态密码 Hill 密码	混沌密码 量子密码 等	DES，Triple DES，MMB，IDEA， RC-4，RC-2，Safer k-64， Khufa，Shark，Cast，Feal-N， Khafre，Lucifer，Loki-89， Skipjack，Madraga，AES 等	Rabin， 背包密码， ELGamal， QRS 等

单钥密码包括古典密码、流密码和分组密码三类，分组密码将数据分成块进行加密，流密码对数据字节流或位流进行加密。流密码作为一个吸收了古典密码算法优点的加密机制，一直被人们广泛关注，混沌理论在密码学上的应用，目前只是由于其在数学上难以突破，一时还未有十分成功的应用推出；量子密码在传输距离上与实际光纤还有一定的差距，还需在实验室进行一段时间的研究。分组加密算法是近20年来最为活跃的加密手段之一，其算法有很多，最为著名的当推DES（Data Encryption Standard），该算法于1977年正式投入使用，一直用到1998年，20多年来一直作为美国联邦信息加密处理标准。

DES采用分组方式工作，它的基本思想是将二进制序列的明文分成每64位一组，用长为64位的密钥对这些明文进行16轮代换和置换加密，这些运算被称为函数f，在运算过程中数据于密匙结合。经过16轮候，左(L)，右半部分(R)合在一起经过一个末置换，最后形成密文，输出密文也为64位。它的巧妙之处就在于，除了密钥输入顺序之外，其加密和机密的步骤完全相同，从而在制作DES芯片时很容易达到标准化和通用化，非常适合现代通信的需要。DES算法目前已广泛用于电子商务系统中，算法过程如图4所示。

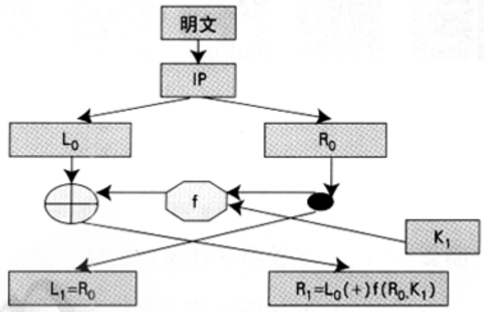


图 4 DES算法过程

但不幸的是，由于它时间久远，从而成为古往今来黑客们乐此不疲的攻击对象。随着研究的发展，针对DES的缺陷，DES在基本不改变加密强度的条件下，发展了许多变形DES。1992年命名的"国际加密标准"-IDEA算法，它的分组长度为64比特，密钥长度128位，硬件实现速度比DES快将近10倍，该算法的核心是设计了一个乘法/加法非线性构件，通过8轮迭代，能使明码信息更好地扩散和混淆。目前，尚无一篇公开发表的试图对IDEA进行密码分析的文章。因此，就现在来看应当说IDEA是非常安全的。

在双钥密码体制中，最具代表性的算法当数RSA，它从1979年公布至今，一直是加密中的主要算法之一，尽管该算法吸引了无数研究者，但在数学上还未找到最佳破译方法。RSA算法的核心建立在两个足够长（100位十进制）的大素数基础上，选择两个大素数，p和q。计算：n = p * q；然后随机选择加密密钥e，要求e和(p-1)*(q-1)互质；最后，利用Euclid算法计算解密密钥d，满足e * d = 1 (mod (p-1)*(q-1))，其中n和d也要互质。数e和n是公钥，d是私钥。两个素数p和q不再需要，

应该丢弃，不要让任何人知道。以目前每秒运行100万步的计算资源来破译则大约需1023步，相当于1000 年。因此，RSA算法在计算理论上仍然是十分安全的。由于RSA的加密/解密互为逆运算，因此，该算法不仅可用于信息加密，也可用于数字签名认证，如图 3 所示。

其他的双钥密码体制，有些虽很著名，但已被破译，如背包密码；有些还处于研究和发展阶段，如椭圆曲线密码；有些密码体制在算法上与RSA 有相似之处，破译的途径之一是大素数的分解，如Rabin、ElGamal体制等。

4 加/解密技术在电子商务中的应用分析

在信息安全领域中，凡涉及到数据通信均需采用加/解密技术。而目前日益发展的电子商务正是充分展示加/解密技术的一个十分重要的领域。电子商务涉及到的对象总体上可分四类，即客户、网上商店、网上银行、认证中心，它们之间的关系如图5所示。

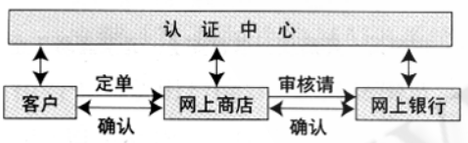


图 5 电子商务关系图

在交易之前，客户、商店和银行均需在认证中心注册，以获取唯一的身份号码ID。为了使交易具有安全可靠性、防抵赖性、防假冒性等，这三者的每一次交易通信均应被认证中心确认，而认证的重要工具便是数字签名。被认证者只需将自己的ID用双钥体制中的私钥加密，并发送给认证中心，认证中心便从公钥信箱中找出能解读此ID的那把公钥，便可确认ID的身份，并注册交易，每一步的确认过程就是一个认证的过程。

在电子商务中，订单的保密性需用加密技术来处理，而订单的可靠性、时间性等则需用数字签名技术，有时往往还要双重签名。例如，王小姐要买赵先生的一款轿车，她发给赵先生一个购买报价单及她对银行的授权书消息，如果赵先生同意按此价格出卖，则要求银行将钱划到赵先生的账上。但是王小姐不想让银行看到报价，也不想让赵先生看到她的银行账号信息。此外，报价和付款是相连的、不可分割的，仅当赵先生同意她的报价，钱才会转移。要达到这个要求，采用双重签名即可实现。

具体的实现方法是：首先生成两条消息的摘要，将两个摘要连接起来，生成一个新的摘要（称为双重签名），然后用签发者的私有密钥加密，为了让接收者验证双重签名，还必须将另一个消息的摘要一起传过去。这样，任何一个消息的接收者都可以通过以下方法验证消息的真实性：生成消息摘要，将它和另外一个消息摘要连接起来，生成新的摘要，如果它与解密后的双重签名相等，就可以确定消息是真实的。在上面的例子中，如果赵先生同意，他发一个消息给银行表示他同意，另外包括报价单的消息摘要，银行能验证王小姐授权的真实性，用王小姐的授权书生成的摘要和赵先生消息中的报价单的摘要验证双重签名。银行根据双重签名可以判定报价单的真实性，但却看不到报价单的内容。

5 电子商务的安全协议

目前,Internet 上有几种安全协议在使用,对应OSI每一层都已经提出了相应的协议。对应用层有SET(安全电子交易)协议,对会话层有 SSL(安全套接层)协议。这两种协议对电子商务的关系最为密切。

5.1 SSL(Secure Sockets Layer)安全协议

SSL主要用于提高应用程序之间的数据的安全系数。它涉及所有的TCP/IP应用程序,提供代理、服务器会话的有关安全业务,包括:服务器认证、代理的认证、完整性、保密性。

SSL由两个子协议构成,即SSL记录(Record)协议和SSL 握手(Handshake)协议。前者定义了会话中传递的所有数据项的基本格式,提供压缩数据、生成数据的完整性检验值(MAC)、对数据进行加密、标示数据长度、填充、流水作业号,并支持不同的加解密和杂凑算法。后者用作代理/服务器之间相互认证所用的算法、传送所需的公钥证书、建立SSL记录协议处理完整性校验和加密所需的会话密钥。SSL握手协议是较SSL记录协议更高层的协议,必须先执行握手协议后,才可能实现 SSL 记录协议中的加密和完整性校验。

在电子商务交易过程中,由于有银行参与,按照 SSL 协议,客户购买的信息首先发往商家,商家再将信息转发银行,银行验证客户信息的合法性后,通知商家付款成功,商家再通知客户购买成功,将商品寄送客户。在SSL协议中主要提供三方面的服务:(1)认证用户和服务器,使得他们能够确信数据将被发送到正确的客户和服务器上;(2)加密数据,以保证数据在传送过程中的安全,即使数据被窃,盗窃者没有解密密钥也得不到可读的资料;(3)维护数

据的完整性,确保数据在传送过程中不被改变。

SSL协议运行的基点是商家对客户信息保密的承诺。客户的信息首先传到商家,商家阅读后再传到银行。这样,客户资料的安全性便受到威胁。另外,整个过程只有商家对客户的认证,缺少了客户对商家的认证。

5.2 SET(Secure Electronic Transaction)安全协议

SET使用信用卡进行Internet支付,它是开放网络环境中的卡支付安全协议,支持了电子商务的特殊安全需要。它提供对消费者、商户和收单行的认证,确保交易数据的安全性、完整性和交易的不可否认性,特别是保证了不会将持卡人的信用卡号泄露给商户。SET函盖了信用卡在电子商务贸易中的交易协定、信息保密、资料完整及数字认证、数字签名等。这一标准被公认为全球国际网络的标准。

SET协议包含SET证书、认证中心(CA,Certificate Authority)、支付网关以及用户注册等内容。SET证书主要包含申请者的个人信息和其公共密钥。在SET中,主要有由持卡人认证中心、商户认证中心、支付网关认证中心颁发的持卡人证书、商户证书和支付网关证书。认证中心负责发放和管理用户的数字证书。支付网关是金融专用网与公用网之间的接口,是金融网的安全屏障。用户注册由持卡人注册和商户注册两部分构成。

SET的缺点是它在相互操作方面存在着一些问题。它的局限性还在于它仅限于使用信用卡方式的支付手段,用户需要安装特殊的软件,并且因网络带宽等原因,速度问题比较突出。

中国的商业银行在其电子支付系统中普遍选择了国际上流行的SSL和SET两种。

6 结论

尽管双钥密码体制较单钥密码体制更为可靠,且无需复杂的密钥管理,大多数双钥体制还可用于数字签名,然而,由于其计算的复杂性,在进行大信息量通信时,其速率为单钥体制的1/1000～1/100。正是由于不同体制的加密算法各有所长,预计在今后相当长的一段时期内,各类加密体制将共存、混和使用。

建立一个电子商务能完全开展的环境,不是说一个产品或者一项技术就能解决问题,如果我们在电子支付方面采用了双钥体制,势必需要一个权威认证中心。因此,电子商务发展还需要各行业、各部门的管理和协调。■

参考文献

1 张辛平主编,电子商务技术,电信业务实用全书(中卷),台海出版社。

2 Arto Salomaa著,丁存生、单炜娟译,公钥密码学,北京国防工业出版社,2000,10。

3 W.Diffie and M.Hellman: New directions in cryptography.IEEE Transactions on Information Theory IT-22(1976).Page 644 to 654。

4 冯登国、卿斯汉,信息安全,北京国防工业出版社,2000,6。