电子商务的数据加密算法

On the Data Encrypted Algorithms of Electronic Commerce

周兆祥

Zhou Zhaoxiang

(南宁职业技术学院,广西南宁 530007)

(Nanning Coll. for Vocational Tech., Nanning, Guangxi, 530007, China)

摘要:介绍电子商务高层和低层的2个应用层面,分析数据加密算法中的对称加密算法和非对称加密算法,对电子商务的数据加密算法进行了展望。认为非对称加密算法由于易于理解和操作,是目前普遍使用的算法;对称算法由于具有速度快的优点,主要用于对实时性要求较高的领域;摘要函数、多步加密法、插入校验码、生物识别技术将是电子商务数据加密算法下一步的研究方向。

关键词:电子商务 数据加密 解密 算法

中图法分类号:TP393 **文献标识码**:A **文章编号**:1002-7378(2005)02-0115-03

Abstract: The high and low levels of E-commerce application are introduced. An analysis is preformed on symmetric and non-symmetric algorithms in data encrypted algorithm. The non-symmetric algorithm is widely used currently due to its easy understanding and operation, while the symmetric algorithm is applied in the field of high demand in real time owing to its fast speed. The abstract function, multi-step encryption method, inserted checking code and biologicallyidentified technology would be the coming research hotspots in E-commerce encryption algorithm.

Key words: electronic commerce, data encryption, decryption, algorithm

20世纪90年代以来,计算机网络技术得到了飞速的发展,网络化和全球化成为不可抗拒的世界潮流。计算机网络技术一直在寻找除文字处理和信息传递领域外的更大、更直接的利润空间,商务领域自然成为其首选对象[1]。电子商务从单纯的网上发布信息、传递信息到在网上建立商务信息中心,从借助于传统贸易手段的不成熟的电子商务交易到能够在网上完成供、产、销全部业务流程的电子商务的虚拟实现,从封闭的银行电子金融系统到开发式的网络电子银行,电子商务如火如荼[2]。电子商务的本质是企业利用电子方式在客户、供应商和合作伙伴之间实现在线交易、相互协作和价值交换。电子商务(不管是B2B还是C2C)的实质就是帮助企业实现网络技术与传统资源的有效结合[3]。

电子商务目前可分为:信息服务、交易和支付等3个方面,主要包括:电子商情广告;电子选购和交易、电子交易凭证的交换;电子支付与结算以及售后的网上服务等。电子商务的手段包括网络营销、网络客户服务、网络调查以及网络广告等等。电子商务具有开放性、全球性、低成本、高效率的特点,因而其安全问题深受人们的关注。

由于电子商务的安全保障不单纯是技术问题,还涉及管理、制度、法律、历史、文化、道德等诸多方面。从技术层面上看,电子商务除了信息的保密性外,还涉及信息的完整性、信息的非否认性、信息发送者的可鉴别性、信息的可用性、信息的可控性等[4]。从信息保密层面看,加密技术包括密码算法设计、密码分析、安全协议、身份认证、消息确认、数字签名、密钥管理、密钥托管等多项内容。本文尝试从加密算法设计的角度来论述电子商务的安全防范技术。

1 电子商务的应用层次及其数据加密技术

1.1 电子商务的应用层次

从贸易活动的角度分析,电子商务可分为较低层次和高层次。较低层次的电子商务如电子商情、电

收稿日期:2005-04-18

作者简介:周兆祥(1943-),男,湖南湘潭人,副教授,主要从事计算机教学工作。

子合同、电子贸易等，它虽然还没有充分利用因特网网络资源，但也必须建立可靠的网上安全认证体系。该层次的电子商务必须对数据进行加密并进行身份的验证、授权、抗否认、自动撤消检查等。此时，电子商务服务系统要做好交易主体的身份识别，交易记录的保存和管理，同时保护电子通讯的安全和交易过程的商业秘密，对未经授权的入侵要能有效的拦截，使得在网络中交易的各方都具有平等的安全地位。

高层次电子商务的特点是更充分地利用因特网网络进行全部的贸易活动，即在网上将信息流、商流、资金流和部分的物流完整地实现。也就是说，从寻找客户，一直到洽谈、订货、在线付(收)款、开据电子发票以至电子报关、电子纳税等都在因特网上完成，因而它们的安全显得至关重要。因此，对网络的质量，特别是网络的安全要求就更高。但数据安全的核心是对要保密的数据进行有效加密。因此，数据加密技术是电子商务安全的关键技术。

1.2 电子商务的数据加密技术

过去数据加密技术主要应用于军事通信领域，现已转向民用。数据加密技术结合了数学、通信技术和计算机科学等学科，是一门交叉学科。数据加密通过对原来为明文的文件或数据按某种算法进行处理成为不可读的一段代码，通常称为“密文”。密文只能在输入相应的密钥之后才显示原文，以此达到保护数据的目的。加密技术的逆过程叫解密，如果加密技术能使解密成本(包含时间成本)大于解密后获得的利益，加密技术就是成功的。

一个安全加密算法还应当同时具备以下几个条件：提供高质量的数据保护，防止数据未经授权的泄露和未被察觉的修改；具有相当高的复杂性，使得破译的开销超过可能获得的利益；密码体制的安全性应该不依赖于算法的保密，即算法可以公开，其安全性仅以加密密钥的保密为基础；经济、运行有效，便于理解和掌握；能够适用于多种完全不同的应用领域。

2 数据加密技术的主要算法

加密算法主要可分为对称式加密算法和非对称式加密算法[5]。对称式加密算法即是加密、解密都使用相同的密钥，它通常称之为单钥密码算法、对称式密钥算法、秘密密钥密码算法等。非对称加密算法就是加密解密使用不同的密钥，也称双钥密码算法、非对称密钥算法、公开密钥密码算法等。

除此之外，也常常使用某种信息函数作为辅助的加密算法提高密度，或同时使用对称和非对称算法，如美国的SSL3.0电子证书，就同时使用对称和非对称两种加密方法。非对称式的加密密钥称为公钥，用于解密的密钥称为私钥。加密密钥和解密密钥两者互不相同，但都是对方的解密密钥，从其中的一个推导不出另一个。加密密钥和解密密钥配对使用才能打开加密文件。密钥为随机产生。因此，公钥可以对外公布，而私钥则只能由持有人知道。例如，假设用户甲想要和用户乙进行商务活动，则用户甲先在服务器申请，服务器随机选择一个对话密钥，并生成一个标签，这个标签由服务器和用户乙之间的密钥进行加密，并设法交给用户乙。只有用户乙收到后才能使用用户乙和服务器知道的密钥进行解密，所以能保障甲乙通信的安全。如果这个会话密钥是一次性的，这样破解的概率就很小。

2.1 非对称加密算法

非对称密钥的典型算法有：RSA，ECC，DSA，ElGamal，Diffie-Hellman(DH)密钥交换算法等，它常用于数据加密、密钥分发、数字签名、身份认证、信息的完整性认证、信息的非否认性认证。它们当中可以用于数据加密的算法有：RSA，ECC，ElGamal；可以用于密钥分发的算法有：RSA，ECC，DH；用于数字签名、身份认证、信息的完整性认证、信息的非否认性认证的有：RSA，ECC，DSA，ElGamal。

本文以RSA算法为例来说明非对称加密算法的步骤。

步骤1 设有3个整数 p,q,r，其中 p,q 是2个不同的素数，r 是与 $(p-1)(q-1)$ 互质的数，p,q,r 这三个数便是私钥。

步骤2 因为 r 与 $(p-1)(q-1)$ 互质，利用辗转相除法求可出 m，使得 $rm==1 \bmod (p-1)(q-1)$。

步骤3 计算合数 n，使 $n=pq$，这样 m,n 这2个数便可设成为公钥。

步骤4 进行编码。过程是，若加密的资料为 a，使其加密后变成 b。先将 a 看成是一个大整数，假设 $a<n$；如果 $a\geqslant n$ 的话，就将 a 处理成 s 进位($s\leqslant n$)，则每一位数均小于 n；然后分段编码，接下来计算 $b==a\hat{}\ m \bmod n$，$(0\leqslant b<n)$，b 就是编码后的资料。

解码的过程通常先计算 c，使 $c==b\hat{}\ r \bmod pq$ $(0\leqslant c<pq)$ 即可。

攻击者如要非法解密，首先需得到几个数：$m,n(=pq),b$，即使这样，也必须设法对 n 作质因数分

解，得到 r，这大大增加了破解的难度。

理论上从一个公钥中通过一些算法可以得到私钥，如因数分解，只要使用 2 个足够大的素数 p 与 q，但这个运算所包含的计算量就非常巨大，使得现实上非法解密是不可行的。但技术上这么做的同时使得加密算法本身也很慢，加上分组长度太大，难以做到一次一密。为保证安全性，n 至少也要 600bits 以上，这使得使用 RSA 算法来加密大量的数据变得很困难。但即使这样，由于 RSA 算法是第一个既能用于数据加密也能用于数字签名，且易于理解和操作，目前仍是使用较为广泛的加密算法。

2.2 对称加密算法

对称密码算法的加密密钥和解密密钥相同，由其中一个很容易推导出另一个，其优点是速度快。根据加密模式又可分为分组密码和序列密码。分组密码的典型算法有：DES，3DES，IDEA，AES，SKIPJACK，Karn，RC2 和 RC5，目前它是商业领域使用较多的密码算法，广泛用于信息的保密传输和加密存储。序列密码的典型算法有：RC4，SEAL，A5，它多用于流式数据的加密，特别是对实时性要求比较高的语音和视频流的加密传输。

DES 算法的基本思路是，把 64 位的明文输入块变为 64 位的密文输出块，使用的密钥也为 64 位。加密前先把输入的 64 位数据块按位重新组合，并把输出分为 $L0$、$R0$ 两部分，每部分各长 32 位，利用置换规则加密。

例如，对下面的数组进行加密：

(58,50,12,34,26,18,10,2,60,52,44,36,28,20,12,4, 62,54,46,38,30,22,14,6,64,56,48,40,32,24,16,8,57,49,41,33,25,17,9,1,59,51,43,35,27,19,11,3,61,53,45,37,29,21,13,5,63,55,47,39,31,23,15,7).

其加密步骤是，先将输入的第 58 位换到第一位，第 50 位换到第 2 位，...，依此类推，最后一位是原来的第 7 位。$L0$、$R0$ 则是换位输出后的两部分，$L0$ 是输出的左 32 位，$R0$ 是右 32 位，经过 16 次迭代运算后，得到 $L16$、$R16$，将此作为输入，进行逆置换，即得到密文输出。逆置换正好是初始置换的逆运算，例如，第 1 位经过初始置换后，处于第 40 位，而通过逆置换，又将第 40 位换回到第 1 位等等。

3 数据加密算法的研究进展

(1)采用摘要函数。摘要是一种防止改动的方法，其使用的函数称为摘要函数。这些函数的输入可以是任意大小的字符，而输出是一个固定长度的摘要。摘要有一个重要特性：如果改变了输入字符中的任何东西，甚至只有一位，输出的摘要都有影响。

(2)多步加密法。它使用一系列的数字(比如说 128 位密钥，一次使用 256 个表项)，来产生一个可重复的但高度随机化的伪随机的数字的序列。使用随机数序列来产生密码转表，用这个程序来加密一个文件，破解这个文件可能会需要非常巨大的时间以至于在现实上难于实现。

(3)插入校验码。循环冗余校验是一种典型的校验数据的方法。对于每一个数据块，它使用位循环移位和 XOR 操作来产生一个 16 位或 32 位的校验和，这使得丢失一位或两位的错误一定会导致校验和出错。

(4)生物识别技术。密码技术，特别是公钥密码技术的快速发展给网络信息的交换开拓了众多崭新的领域，最近约 10a 时间，基于 PKI(公钥基础设施)的商业和专用的网络系统在全世界范围内不断涌现。各种密码体制和密码算法的成熟和完善，为信息的安全传输提供了很多有效的解决方案。特别注意的是，近年来许多企业已经采用生物识别技术来保证他们的无线和远程网络的安全识别。生物识别是指通过对诸如指纹、声音或虹膜图案之类生物特征的测定来进行身份认证。某些生物具有复杂的、相异的特征，如指纹分析系统，通常能抓住 40～60 个个体特征，而新发明的虹膜测定技术识别的误差率只有 1/121 万。利用虹膜测定技术可以捕捉虹膜上超过 250 个与其他虹膜相异的特征。用 200 个样本做实例，虹膜识别系统创造了判断无错的记录，可以认为虹膜测定技术可以发展为最有效的身份识别技术。

参考文献：

[1] 尹 洁，贾林蓉. 浅谈企业与电子商务[J]. 西昌农业高等专科学校学报，2004，18(4)：43-45.

[2] 安继芳，孙建华. 密码技术与电子商务[J]. 网络安全技术与应用，2005，(2)：10-11.

[3] 肖 玎，刘建成. 一种电子商务的设计与实现[J]. 企业技术开发，2005，24(1)：27-29.

[4] 段 钢. 加密与解密[M]. 北京：电子工业出版社出版，2003.6.

[5] 钱树明，吴 灏. 密码算法[J]. 计算机与信息技术，2004，9：8.

(责任编辑：黎贞崇)