文章编号:1673-1549(2010)05-0562-04

非对称加密技术研究

卓先德,赵 菲,曾德明

(泸州职业技术学院信息工程系,四川 泸州 646005)

摘 要:随着网络技术的飞速发展,数据加密让信息变得安全,文章通过非对称加密算法的研究希望提高网络信息的安全性,降低网络传播中的风险。采用理论结合实际的分析方法,首先在介绍密码学基本概念的基础上,然后论述和分析了非对称加密的特性和不足,最后通过具体的案例介绍非对称加密技术在少量数据加密和混合加密体系的应用,证明其现实意义。

关键词:数据加密;非对称加密;混合加密

中图分类号:TQ423.3 文献标识码:A

引 言

随着计算机网络的发展,尤其是 Internet的广泛使用,信息安全问题日益突出和复杂。网络安全面临着计算机病毒、黑客入侵、机密文件泄露、DOS(拒绝服务攻击)和 DDOS(分布式拒绝服务攻击)等诸多威胁。因而,保证数据的保密性和完整性以防止非法获悉数据内容和非法修改数据成为信息安全的两大主要内容。

数据加密作为一项基本技术是所有通信安全的基石,是保证信息安全的主要方法,是数据安全技术的核心。非对称加密技术使用不同的密钥进行加密和解密操作,不同于对称加密,在非对称加密中,加密密钥仅用于加密而对解密完全无用;解密密钥仅用于解密而对加密无用。密钥分离的特点决定了非对称加密技术适用于对 Internet等分布式系统中传输的数据加密。

1 密码技术概况

密码技术作为信息安全的核心技术,主要包括两个分支:密码编码学和密码分析学。密码编码学主要研究对信息进行编码以实现信息隐藏,从而保护信息在传输的过程中不被窃取、解读和利用,实现信息的保密和认证。密码分析学是研究破译密文的科学与技术,主要研究如何分析和破译密码。这两个分支既相互对立又相互促进,推动了密码学的发展[1]。

根据加密与解密算法中使用的密钥是否相同,密码体制可以分为对称密码体制和非对称密码体制。在对称密码体制中,加密密钥和解密密钥是一样的或彼此之间容易相互确定,因此对称密码体制的安全性主要取决于密钥的安全性。非对称密钥密码体制,又称为双钥或公钥密码体制。在非对称密钥密码体制中,加密密钥不同于解密密钥,加密密钥公之于众,谁都可以使用。解密密钥只有解密人自己知道,分别称为公开密钥和秘密密钥[2]。

对称密钥技术由于其自身的局限性,无法提供数字签名的功能。数字签名是网络应用中表征人或机构的真实性、唯一性和私有性的重要手段,而对称密钥技术中的密钥至少需要在交互双方之间共享,不满足惟一性、私有性,无法用于实现数字签名。相比之下,公钥密码技术由于存在一对公钥和私钥,私钥可以表征惟一性和私有性,而且经私钥加密的数据只能用与之对应的公钥来验证,其他人无法仿冒,因此广泛用于实现网络中的数字签名服务。另外,公钥密码体制的一个重要优点就是易于建立两个相距遥远的终端用户间的密钥信道,而不需要他们彼此见面或者使用在线认证服务,这正好克服了传统对称技术的缺点。

收稿日期:2010-03-22

作者简介:卓先德(1972-),男,四川叙永人,讲师,硕士,主要从事校园信息化建设,信息安全技术方面的研究。

2 非对称算法

1976年, 著名学者 Diffie和 Hellman"密码学新方向"的发表, 奠定了公钥密码学的基础; Diffie和 Hellman描述了几个可能用来实现公钥密码的数学变换, 称之为单向陷门函数, 简单地理解即是从 x计算 y= f(x)是容易的, 而从 y计算出 x是困难的, 单向陷门函数的概念使得公钥密码系统成为可能[3]。随着计算机网络的发展, 信息保密性要求的日益提高, 公钥密码算法体现出了对称密钥加密算法不可替代的优越性。近年来, 公钥密码加密体制与 PKI数字签名和电子商务等技术相结合, 保证网上数据传输的机密性、完整性、有效性和不可否认性, 在网络安全及信息安全方面发挥了巨大的作用[4]。

2.1 非对称算法特性

该加密方式在信息的加密与解密中, 使用"公开密钥"与"私有密钥"对, 这个密钥对由解密者 (即信息的接收者)做成, "公开密钥"作为对信息进行加密的密钥, 对发送者发布, 同时接收者保管好解密所需要的"私有密钥"。在这里, 利用公开密钥加密的信息只能通过私有密钥解密, 但不能根据公开密钥推测私有密钥, 所以可以在经由第三者的环境中发布公开密钥。如果用户 A要给用户 B传送秘密信息 m, 则 A首先应从公开钥本上查到 B的公开钥, 并形成 B的加密算法 EB, 用 EB对明文 m加密编码, 得到密文: C= EB(m), 再将 C发送给 B; 用户 B在接收到密文 C后, 就可以用自己的密钥所确定的解密算法 DB来恢复明文: m= DB(C) = DB(EB(m)), 这就是一般公开密钥密码系统的加密、解密过程。

由此可见, 一方面, 公开密钥密码系统使得任何人都可用其他用户 U公开的加密密钥 K给该用户发送经公开加密算法 Ek加密的信息, 而不必事先分配和保管传统密码系统所需的大量密钥; 另一方面, 当加密、解密变换可交换时, 即 EkDk= DkEk, 由于仅由用户 U自己才具有唯一的一个解密密钥 K, 对某一有意义的信息, 经过用户 U的解密算法 Dk变换后的结果, 就可以由用户 U公开的加密算法 Ek变换以恢复原来的信息。而用不同于 Dk的解密算法对原信息作变换后的结果, 经用户 E的加密算法 Ek变换后均不能产生有意义的信息。在此情况下, 该公开密码系统就给用户 U提供了对信息进行签名和身份验证的功能。

2.2 非对称算法优势和缺陷

公钥密码体制采用的加密密钥 (公开钥)和解密密钥 (秘密钥)是不同的。由于加密密钥是公开的, 密钥的分配和管理就很简单, 而且能够很容易地实现数字签名, 因此最适合于电子商务应用的需要。其主要的优点是[4]:

(1)密钥分配简单。

(2)密钥的保存量少。

(3)可以满足互不相识的人之间进行私人谈话时的保密性要求。

(4)可以完成数字签名和数字鉴别。

但在实际应用中, 公钥密码体制并没有完全取代私钥密码体制, 这是因为公钥密码体制在应用中存在以下几个缺点:

(1)公钥密码是对大数进行操作, 计算量特别浩大, 速度远比不上私钥密码体制[5]。

(2)公钥密码中要将相当一部分密码信息予以公布, 势必对系统产生影响。

(3)在公钥密码中, 若公钥文件被更改, 则公钥被攻破。

3 非对称加密算法的运用

非对称加密技术是为解决信息公开传送和密钥管理问题而提的出一种加密技术。它允许在类似 Internet这样不安全的媒体上的通讯双方交换信息, 安全地达成一致的密钥, 保证信息传送的安全性。由于非对称加密算法要求较复杂的数学运算, 所以更适合针对少量数据加密。对于大量数据, 单独使用公钥密码加密开销极大, 因此通常使用公约密码对对称密钥进行加密, 而用对称密钥来加密数据。

3.1 非对称算法在手机短信安全中的运用

手机短消息已经成为人们一种不可或缺的通信方式, 随着短信息业务向移动支付、移动证券交易等金融领域的扩展, 传统的短信息的文本传递方式已经不能满足业务发展的需要, 尤其对短信息的安全性提出了更高的要求[6]。

为了确保短信息传输的安全性, 对短信可以采用加密技术。可以采用基于 RSA算法的现代密码技术加密短信, 这样可以提高短信的安全性。这个技术运行时, 首先生成一对密钥, 在手机发送端和接收端分别对短信息数据进行安全性处理。手机发送端发送的是密文, 而发送端发送的是短信息明文; 与之相反, 接收端信息服

务中心发送的是加密后的密文信息，被呼叫手机进行相同解密后得到的是发送端发送的明文信息。

具体的实现过程是：首先，在手机发送端，用户编辑好要发送的短信息文本信息，为保证短信息在传输中的安全性，在手机里对用户发送的短信息文本数据进行加密，同时，将公钥，私钥附加到信息头部一并发送；接着接收端从服务中心获得解密密钥然后按照 RSA算法进行解密，密文被还原成明文；接着接收端网关检测目标用户的 VLR，然后将明文短信息通过网络运营商内部网络传输到对方的地址，在双方的地址之间传输的短信息是明文传输的。他们在传递过程中，利用 VLR中的路由器发送短信息至目标用户手机。目标用户手机接收到本地传输的短信息密文后，按照源信息地址中的工作流程对短信息密文进行解密，恢复得到源地址手机发送的短信息原文。

这种加密技术增强了短信息服务的安全性，能够加强使用短信息进行大额付款和其他移动电子商务的实用性，因而受到很多客户的喜爱。

3.2 非对称算法在视频会议中的运用

对于视频方面，视频会议变得越来越普遍，对于信息的外泄，成为视频会议的重要安全问题。视频会议一般是企业、公司和国家等内部人员进行的重要的沟通和联络，里面涉及很多的机密，因而不允许无关人员擅自闯入会议之中，也不能让数据资料复制或进行破坏，造成不该有的损失。加上视频会议系统在国防机构、企业和政府机构的运行，会议内容会涉及到更多的国家机密、军事情报和商业秘密等重要信息，因此，视频会议的安全保密就显得至关重要。

运用现代密码学可以实现对视频会议的加密，运用基于 DES算法和 RSA算法组成的混合加密算法体系加密[7]，应用在视频会议系统。该混合密码体系采用公开密钥密码保护和分发会话密钥，这些会话密钥用在对称算法中，采用对称算法对通信消息进行保密。安全子系统的加、解密过程如图 1所示，其中视频会议传输中的多点控制单元（MCU)处理如图 2所示：

视频会议系统的子系统对整个安全保密系统可以统计通过加密解密算法独立实现。原始数据使用测试数据单独处理，采用多点控制单元（MCU)中的 RSA密钥处理器设计与实现，这主要是由于传输信道使用公用信道，无法加密处理，只能对传输数据进行加密管理，在信道与终端之间采用专用芯片加、解密数据，同时传送、

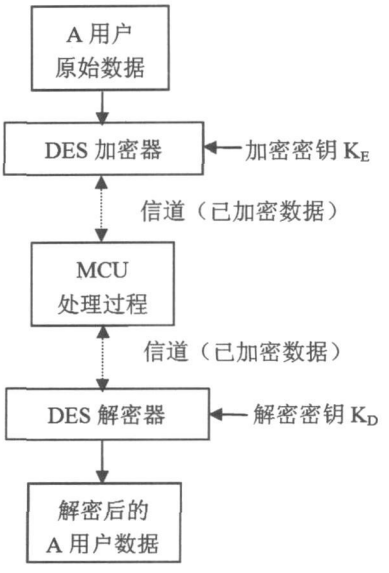

图 1 安全子系统加密解密过程

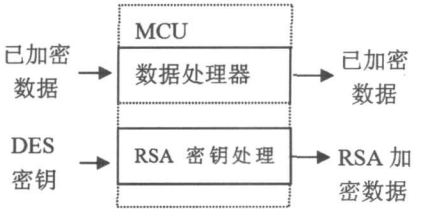

图 2 MCU 处理过程

接收密钥，MCU中的 RSA密钥处理器对接收到的 DES密钥进行识别、处理，从而实现整个保密子系统。

通过混合加密算法的运用，采用专用芯片对数据流进行加、解密处理，从而极大提高了加、解密处理速度，减少整个系统的运算处理时间。这个加密系统确保了视频会议的安全，操作方便，因此可以广泛运用到现在的视频会议中。

4 结束语

非对称算法是现代密码学中最重要的研究内容之一，它不但能为在网络中传递的信息提供机密性的保护，而且还能提供信息的发送人的身份认证以及信息的完整性检查。本文重点分析了非对称算法的特点和优缺点，通过这些分析，可以清楚的了解非对称算法，并且通过手机加密和视频会议加密验证了非对称加密算法运用的安全性。随着对非对称加密技术的不断研究和科技的不断延伸，非对称加密算法会得到更加广泛的运用。

（下转第 569页）

gy-Based Information Retrieval Model[C]. The Semantic Web: Research and Applications, Second European Semantic Web Conference, 2005, 3532: 455-470.

[7] 王成敏. 基于规则的汉语名词短语自动识别方法研究[J]. 四川理工学院学报:自然科学版, 2009, 22(2): 55-57.

Research on the Improve Model of MO_CRM

XIA Lei, HE Min

(1. Department of Computer Science, Chengdu Neusoft Institute of Information Technology, Chengdu 611844, China)

Abstract: For users on internet used to search information by several simple words, we try to satisfy them by expanding those words. We build the MO_CRM by combine the mutual information and ontology. But as deep research into the model, we improve the way of revise and complementary of the domain ontology and get the MO_CRM. As a result, a higher chance of recall and precision by MO_CRM is obtained.

Key words: domain ontology; mutual information; reference ontology; collaboration

---

(上接第 564页)

参 考 文 献:

[1] 冯登国. 国内外密码学研究现状与发展趋势[J]. 通信学报, 2002, 23(5): 18-26.

[2] 于学江. 对称密码体制及其算法研究[J]. 齐齐哈尔大学学报, 2007, 23(6): 38-40.

[3] 吴昌银, 岳青松. AES安全性及其影响研究[J]. 信息安全与通信保密, 2006, 32(11): 77-79.

[4] 胡向东. 应用密码学[M]. 北京: 电子工业出版社, 2006.

[5] 谢 扬, 王金凤. 浅谈公钥密码体制[J]. 计算机科学, 2008, 35(4): 157-158.

[6] 张焕国, 冯秀涛. 演化密码与 DES密码的演化设计[J]. 通信学报, 2002, 23(5): 29-32.

[7] 王宏杰. RSA算法、DES算法的特点分析及结合[J]. 天津科技, 2005, 19(4): 65-69.

Research of Asymmetric Encryption Technology

ZHOU Xian-de, ZHAO Fei, ZENG De-ming

(Department of Information Engineering, Luzhou Vocational and Technical College, Luzhou 646005, China)

Abstract: With the rapid development of network technology, data encryption makes information safe. This paper, asymmetric encryption algorithm is studied to improve the security of network information, reducing the risk of cyber communications. The paper firstly introduced the basic concepts of cryptography, then discussed and analyzed the characteristics of asymmetric encryption and weaknesses, finally with the introduction of specific cases by non-symmetric encryption data used in encryption and hybrid encryption system showed that this research can be more convincing and realistic significance.

Key words: data encryption; non-symmetric encryption; Hybrid Encryption