

用数字签名解决电力系统敏感文档签名问题

胡 炎¹, 董名垂²

(1. 清华大学电机系, 北京市 100084; 2. 澳门电脑与系统工程研究所, 澳门)

摘要: 目前电力系统中普遍采用 MIS 实现办公自动化, 完成文档的生成、确认、签发、传递、存档等工作。当前的 MIS 都是采用简单的用户名/口令机制实现对用户的身份认证, 不能提供实质上的安全签名服务。采用基于公钥密码算法的数字签名可以充当个人在网络空间“身份证”的角色, 能够很好地解决目前 MIS 存在的敏感文档签名问题。文中介绍了密码算法的基本原理, 给出了数字签名的解决方案。

关键词: 数字签名; 密码算法; 数字证书; 管理信息系统; 电力系统

中图分类号: TM73; TN918.4

0 引言

电力系统的日常运行维护涉及大量文档在电力系统各部门之间传递, 通过文档传递实现各部门分工协调合作, 共同维护电力系统的安全、经济、高效运行。这些文档包括变电操作票、第 1 种和第 2 种工作票、设备变更记录、调度操作票等, 它们在传递的流程中需要经过不同部门确认签发。为了提高工作效率, 目前电力系统中普遍采用管理信息系统 (MIS) 实现办公自动化, 完成文档的生成、确认、签发、传递、存档等工作, 其中不可避免地涉及到敏感文档的签名问题。文档签名要求把被签发的文档与签发人联系起来, 以明确责任分工。但是, 当前的 MIS 都是采用简单的用户名/口令机制实现对用户的身份认证, 进而控制文档的确认签发, 不能提供实质上的安全签名服务^[1], 更不用说其他安全服务如数据保密、完整性检查和抗否认等。本文采用基于公钥密码算法的数字签名可以充当个人在网络空间“身份证”的角色, 能够很好地解决目前 MIS 存在的敏感文档签名问题。

1 目前的解决方案及存在的缺陷

目前 MIS 文档传递的方式如图 1 所示。系统的安全性完全取决于用户名/口令认证机制的安全性。这种机制的缺陷在于: ①用户名和口令在不安全网络环境下传输, 容易被监听、窃取。②没有解决文档的电子签名问题, 需要签名时必须把文档打印出来。因为文档的传递由各部门负责人签发, 这样难以实现无纸化办公, 只能是半自动化的辅助办公。③文档

在不安全网络环境下明文传输, 可能被篡改, 敏感信息可能被窃取。④难以实现完备的电子存档(包括签名), 进而实现卷宗管理(某项工作在其流程中所涉及的所有文档的总和称为一个卷宗)。

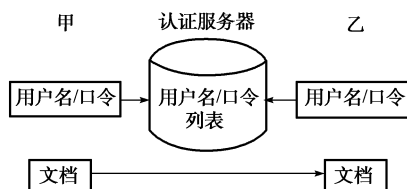


图 1 目前 MIS 文档传递的方式

Fig. 1 Delivery mode of documents in current MIS

2 密码算法与数字签名

2.1 密码算法

要理解数字签名的基本原理, 就不能不先介绍密码算法。密码算法有 3 类^[2]。

a. 共享密钥算法(shared-key cryptography): 又称对称密钥算法, 加密和解密过程共享同一个密钥, 如 DES 算法。

b. 公钥算法(public-key cryptography): 又称非对称密钥算法, 加密密钥和解密密钥不是同一个密钥, 而且几乎不可能从已知的一个密钥推导出另一个密钥, 如 RSA 算法。

c. 单向散列函数(one-way hash function): 严格地说, 它并不是一种密码算法, 但是和公钥体制密切相关。本质上它是一种数学变换函数, 把可变长度输入串变换为一定长度的输出串, 而且此过程不可逆, 如 MD5 算法。

3 种密码算法可以形象地表示成图 2 所示。

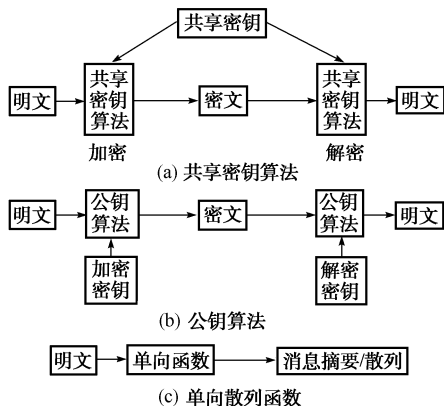


图 2 3 种密码算法

Fig. 2 Three types of cryptographic algorithms

2.2 数字签名

公钥算法有一对密钥,一个公开于世,称为“公钥”(public key),另一个不告诉任何人,称为“私钥”(secret key or private key)。这 2 个密钥是互补的,就是说用公钥加密的密文可以用私钥解密,反过来也一样。假设甲要传递文档给乙,他们互相拥有对方的公钥。甲用乙的公钥加密文档后递出,乙收到后就可以用自己的私钥解密得到甲的原文。由于没有别人知道乙的私钥,所以即使是甲本人也无法解密那份文档,这就解决了文档保密的问题。另一方面由于每个人都知道乙的公钥,他们都可以给乙传递文档,因而乙就无法确定是否是甲递出的文档,这时就需要数字签名了。

数字签名(digital signature)是一个用某人的私钥加密的消息摘要(message digest),用于确认消息的来源和内容。这种用私钥对消息摘要加密的过程称为签名。简单地讲,就是对文档用某种单向散列函数算出一个最能体现该文档特征的数来,文档的任何修改都能够体现为该特征数的变化,那么这个数加上作者的名字、日期等,再用作者的私钥加密就可以作为该作者对这份文档的数字签名了。

3 数字签名的安全性

数字签名的安全性决定于公钥算法和单向散列函数的安全性,而它们的安全性是由其数学原理保证的。

3.1 公钥算法的数学原理

公钥算法的主要特征在于使用一对密钥——加密密钥和解密密钥,而且从解密密钥推出加密密钥是不可行的。下面以 RSA 算法为例说明公钥算法的数学原理。

为了产生 2 个密钥,选取 2 个大素数 p 和 q ,计算乘积 $n = pq$ 。然后随机选取加密密钥 e ,使 e 和

$(p-1)(q-1)$ 互素。最后用欧几里德扩展算法^[1]计算解密密钥 d ,以满足

$$ed = 1 \bmod [(p-1)(q-1)]$$

可以证明 d 和 n 也是互素的,则 e 和 n 是公开密钥, d 是私人密钥。2 个素数 p 和 q 不再需要,但绝不可泄漏。RSA 算法可以简化为表 1,其中 m 为待加密的消息, c 为用 RSA 算法加密消息 m 后得到的密文。

表 1 RSA 算法
Table 1 RSA algorithm

公开密钥	n : 2 个大素数 p 和 q 的乘积(p 和 q 必须保密) e : 与 $(p-1)(q-1)$ 互素
私人密钥	$d: e^{-1} \bmod ((p-1)(q-1))$
加密过程	$c = m^e \bmod n$
解密过程	$m = c^d \bmod n$

由于 e 和 n 必须公开,如果通过分解 n 得到 p 和 q ,就可以利用欧几里德扩展算法从公开密钥 e 计算出私人密钥 d ,所以 RSA 算法的安全强度等价于对 n 进行质因数分解的难度。目前在数论中,对大数进行质因数分解尚没有有效的算法,因此只要选择足够大的 p 和 q ,RSA 算法的安全性是可信的。但是在数学上从未证明过必须分解 n 才能从 c 和 e 计算出 m 。当然也可以通过猜测 $(p-1)(q-1)$ 的值来攻击 RSA,但这种攻击没有分解 n 容易^[3]。密码分析者仍有可能尝试采用其他的方法绕过大数质因数分解的困难去破解 RSA 算法,然而目前在密码学领域,RSA 算法被公认为是非常安全的。

3.2 单向散列函数的数学原理

在密码学中,需要进行数字签名的文档被称为消息,而由单向散列函数计算出的文档特征值被称为散列值。

单向散列函数是建立在压缩函数的基础上的。给定长度为 m 的输入,压缩函数输出长度为 n 的散列值。压缩函数的输入是消息当前分组和消息前一分组的输出。压缩函数的输出是消息从第 1 个到当前分组的散列值,即分组 M_i 的散列值为:

$$h_i = f(M_i, h_{i-1})$$

该散列值和下一轮的消息分组在一起,作为压缩函数下一轮的输入。最后一个消息分组的散列值就是整个消息的散列值。

单向散列函数有多种实现算法,目前较为实用的算法有 MD5 和 SHA 等^[4]。一个有效的单向散列函数 $h = H(M)$ 在数学上必须满足 2 个条件。

a. 单向性。即该函数必须具有如下 3 个特征:
① 给定消息 M ,很容易计算散列值 h 。② 给定 h ,由

$h=H(M)$ 很难计算 M 。③给定 M ，很难找到另一个消息 M' 并满足 $H(M)=H(M')$ 。

b. 抗碰撞性。即要找出 2 个随机的消息 M 和 M' ，满足 $H(M)=H(M')$ 很难。

由于单向散列函数在数学上必须满足以上 2 个条件，保证了任何对文档的修改都可以体现为该文档散列值的变化，所以把文档作为单向散列函数的输入而得到的散列值可以作为该文档的特征值。

4 基于数字签名的解决方案

基于数字签名的解决方案首先需要解决公钥在不安全网络环境中分发的问题。目前的解决方法是用证书认证中心(certification authority, 简称为 CA 中心)签发的数字证书存储公钥，公钥随着数字证书的发行而分发。

4.1 数字证书

公钥算法的提出是为了解决传统加密体制中公钥分配过程保密难的缺点。对公钥而言本来就是要公开的，没有防监听和泄漏的问题，但是公钥的发布仍然存在安全性问题，例如公钥被篡改(public-key tampering)。必须确信拿到的公钥确实属于它声明的那个人，否则就会受到中间人的攻击，攻击过程见图 3 所示。其中，“消息(公钥)”表示用公钥加密的消息。

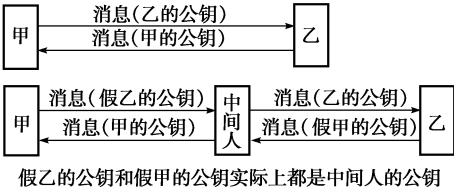


图 3 中间人攻击甲乙通信示例

Fig. 3 The middle attacks communication between A and B

防止这种情况出现的方法显然是通过信任渠道得到公钥。记住我们最初的目标是要在不安全网络环境下安全地传递敏感文档，通过对文档数字签名将问题转换为如何在不安全网络环境下传递公钥。在实际运作时，通信双方需要信任一个 CA 中心，它负责管理证书的发布。数字证书包含许多信息，其中最重要的就是公钥、有效期、证书申请人和 CA 中心的签名。通信双方都拥有 CA 中心的公钥(存储在 CA 中心自身的数字证书中)，通过信任 CA 中心的公钥，进而信任由 CA 中心签发的通信双方数字证书中存储的公钥。可见通信双方公钥传递的安全性也是用数字签名的方法解决的。通过引入 CA 中心，又进一步把问题转换为如何在不安全网络环境下传

递 CA 中心的公钥。到了这里问题就可以解决了，CA 中心广泛提供证书服务，假冒它的公钥和数字证书是极其困难的，而且很容易被发现。这样大家就普遍信任 CA 中心的公钥，从而信任所有由该 CA 中心签发的通信各方的公钥。这种信任关系可以用图 4 形象地表达出来。

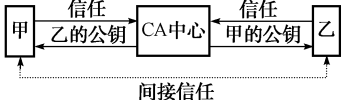


图 4 甲乙通过 CA 建立信任关系

Fig. 4 A and B trust with each other through CA

4.2 解决方案

以甲向乙传递文档为例说明采用数字签名后文档的传递过程(如图 5 所示)。

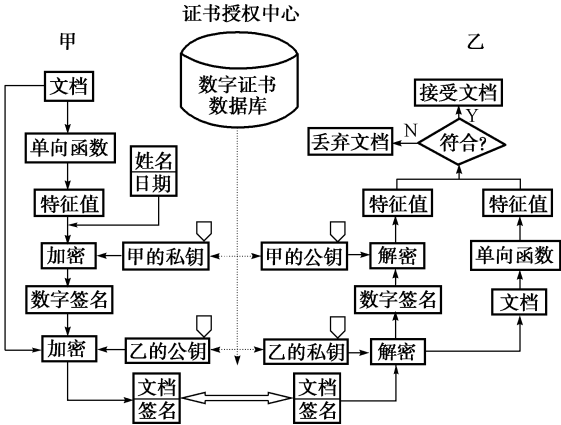


图 5 采用数字签名后的文档传递方案

Fig. 5 Delivery mode of documents with digital signatures

甲用自己的私钥将文档的特征数及其他相关信息加密(即为甲的数字签名)附在文档后，再用乙的公钥将整个文档加密(注意这里的次序，如果先加密再签名的话，别人可以将签名去掉后附上自己的签名，从而可以篡改签名)。这样当这份密文被乙收到以后，乙用自己的私钥将文档解密，得到甲的原文和签名，乙用同样的单向散列函数从原文计算出一个特征数并与用甲的公钥解密签名所得到的数比较，如果符合就说明这份文档确实是甲寄来的。这个过程满足 4 个方面的安全性要求：①认证性：乙用甲的公钥解密甲的签名，同时就认证了该签名的文档是甲递出的。②保密性：经过签名的文档是用乙的公钥加密的，由于没有别人知道乙的私钥，所以只有乙能够对这份密文解密，从而满足保密性。③抗否认：由于没有别人拥有甲的私钥，只有甲能够生成可以用甲的公钥解密的签名，所以甲不能否认曾经对该文档进行过签名。④完整性：由于文档的任何改变都可

由单向散列函数得到与原文不同的特征值,因此可以验证该文档在被甲递出后和被乙接收的期间是否曾被篡改,从而满足提供完整性检查的要求。

当然,有时文档不需要保密,这时可以用乙的公钥仅仅对甲的签名加密,仍然可以满足认证性、完整性和抗否认的要求。

5 方案评价与结论

为了避免目前 MIS 采用简单的用户名/口令机制控制文档传递的缺点,本文提出利用基于公钥算法的数字签名对文档进行电子签名,从而大大增强了文档在不安全网络环境下传递的安全性,签名和文档可以同时存档,有利于实现完备的电子存档和卷宗管理。该方案向用户提供了完整的安全服务^[5],包括身份认证、保密性、完整性检查、抗否认等。但是由于它基于公钥体制,所以还存在以下不足:①需要公钥基础设施(public key infrastructure)的支持。需要证书认证中心提供证书服务^[6],负责公钥的生成、分发、撤销等。②私钥虽然不需要在不安全网络环境下传递,不用担心被监听的危险,但是它仍然有泄漏的可能,因此私钥的存储也是整个安全体制的关键。为了降低对终端用户的要求,可以采用 IC 卡存储私钥,由证书认证中心统一发布。

尽管如此,采用数字签名后把文档传递的安全性转嫁为公钥体制的安全性,由公钥基础设施统一负责,这无论对提高目前分布式应用本身的安全性,

还是未来的扩展性或实现同其他应用的相互认证,都是非常有利的。

参 考 文 献

- 1 Ganley M J. Digital Signatures. Information Security Technical Report, 1997, 2(4): 12~22
- 2 余建斌(Yu Jianbin). 黑客的攻击手段及用户对策(Hacker's Attacking Art and User's Countermeasure). 北京:人民邮电出版社(Beijing: People's Posts & Telecommunications Publishing House), 1998
- 3 Wu C K, Wang X M. Determination of the True Value of the Euler Totient Function in the RSA Cryptosystem from a Set of Possibilities. Electronics Letters, 1993, 29(1): 84~85
- 4 Schneier B. 应用密码学: 协议、算法与 C 源程序 (Applied Cryptography: Protocols, Algorithms and Source Code in C). 吴世忠, 祝世雄, 张文政, 等译(Wu Shizhong, Zhu Shixiong, Zhang Wenzheng, et al Trans). 北京: 机械工业出版社(Beijing: China Machine Press), 2000
- 5 Leung K R P H, Hui L C K. Handling Signature Purposes in Workflow Systems. Journal of Systems and Software, 2001, 55(3): 245~259
- 6 Wright M A. A Look at Public Key Certificates. Network Security, 1998 (2): 10~13

胡 炎(1975—),男,博士研究生,研究方向为电力工业中的信息安全问题。E-mail: huyan99@mails.tsinghua.edu.cn

董名垂(1947—),男,澳门大学高级研究员,现任澳门电脑与系统工程研究所总工程师,研究方向为智能及系统集成技术。E-mail: dmc@sftw.umac.mo

SOLVING SIGNATURE PROBLEM OF SENSITIVE DOCUMENTS WITH DIGITAL SIGNATURE IN POWER SYSTEM

Hu Yan¹, Dong Mingchui²

(1. Tsinghua University, Beijing 100084, China)

(2. Computer and System Engineering Institute of Macau, Macau, China)

Abstract: Currently MIS has been widely applied in power system to realize office automation that includes creating, confirming, signing, delivering and archiving of documents. Now MIS generally identifies a user via a simple user/password mechanism, but is unable to supply secure signature services in essence. A digital signature based on public key algorithms is illustrated, which can be regarded as an identification card in cyberspace and can properly solve the signature problem of sensitive documents in power system. The principles of cryptographic algorithm are analysed, and the plan of solving signature problem of sensitive documents with digital signature is proposed in detail.

Key words: digital signature; cryptographic algorithm; digital certification; MIS; power systems