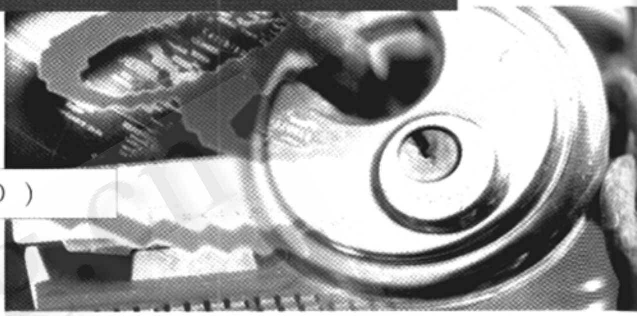
网络安全中的数字签名技术分析与应用



曾 孜 （广州广东工业大学计算机学院 510090）

随着社会、经济的高速发展，计算机技术已深入到社会的各个领域。INTERNET的迅猛发展及其需求的复杂化使得网络通信的安全问题越来越突出。网络信息的可靠性也同样令人担忧。特别是日益完善的电子商务系统中涉及到的信息传送、身份确认、签署文件等方面更要求真实性、机密性、不可否认性、可控性及服务的可用性。许多法律、财务以及其他文件的真实性和可靠性最终还是由授权的亲笔签名存在与否来确定，复印件是无效的。如果要用计算机化的报文代替纸墨文件的传送，就需要设计一个代替亲笔签名的方案。从根本上说，需要这样一个系统，一方通过该系统能以如下方式向另一方发送自己的签名文件：

（1）接收方能验证发送方所宣称的身份；

（2）发送方以后不能否认文件是他发送的；

（3）接收方自己不能伪造该文件。

因此，加密技术、数字签名技术、公钥证书架构三个主要的安全技术应运而生，利用这些技术能有效地实现上述多种要求。本文首先介绍了加密技术中的公开密钥加密体制和数字签名技术，并在此基础上研究了一对一安全通信方式以及多人签名的一种实现方法。

1 公开密钥加密技术

公开密钥加密技术，即非对称密钥技术，要求密钥成对使用，加密和解密分别由两个密钥来实现。每个用户都有一对选定的密钥，一个可以公开，即公开密钥，用于加密；另一个由用户私人拥有，即秘密密钥，用于解密。当给对方发送信息时，用对方的公开密钥进行加密，而接收方接收到信息后，则用自己的秘密密钥进行解密。目前，最为成功和安全的公开密钥加密体制是基于数论原理的RSA算法，该算法的安全性建立在难于对大数提取因子的基础上。

在公开密钥加密体制中，加密密钥PK（即公开密钥）是公开信息，而解密密钥SK（即私人密钥）是保密的。加密算法E和解密算法D都是公开的。虽然SK是由PK决定的，但却难以根据PK计算出SK。公开密钥算法的特点如下：

（1）用加密密钥PK对明文X加密后得到密文，用解密密钥SK对密文进行解密可恢复出明文，且加密和解密运算可以对换。即 $D_{SK}(E_{PK}(X))=X$，$E_{PK}(D_{SK}(X))=X$；

（2）加密密钥不能用来解密，即 $D_{PK}(E_{PK}(X))\neq X$；

（3）在计算上可以容易地产生成对的PK和SK；

（4）从已知的PK推导出SK在计算上极其困难。

2 数字签名技术

数字签名技术是建立在公开密钥加密体制的基础上的。根据数字签名标准DSS(Digital Signature standard)，数字签名的步骤一般如下：

步骤一：发送方用一个HASH函数对信息明文M进行处理，产生报文摘要MD（Message Digest）。任意长的信息经过HASH函数处理后，都能计算出固定长度比特序列的报文摘要MD，这种方法的特点是因为HASH函数具有以下属性：

（1）HASH函数的单向性。HASH函数的计算不可逆，既使知道了MD（M），也不能推出M；

（2）HASH 函数的免碰撞性：对不同的信息一定产生不同的报文摘要。即不存在信息P1和P2，P1 ≠ P2，而MD（P1）=MD（P2）；

（3）任意长的信息X，经过HASH函数处理后，都可以产生固定长度的HASH值。

步骤二：发送方用自己的私钥SK和报文摘要MD进行DSA算法（Digital Signature Algorithm）计算，产生数字签名X；

步骤三：将数字签名X和信息M一起发送出去；

步骤四：接收方接收到信息后，用同样的HASH函数对信息M进行计算，产生报文摘要；

步骤五：接收方用DSA算法对报文摘要和发送方的公开密钥进行计算，产生数字签名Y。同时，从接收到的信息中可以得到数字签名X。

若X=Y，则该数字签名得到验证；否则，数字签名验证失败，说明信息发出后可能被修改过或者是伪造的通信步骤如图1所示。

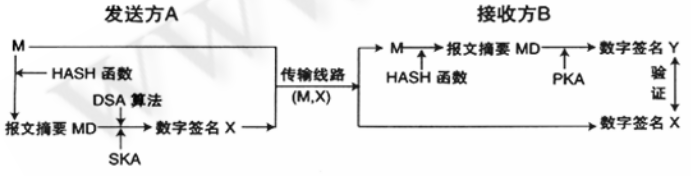


图 1

由以上讨论可知数字签名的基本功能是：(1)。能够保证数据的完整性。如果数据在传送过程中被修改过或者根本就是伪造的，则无法通过接收方的数字签名验证。(2)。具有不可抵赖性。发送方不能抵赖他曾发送了该信息，因为别人无法伪造他的数字签名，除非他的私人密钥被窃取。

3 数字签名在网络通信中的应用

根据DSS标准只实现了数字签名的基本功能，信息M的内容可能被任何知道信息发送者公开密钥的人阅读，信息不具备保密性，而且签名也只局限于一个人签名。在INTERNET上，可能经常需要有特定的一对一的安全通信，如两个企业领导之间的通信。随着网上交易的发展，多人签名也成为需求，例如经常需要几位领导同时签署一份合同或文件。在DSS标准和公开密钥加密体制的基础上，可以设计出一对一安全通信方式以及多人签名实现方法。

3.1 一对一安全通信方式

在一对一的安全通信方式中，发送方可以指定接收方，发出的信息只能被指定的接收方阅读。如果信息被截取，则截取者因没有解密密钥而无法解密该信息。令发送方为A，接收方为B，PKA和SKA分别是A的公开密钥和私人密钥，PKB和SKB分别为B的公开密钥和私人密钥，A发送的信息为M。实现步骤如下：

（1）对信息M进行函数处理得到报文摘要MD，A用DSA算法和自己的私钥SKA对MD进行计算，产生数字签名X；

（2）A用B的公开密钥PKB对（M+X）进行加密，产生E_{PKB}（M+X）；

（3）将E_{PKB}（M+X）发送给B；

（4）B接收到后，用他的私钥SKB对信息进行解密，即D_{SKB}（E_{PKB}（M+X））=M+X；

（5）B用DSA算法和A的公开密钥PKA对M进行计算，产生一个数字签名Y。

如果X=Y，则数字签名得到验证，否则，该信息被拒绝（通信步骤如图2所示）。

图 2

3.2 多人签名

以上的一对一通信方式在多数情况下，尤其是在电子商务中还不能满足需要，我们常常会遇到要求有多个人在同一份合同或文件上签名的情况。在一对一安全通信的基础上，多人签名则还要求签名顺序的组织。在此介绍一种多人签名的实现方法：每个签名者只验证前一个签名人的签名，如果验证通过就在此基础上加上自己的签名，否则终止签名。每个签名者都可以推算出前一位签名人和后一个签名人并且知道他们的公开密钥。最后一位签名者在签名完成后将最终信息和签名一起发送出去。

令发送方（按签名顺序）为A1、A2、A3 …… An，接收方为B，PKAi和SKAi分别为Ai的公开密钥和私人密钥，发送的信息为M。多人签名过程如下：

(1) A1用DSA算法和自己的密钥SKA1对M进行计算，产生数字签名X1，并用下一位签名者A2的公开密钥PKA2对（M+X1）进行加密，产生E_{PKA2}（M+X1）并发送给A2；

(2) A2接收后，用他的私人密钥SKA2对信息解密，产生D_{SKA2}（E_{PKA2}（M+X1））=M+X1，并用DSA算法和前一位签名者A1的公开密钥PKA1对前一位签名者的签名X1进行验证。如果前一位签名者的签名X1得不到验证，则签名过程终止。反之，继续下一步；

(3) A2将（M+X1）作为新的信息M2，用DSA算法和自己的私钥SKA2对M2进行计算产生新的签名X2，并用后一位签名者的公开密钥PKA3加密产生E_{PKA3}（M2+X2），发送给下一位签名者A3；

(4) A3接受后，按照步骤（2）~（3）处理。每个签名者如此依此顺序签名，直到最后一个签名者An签名完成，产生最终的签名Xn以及最终的信息Mn；

(5)最后，An用接收者B的公开密钥PKB对(Mn+Xn)进行加密，产生E_{PKB}（Mn+Xn）并发送给B。

多人签名的验证如下：

① B接收后，用他自己的私人密钥对信息解密，即D_{SKB}（E_{PKB}（Mn+Xn））=Mn+Xn；

② B用DSA算法和An的公开密钥PKAn对Mn进行计算，产生数字签名Yn；

③ 如果Xn ≠ Yn，则数字签名得不到验证，签名验证过程终止，信息被拒绝。反之，继续下一步；

④ 由产生多人签名的步骤（3）可知Mn=Mn-1+X n-1（但M2=M+X1），从中可以分离出M n-1和X n-1，按上述步骤可继续验证M n-1和X n-1，如此循环，直至验证到M和X1，如果X1验证通过，则整个签名验证成功。

4 在Outlook Express使用数字签名和邮件加密

在Outlook Express中撰写邮件，若要为邮件添加数字签名，在“工具”菜单中，单击“数字签名”；带数字签名的电子邮件允许电子邮件的收件人验证发件人的身份。若要加密邮件，则在“工具”菜单中，单击“加密”；加密电子邮件则可以防止其他人在邮件传递过程中偷阅邮件。

在使用Outlook Express发送带有数字签名的邮件之前，发送方必须先获得自己的数字ID；而要发送加密邮件，则在发送方的通信簿中必须包含收件人的数字ID。数字ID由独立的授权机构发放。在向授权机构的Web站点申请数字ID时，授权机构在发放标识之前有一个确认申请人身份的过程。数字ID由“公用密钥”、“私人密钥”和“数字签名”三部分组成。当发送方A向邮件添加数字签名时，就在邮件中加入了A的数字签名和公用密钥。收件人B可以使用邮件中的数字签名来验证A的身份，并可使用A的公用密钥向A发送加密邮件，这些邮件必须用A的私人密钥才能阅读。

进行数字签名校验时，Outlook Express会向相应的授权机构索取该数字ID的有关信息。授权机构发回该数字ID的状态信息，其中包括该标识是否已被撤销等。授权机构会监控由于遗失或终止等原因而被撤销的证书。

5 数字签名的优点

(1) 保证数据的完整性。如果数据在传送过程中被修改过或者根本就是伪造的，则无法通过接收方的数字签名验证。

(2) 具有身份识别功能。数字签名很容易就可以确定信息的发送方和接收方的身份，这一点对网上商务尤其重要。

(3) 数字签名通常采用加密技术，提高了信息的机密性。

(4) 具有不可抵赖性。发送方不能抵赖他曾发送了该信息，因为别人无法伪造他的数字签名，除非他的私人密钥被窃取。

(5) 对一个有多页的文件而言，传统签名难以确定签名的有效范围（是对整个文件还是对所签单页有效），也很难判断文件签名后是否被增加或删改过。而数字签名则彻底解决了这个问题。

(6) 数字签名可以提高交易的速度和准确性，能自动产生并包括一个时间戳，这对网上交易而言特别重要。

6 结束语

本文介绍了公开密钥体制，并在此基础上介绍了一对一安全通信方式和多人签名的实现方法。数字签名技术是实现网络环境下数据安全传输的重要手段之一。它是一种主动安全防御策略，为信息传输提供安全保护，并和其他网络安全技术（如防火墙、访问控制系统等）一起构筑安全可靠的网络环境，使得计算机的应用更加广泛和深入。■