浅谈 RSA 数字签名技术在综合船桥系统中的应用

刘桂洪,张海波,于春梅

(山东省青岛平度市明村镇投资服务中心,山东 青岛 266723)

摘 要:随着 Internet 的快速发展,网络在综合船桥系统中得到了广泛的应用。在享受网络带来的便利的同时,它的各种弊端也日益显露,如网上数据传输的完整性等问题。为了很好地解决这一问题,将 RSA 数字签名和数字摘要应用于综合船桥系统中。在保证数据安全传输的同时,很好地验证了数据的完整性,同时完成了发送方的身份验证。

关键词:综合船桥系统;RSA 数字签名;MD_5 数字摘要

中图分类号:TP301.6 **文献标识码**:A **文章编号**:1674-7720(2011)03-0052-02

The application of RSA digital signature technology in the integrated bridge system

Liu Guihong, Zhang Haibo, Yu Chunmei

(Service Centre of Investment of Mingcun Town Pingdu County, Qingdiao 266723, China)

Abstract: With the rapid development of internet, network is widely used in the integrated bridge system. While enjoying the convenience of the network, it has shown all the disadvantages, such as the data integrity issues. In order to solve this problem, this paper will apply RSA digital signatures and digital summary in the integrated bridge system. At the same time, it ensures the secure transmission of data, verifies the integrity of the data and completes the sender's identity authentication.

Key words: integrated bridge system; RSA digital signatures; MD_5 digital summary

随着计算机网络的快速发展,信息网络化在综合船桥系统中得到广泛的应用,而网络的各种弊端也日益显露,如数据传输的完整性、保密性以及各种访问者的身份验证等问题。综合船桥系统各子系统的日常运行涉及大量信息在各部门之间传递,通过信息传递来实现各部门的分工协调工作,因此重要信息的保密和确认也是亟待解决的问题。而目前这些信息的保密性一般采用明文传送和简单的口令机制实现对用户的身份认证,进而控制用户访问重要信息的权限及确认信息发送者的身份,但这不能完全保证重要信息的保密性、完整性和抗否认性。本文采用的数字签名可以很好地解决这一问题。

1 综合船桥系统信息安全

综合船桥系统 IBS (Integrated Bridge System)是新一代多功能综合型船桥系统,数据通信网络是综合船桥系统的重要组成部分,数据通信网络实现了在 IBS 内任一工作站的信息共享,是实时监测船舶航行状态和船舶自身工作状态,控制船舶按照预定航线航行,快速实施避碰,实现安全航行的保证[1]。

综合船桥系统中包含的信息广泛,有些信息(如航行状态、船舶工作状态等)是非常重要的,各子系统间不断地进行数据交换,以保证日常工作的正常运行,因此信息的传输非常重要。由于计算机网络缺乏足够的安全性,网络上传输的信息随时都受到各种威胁,如被非法用户盗听、窃取,未被授权用户的非法查看、篡改和破坏。

为了保证信息传输的完整性、用户身份的正确性和不可抵赖性,本文将基于 RSA 算法的数字签名技术应用于综合船桥系统信息交换过程中,以确保综合船桥系统数据的完整性和保密性。

2 RSA 数字签名算法和单向散列函数 MD_5

所谓“数字签名”就是通过某种密码运算生成的一系列符号及代码组成电子密码进行签名,用来代替书写签名或印章。数字签名已经在很多领域得到了普遍应用,可操作性强,很好地保证了文件在传输过程中的完

整性、真实性和不可抵赖性。

在 RSA 数字签名变换前，先使用单向散列函数 MD_5 对明文进行数字摘要操作，其在保证数字签名效果的同时更好地提高 RSA 数字签名操作的运行速度。

2.1 数字签名的作用

(1)身份认证：利用数字签名辨认和鉴定被指定方身份的真伪，如果该签名通过验证，则可以肯定其身份确凿无疑。

(2)数据完整性：利用数字签名技术确认数据在传输和存储过程中没有被修改。

(3)数据保密性：除了指定的授权者外，其他没经授权的人无法读出或即使读出也无法看懂该数据信息。

(4)不可否认性：一方面，用数字签名的方法从技术上防止签名者对其行为的否认，另一方面，确保数据来源的不可否认性，即用户不能否认信息和文件是来源于他。

2.2 单向散列函数 MD_5

MD_5 函数是一种单向散列函数，它将任意长度的消息压缩成 128 bit 的消息摘要。应用 MD_5 的单向性和抗碰撞性，可以实现信息的完整性检验。另外，该函数执行的速度快，是一种被广泛认可的单向散列算法。

MD_5 数字摘要过程：发送者利用 MD_5 函数对传送的信息进行数字摘要操作得到 128 bit 的摘要值，并将此摘要值与原始信息数据一起传送给接收者，接收者用此摘要值来检验信息数据在网络传送过程中是否有改变，以此来判断信息的真实性[4-6]。

3 可行性分析

对于综合船桥系统的数据，在其传输过程中，可能因某些传输协议、信道、防火墙的问题，或者黑客攻击而导致信息被拦截、窃取、破坏和篡改，因此在数据传输之前使用一些数字签名算法对重要核心数据签名，然后再进行传输，这样就大大提高了信息传输的完整性和抗攻击能力。

与此同时，可能因为一些特殊的需要，会遇到关于传输者的身份和文件的不可抵赖性，以及文件的保密性和完整性等问题的困扰，为了解决这个难题，本文引入了数字签名机制，在进行数字签名前，首先采用 MD_5 哈希函数在信息转换前对它进行数字摘要，以提高 RSA 数字签名的速度。这样既解决了信息验证的问题，又有效地解决了 RSA 速度上的缺陷。

4 RSA 数字签名算法流程和实现

4.1 算法流程

综合考虑综合船桥系统的各种信息的安全性问题，在信息传输前对信息进行数字签名，可以很好地保证信息在传输过程中不会被未被授权的用户查看、篡改和破坏，接收到数据后还可以验证发送方的身份，以及验证文件信息的不可否认性。

本文的数字签名过程如下：

(1)数字摘要过程：发送者使用 MD_5 算法对明文信息进行数字摘要变换。

(2)签名过程：发送方使用自己的私钥对明文信息进行数字签名变换，将加密后的消息和签名发送给接收方。

(3)验证过程：接收方使用发送方的公钥对收到的消息进行数字签名验证变换，然后再比较与发送方的公钥解密恢复消息 M 即可。

数字签名算流程框图如图 1 所示。

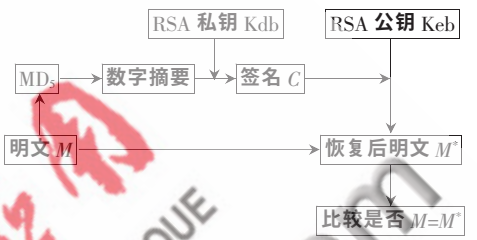

图 1 数字签名算法流程

RSA 数字签名易于实现，并且可以和加密算法相结合。但是签名者每次只能签名 $\log_2 n$ bit 长的消息，获得同样长的签名。一般说来，如果所要签的消息很长，签名前只能把消息分成 $\log_2 n$ bit 大小的分组，逐组进行签名。由于 RSA 数字签名中基本运算都是长字节运算，这样运行的速度较慢，如果整个发送信息都使用 RSA 签名，速度就成了瓶颈。为了解决速度的约束，本文在对明文消息进行签名之前首先采用 MD_5 对明文信息进行数字摘要，然后再由 RSA 算法对固定长度的数字摘要进行数字签名变换[2]。

对于 MD_5 算法，要找到两个具有相同散列值的信息在实现上是不可行的，因此解决了信息在传输过程中被篡改的问题。

4.2 数字签名在 IBS 中的算法实现

图 1 给出了 RSA 数字签名的算法流程，其算法的实现步骤如下：

(1)发送方首先使用 MD_5 算法对明文信息 M 进行数字摘要变换。

(2)发送方使用自己的私钥 Kdb 对明文信息 M 进行数字签名变换：$C=M^{Kdb}(\mathrm{mod}n)$。

(3)将加密后的消息 M 和签名发送给接收方。

(4)接收方使用发送方的公钥 Keb 对收到的消息 C 进行数字签名验证变换：$M^*=C^{Keb}(\mathrm{mod}n)$。

(5)比较 M^* 与发送方的公钥解密恢复消息 M。

(6)如果 $M^*=M$ 则证实发送方的身份合法。

在信息安全领域存在多种加密算法，随着计算机网络技术的发展，信息安全越来越受到重视，本文针对问题的实际情况，在 RSA 数字签名算法和 MD_5 算法的基

础上，将 RSA 数字签名机制应用到综合船桥系统中。此算法原理简单、易于实现，既保证了信息的完整性，又保证了信息的真实性和完成用户的身份验证。同时，在签名操作前使用 MD_5 进行数字摘要操作，使得加密速度较快，而对安全性没有影响，很好地符合了系统的要求。

参考文献

[1] 曾庆军，周耀庭.综合船桥系统研究综述[J].中国航海，2000，46(1)：28-37.

[2] 徐炜，陶翔.数字签名在网上交易中的应用[J].电子商务，2006(34).

[3] 王保义，张少敏.用混合密码算法实现电力系统重要信息的安全传送[J].电力自动化设备，2004，24(4)：64-67.

[4] 凌捷. 计算机数据安全技术 [M]. 北京：科学出版社，2004.

[5] 牛少彰.信息安全概论[M].北京：北京邮电大学出版社，2004.

(收稿日期：2010-10-12)

作者简介：

刘桂洪，男，1969年生，本科，工程师，主要研究方向：计算机应用。