第13卷第2期 广西科学院学报 Vol. 13, No. 2
1997年5月 Journal of Guangxi Academy of Sciences May 1997

电子邮件系统R-MAIL的安全机制设计*
Design of the Security Mechanism of R-MAIL: an E-Mail System

石文昌
Shi Wenchang

(广西计算中心 南宁 530022)
(Guangxi Computing Center, Nanning, 530022)

摘要 介绍研制的图形视窗式电子邮件系统R-MAIL中的安全机制的设计思想。
关键词 电子邮件 安全 加密 压缩 密码
Abstract Intruduce designing ideas of the security mechanism of R-MAIL: a graphic window based E-Mail system developed by us.
Key words E-Mail, security, encryption, compression, password
中图法分类号 TN919.8

电子邮件系统的最基本功能是利用计算机和现代通讯设施实现人们相互之间通信的电子化。安全保密机制是电子邮件系统的重要组成部分。考虑电子邮件系统的安全保密性时，需要注意以下问题：

(1) 防止邮件在传输过程中被他人窃取；
(2) 防止邮件内容被他人篡改；
(3) 防止发送者伪造他人签名；
(4) 防止他人偷看邮件内容。

R-MAIL是我们研制的一个图形视窗式电子邮件系统[3]，在该系统的安全保密机制设计方面，我们尽量使系统满足以上各项要求。本文首先对国外一些值得借鉴的方法进行分析，然后，以此为基础，给出系统的设计思想。

1 PGP方法

PGP (Pretty Good Privacy) 是Phil Zimmermann研制的一个软件包[1]，其作用是实现电子邮件的安全性。PGP方法具有很大的参考价值。以下给出的是PGP方法对电子邮件进行处

1996-09-03收稿。
* 相关项目1996年获广西科技进步奖。

理的过程。

1.1 发送方的处理过程

步骤1：取明码邮件；

步骤2：用MD5（Message Digest version 5）哈斯函数为给定邮件产生一个128位的哈斯码，用发件人的个人密钥对哈斯码进行RSA加密，把加密的哈斯码附加到邮件上；

步骤3：用ZIP算法对附加了哈斯码的邮件进行压缩；

步骤4；产生一个128位的随机数作会话密钥，用该会话密钥对压缩邮件进行IDEA（International Data Encryption Algorithm）加密，用收件人的公开密钥对会话密钥进行RSA加密，并把结果附加到已加密的邮件上；

步骤5：传送经以上处理的邮件。

1.2 接收方的处理过程

步骤1：接收发送方传送的邮件；

步骤2：用收件人的个人密钥对会话密钥进行RSA解密，用会话密钥对邮件进行IDEA解密；

步骤3：用ZIP算法对邮件进行解压；

步骤4：用发件人的公开密钥对哈斯码进行RSA解密，用MD5对收到的邮件产生一个新的哈斯码，将新哈斯码与收到的哈斯码作比较，两者一致时，表明收到的邮件是发件人发出的原件，否则，表明邮件已被篡改或发件人署名是伪造的。

1.3 分析

从发送方的处理过程看，步骤2实现的是数字签名，步骤3实现的是压缩，步骤4实现的是加密。

2 Snow 与 Whitfield 注册身份识别法

Snow和Whitfield两个人提出了一种在远程注册过程中进行用户身份识别的方法[2]，这里，简称为SW方法。SW方法对确保注册信息的保密性是简单有效的。注册信息包括用户的标识及其注册密码，SW方法的中心点在于防止用户的注册密码被他人窃取。

SW方法把负责注册的程序分为两部分，一部分负责接收用户的输入信息，称为用户端，另一部分负责验证用户提供的注册信息，称为验证端。注册过程定义如下：

（1）用户端启动注册过程，验证端产生一个64位的随机数，并传送给用户端；

（2）用户端接收用户输入的用户标识和注册密码，用确定的算法把注册密码转换成一个64位的密钥，用该密钥对随机数进行DES加密，把加密结果连同用户标识传送给验证端；

（3）验证端以用户标识为关键字，在用户信息登记表中检索出解密密钥，用该密钥对加密的随机数进行DES解密；

（4）验证端把解密后得到的结果与原来产生的随机数作比较，如果两者一致，则注册成功，否则，注册失败。

SW方法在用户注册信息登记表中保存着用户标识和解密密钥，解密密钥是通过确定的算法对用户的真实注册密码进行转换而形成的。

3 R-MAIL 方案

有鉴于各种成功有效的方法，R-MAIL电子邮件系统的安全保密机制采用了注册、加密、

压缩等措施来实现。

用户使用系统，首先必须通过注册这一关。参考 SW 方法，把注册系统的用户端设在用户终端计算机上。由于系统允许用户进行远程注册和本地注册，所以，在中心邮局服务器和用户终端计算机上都设有注册系统的验证端。远程注册时，服务器上的验证端工作，本地注册时，终端机上的验证端工作。

邮件的处理过程，参考了 PGP 方法，但没有完全采用。

PGP 方法对邮件是先压缩后加密，R-MAIL 的方法是先加密后压缩。压缩是在邮件发送前自动进行的。考虑到加密所需的时间开销往往比较长，系统没有统一对邮件进行自动加密。加密的选择留给用户自行确定。为了提高效率，加密的算法尽可能选择简洁有效的，而且，允许采用多种加密算法，对支持的各种加密算法进行编号，加密时，把算法的编号也附加到邮件上，解密时，根据加密算法的编号确定应采用的解密算法。

在防伪造署名方面，目前没有采用数字签名的方法。用户注册进入系统的时候，系统已把用户的身份记录下来，制作信件时，不是让用户自己署名，而是由系统进行自动署名，这样，邮件上声称的发件人只能是注册入系统的用户，不可能是其他人，用户没有机会冒充他人发送邮件。

邮件内容防篡改的要求，通过给邮件设计一个“禁止修改”属性来达到。制作邮件时，允许用户给邮件设置“禁止修改”属性，收件人收到具有这个属性的邮件时只能查看而不能修改其有关信息。

4　结语

R-MAIL 电子邮件系统的安全保密机制，是以 SW 注册身份识别法和 PGP 电子邮件安全处理方法为原型，经过简化和修改后设计出来的。实践证明是成功的，在实际应用中，能够发挥较好的作用。对于常规应用系统而言，该设计已满足了用户的安全保密要求。若需用于安全保密要求特别严格的部门，则该安全保密机制尚有待于进一步加强。

参考文献

1　William Stallings, Pretty Good Privacy, BYTE, 1994, 7.

2　Snow C R, Whitfield H. Simple Authentication, Software Practice & Experience. 1994, 5.

3　石文昌，廖文辉，杨　磊. 图形视窗式电子邮件系统 R-MAIL 的研制. 计算机应用研究，1996，2.