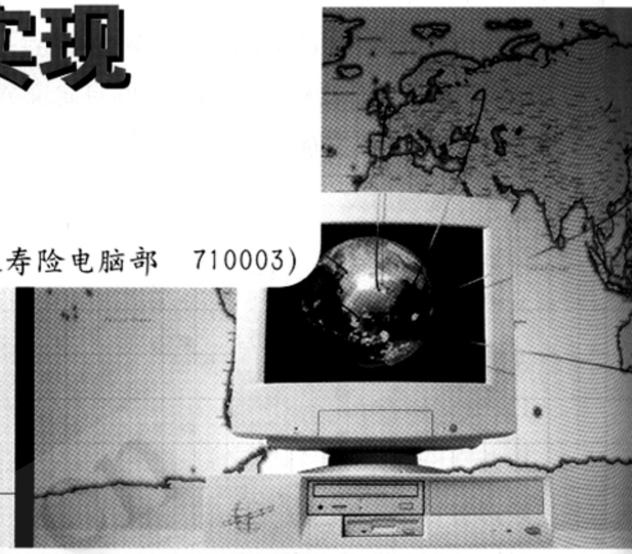
信息安全软件PGP的实现内幕及其应用



周艳梅　马军　(西安南大街3号人寿险电脑部　710003)

摘要　本文详细分析了目前在Internet上广泛使用的加密及数字签名软件PGP的实现原理，包括加密、数字签名、密钥管理与分发、压缩、电子邮件兼容性及分段等技术，并举例说明其在信息安全中的应用。

关键词　PGP　加密　数字签名

1　引言

由于Internet及TCP/IP协议最初设计是非商业用途的，几乎没有考虑安全性，目前在TCP/IP协议之外具有多种实现网络安全的协议，但几乎都属于系统和网络各层次的安全措施，如IPSec、SSL、防火墙等，而系统一级的安全措施不便于用户直接应用，PGP（Pretty Good Privacy）是专门针对广大用户设计的一个小巧而强有力的加密、鉴别、数字签名软件，由于其技术的先进性，目前，仍被美国政府禁止出口，但其免费软件已在Internet和民间广泛应用。本文将剖析PGP的实现内幕和应用。

2　PGP实现内幕

PGP主要由Philip Zimmermann 设计的电子邮件加密、数字签名软件，其实现涉及加密、数字签名、密钥和密钥管理等技术，后来IETE委员会成立了OPEN/PGP工作组，定义了RFC2440 OPEN PGPMessage Format标准，用于为电子邮件和文件存储、传输提供安全服务。

2.1　加密技术

PGP采用常规密钥算法和公开密钥算法相结合实现报文加密。

常规加密算法又称对称密钥算法，它要求发信者和收信者在安全通信前，商定一个共享密钥，解密算法是加密算法的逆过程。常规算法分为：序列算法和块算法两种，序列算法是一次只对明文的一个位/字节进行运算；块算法是一次对明文的一组位进行运算（通常是64位），常用的常规算法是块算法，采用Feistel置换、循环移位密码结构，加密强度很高。其安全性依赖于密钥的保密管理。当多点通信时，每两点之间要共享一密钥，密钥的数量因两两组合而激增，需要有复杂的密钥管理和分发中心，代价极高。其优点是效率高，缺点是密钥保密管理和保密分发的难度大，适用于个人文件加密管理，或同公开密钥算法相结合实现加密通信。著名的常规加密算法有：DES、TDEA、IDEA、CAST-128等。

公开密钥加密算法是加密密钥与解密密钥不同，加密密钥称公钥，解密密钥称私钥，由公钥无法推导出私钥。主通信方在通信前生成公钥/私钥对，然后公开发布公钥，可由多个用户接收，私钥只有主通信方保密持有，接收方用收到的公钥加密报文发送给主通信方，主通信方用私钥解密得到原报文。著名的公开密钥算法RSA是建立在大数分解的数学难题之上，即“两个大素数的乘积分解为两个素数是一个未决的数学难题”。由于公钥是公开发布的，其优点是密钥管理简单易行，缺点是加密效率远远低于常规加密算法，适于短报文加密、数字签名和常规密钥分发。

PGP采用常规加密算法IDEA、TDEA或CAST-128和公开密钥算法RSA、ELGamal（Diffie-Hellman的一种变体）的可选组合实现报文加密。PGP在生成RSA算法的公钥/私钥对时，考虑到了加密速度和保密强度之间的折中（密钥越长，加密强度越高，但加密速度越慢），用户可选512、768、1024三种密钥长度。加密报文的步骤如下：

(1) 发送方创建报文M

(2) 发送方生成一个128位随机数，作为会话密钥K，是一次性密钥

(3) 发送方用会话密钥K加密压缩过的报文M（可选IDEA或TDEA或CAST-128）

(4) 发送方用接收方的公钥KUB对会话密钥K加密，且将结果附在报文上（可选RSA或ELGamal）

(5) 接收方用私钥KRB解密会话密钥得到K

(6) 接收方用K解密密文得到原报文M

PGP加密过程为图1所示。

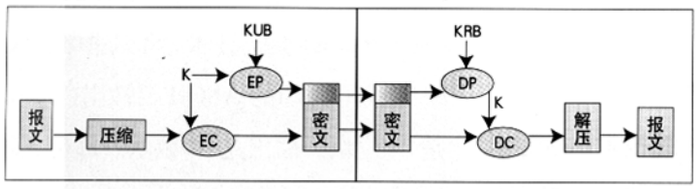


图 1 PGP加密过程

其中：EC 常规密钥加密算法

EP 公开密钥加密算法

K PGP在加密前生成的一次性密钥

KUB 接收方B方的公钥

KRB 接收方B的私钥

DP 公开密钥解密算法

DC 常规密钥解密算法

2.2 数字签名技术

数字签名是签字人首先用单向哈希函数求得原报文的报文摘要，再用RSA算法中的私钥加密报文摘要，就生成了“数字签名”，接收方用签字人的公钥解密“数字签名”，得到签字人发来的报文摘要，然后再计算收到报文的报文摘要，将两个报文摘要进行比较，若相同，则验证了报文及签名是真实完整的。其中：单向哈希函数算法是将任意长度的输入报文，经计算，得出固定位的输出，称为报文摘要。所谓单向是指该算法是不可逆的，找出具有同一报文摘要的两个不同报文是很困难的；找出具有一给定报文摘要的两个不同的报文更为困难。所以只要对原报文稍做修改，就会得出截然不同的报文摘要，通过对比报文传输前后的报文摘要就可判别收到的报文是否被非法修改。由于哈希算法的单向性和严密性，接收方可确保没有其他人能够生成与收到的报文摘要相同的新消息或原始报文的签名，由于RSA算法的坚固性，接收方可确保只有私钥的拥有者才能生成签名，从而验证了发送方的身份，发送方不可抵赖曾给接收方发送过报文的事实，从而实现了数字签名。

PGP采用SHA-1安全哈希函数和公钥算法RSA或DSS的组合实现数字签名。SHA-1算法是将任意长度的输入报文，经计算，生成160位报文摘要。PGP采用SHA-1算法生成报文摘要，用RSA或DSS公开密钥算法将报文摘要用私钥加密并附在报文上一起发送，接收方用发送方的公钥解密得到的报文摘要，再计算收到报文的SHA-1报文摘要，将二者比较，若相同，则证实收到的报文和签名是真实的。步骤如下：

(1) 发送方创建报文M

(2) PGP用SHA-1生成报文的160位报文摘要（哈希码）

(3) PGP采用RSA算法，用发送方的私钥加密报文摘要，将结果附在报文上

(4) 接收方用发送方公钥解密加密的报文摘要，恢复原报文摘要

(5) 接收方生成报文的新报文摘要，并与解密的报文摘要相比较。如二者一致，则报文是真实的，实现报文鉴别和数字签名

PGP数字签名过程为图2所示。

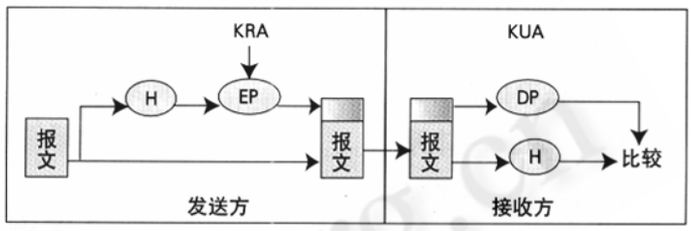


图 2 PGP数字签名过程

其中：H SHA-1安全哈希函数

EP 公开密钥加密算法

DP 公开密钥减密算法

KRA 公开密钥算法中A的私钥

KUA 公开密钥算法中A的公钥

2.3 密钥管理技术

PGP采用密钥环管理密钥，分公钥环和私钥环，公钥环中存放通信对方的公钥，私钥环中存放自己的密钥。

(1) 公钥/私钥对：由本机生成，存在私钥环（SECRING.PGP文件）上。

(2) 接收方公钥：存在公钥环（PUBRING.PGP文件）上。

(3) 常规密钥：在加密前使用一个随机数种子值一次性动态生成密钥，为使每次生成的密钥不同，使用过的随机数种子值存放在文件RANDSEED.BIN中，以保证每次使用不同的随机数种子值生成不同的一次性密钥，该密钥不需要存储，安全性更高。

(4) 私钥的加密存储：由用户输入passphrase,作为SHA-1的输入，生成160位的输出，作为常规加密的密钥对私钥加密。

(5) 私钥环结构

时间戳：密钥对创建时间

密钥ID：唯一地标识一个密钥

公钥：密钥对中的公钥部分，明文存放

私钥：密钥对中的私钥部分，由Passphase生成的160位摘要码加密

用户ID：常为用户的E-mail地址

(6) 公钥环结构

同私钥环结构相比较，没有“私钥”项，但却增加了以下项：

拥有者信任度：表示收到该密钥的用户对密钥的信任程度

密钥合理度：表示该密钥的真实程度，由PGP计算得到。

2.4 PGP的公钥体系

公钥环中的一项对应一个证书，PGP没有专门的认证中心（CA），每个PGP用户为自己的公钥签发证书，这样在证书的分发上存在一定问题，例如发送方使用接收方的公钥KUB是假冒的，那么，由KUB加密的信息只有假冒者可解密，而真正的接收方却无法解密，可通过下述方法解决公钥的安全分发问题。

(1) 在地理范围许可的情况下，将公钥Export到软盘上，通信双方交换软盘实现公钥分发。

(2) 通过电子邮件分发公钥。接收方用PGP生成该公钥的160位SHA-1“指纹”（报文摘要），以16进制格式显示，然后在电话中让发送方口述此“指纹”，如二者相符，可确认收到的公钥。

(3) 从信任的第三方处得到公钥。第三方创建证书，包括：要签发的公钥、创建时间、有效期，然后生成证书的摘要，并用其私钥加密、签名，由于只有第三方持有自己的私钥，所以没有人能伪装第三方来创建假证书。创建的证书可通过电子邮件或在公告板上发布，接收方收到公钥后，用第三方的公钥解密该证书，得到通信对方的公钥。

2.5 PGP压缩技术

PGP使用ZIP压缩技术。加密前对明文采用ZIP算法压缩，可提高加密、传输效率，同时，增大攻击的难度。PGP采用由Jean-lup Gailly、Mark Adler和Richard Wales编写的ZIP压缩包，是由C编写的免费软件。基本思想是：输入的文本流，其内容往往是就一个主题展开的讨论，其中出现重复字符和短语的频率很高，当重复字符或短语出现时，用简短的代码替换重复序列。

2.6 电子邮件兼容性

E-mail以SMTP协议传输，只能传输ASCII码，当要发送的E-mail中包含非ASCII码或ASCII码经压缩后产生非ASCII码时，在传输前，要转换成ASCII码，在接收端进行逆变换。PGP采用基数64转换（Radix-64 Conversion）编码技术，将二进制输入映射成可打印的ASCII码输出，输入是24位块，输出是32位块，每6位输入二进制，输出8位。

2.7 报文分段

基于SMTP的E-mail将受到最大消息长度的限制，任何大于此最大长度的报文必须分成数个小段，每一段都要单独邮寄。PGP在所有处理完成后自动将太长的报文分成可以通过电子邮件发送的小段，在接收端，PGP必须打开所有的电子邮件报头，首先重组出整个电子邮件块，重现发送端在分段前的原始块。

3 一个案例

用PGP软件解决企业内部物流管理中的信息安全问题。案例陈述：某企业有一物资管理部门，要给其他部门发放物资。物资管理部门用Excel电子表格建立起物资发放表，其中有“领用清单及签名”项，须由领用方进行数字签名，且领用清单在网络中安全传递。清单如下表所示：

领用部门	发放人	发放日期	领用清单及签名

实现策略

发方将发放清单签名、加密发给领用方。领用方解密、验证后进行数字签名，然后回送给发方。发方验证后将签名嵌入到对应栏。

具体步骤如下：

(1) 导出公钥。在参与密钥交换的各计算机上安装PGP软件，并生成公/私钥对，再将公钥Export成磁盘文件。

(2) 密钥交换。物资发放部门同各领用部门之间互相分发公钥。公钥可通过交换软盘分发，若以E-mail形式交换公钥，可通过电话来验证，各自将收到的公钥Import到本机的公钥环内。具体方法如上PGP公钥体系所述。

(3) 签名和发送信息。物资发放部门按部门建立物资发放明细表，标明

（下转第18页）

(上接第33页)

日期，预留出“领用人签名”项，生成磁盘文件，并用PGP进行数字签名，再以E-mail（用PGP加密后的电子邮件，下同）或软盘形式（用PGP加密后的文件，下同）发给对方。

(4) 验证签名和交换签名。接收方用发送方的公钥验证明细表，经核对确认后，签署领用人姓名，再数字签名该文件，生成一个数字签名文件，并以E-mail或软盘形式发送给物资发放部门。物资发放部门收到签名后，可用领用方的公钥验证该签名，确认是有效签名后，在物资发放总表的领用部门签名项处将签名文件以OLE方式嵌入，编辑其图标大小到合适为止。

以上步骤实现了企业内部物流管理中的敏感信息的传递和管理。

当然也可以用PGP 创建一个VPN用于信息安全通信。

4 结语

PGP软件的实现自身并没有应用独有的信息安全的新技术，但由于它组合了加密、数字签名、压缩、基数64转换、报文分段等多种先进技术，小巧而强大，使得它在加密重要文件、电子邮件以及为签发的文件作数字签名等信息安全方面应用日益广泛。PGP软件的设计思想值得大家借鉴，深入了解其实现内幕有助于信息安全系统和安全软件开发。■

参考文献

1 *http://www.rsa.com*

2 *http://www.pgpi.com*

3 *吴世忠、祝世雄、张文政等（译），应用密码学，机械工业出版社，2000。*