用PGP加密保护电子邮件

张海洲，车文刚，陈韬伟
(昆明理工大学 信息工程与自动化学院，云南 昆明 650051)

摘要：PGP是目前最流行的应用于电子邮件加密传输的算法.本文从PGP加密软件的原理出发，分析了PGP各主要算法模块的安全性，并给出了一个基于WEB的PGP加密电子邮件系统的具体实施过程.

关键词：PGP；RSA；加密；密钥
中图分类号：TP393 **文献标识码**：A **文章编号**：1007－855X(2003)02－0087－04

Using PGP Encryption to Protect Email

ZHANG Hai-zhou, CHE Wen-gang, CTEN Tao-wei
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China)

Abstract: PGP is the most popular algorithm applied to Email's encryption and transmission. According to the principle, the security of main algorithm modules in PGP is analysed, and a detailed method of PGP's application to Web－based Email System is provided.

Key words: PGP; RSA; encryption; secret key

0 引言

PGP(Pretty Good Privacy)是目前流行的一种加密算法，它是一个基于RSA公钥加密体系的邮件加密算法.用PGP可以防止在网络中传输的信息被非法查看、篡改及伪造.也即是说，它能够对于网络传输的几类安全性问题——保密、鉴别、反拒认和完整性控制，进行有效的保护.在开发昆明理工大学信自学院电子邮件系统PGP加密功能模块时，笔者充分利用PGP算法的安全高效，同时考虑自身应用的一些特点，在应用方法上做了一些改进，取得了良好的效果.

1 PGP的加密机理

PGP不是一种完全的非对称加密体系，它是个混合加密算法，它是由一个对称加密算法(IDEA)、一个非对称加密算法(RSA)、一个单向散列算法(MD5)以及一个随机数产生器组成的，每种算法都是PGP不可分割的组成部分.

1.1 PGP核心：RSA算法

RSA(Rivest－Shamir－Adleman)算法利用数论领域的一个事实设计而成，那就是：把两个大的素数相乘很简单，但是将其结果分解为两个素数却十分困难.合数分解是目前数学领域的一大难题，至今没有任何有效的方法.根据这个基本事实，RSA算法最终得到一个加密/解密钥匙对K1和K2，用K1加密只能用K2解密，反之亦然.其中一把钥匙叫做公钥，可以发布出去供信息发送者进行加密.另一把与其配对的叫做私钥，信息接收者用之对加密的信息进行解密.由于公钥的发布，使得任何人都可以对钥匙所有者发送加密信息，并且也只有他能进行解密，这正是非对称的RSA算法的突出优势[1].

1.2 高效的正文加密：IDEA算法

IDEA(International Data Encryption Algorithm)是一个数据块加密算法，采用128－bit的密钥，属于传统

收稿日期：2002－09－25.
第一作者简介：张海洲(1974～)，男，硕士研究生；主要研究方向：计算机网络与多媒体.

加密算法.也即是说,IDEA 的加密和解密用同一把密钥.由于 RSA 算法的加密速度很慢,(1 024 - bit 的纯粹 RSA 加密要比 128 - bit 的 IDEA 加密要慢4 000多倍)用它来直接对信息进行加密是非常不经济的.因此,PGP 采用 128 - bit 的 IDEA 加密信息正文,其中用于加密正文的 128 - bit 密钥叫做会话密钥.在用会话密钥和 IDEA 算法对正文进行加密以后,又采用信息接收者的 RSA 公钥对这个会话密钥进行加密,将其结果和加密的正文按一定的格式合并后再发送给信息接收者[2].

1.3 PGP 的整个加密/解密过程

PGP 加密过程内部原理如图 1.

由图中可以很容易理解信息接收者对此加密文件的解密过程.信息接收者在收到此文件后,先用自己的私钥解密得到会话密钥,然后再用此会话密钥解密信息正文,由此便可以得到信息明文.

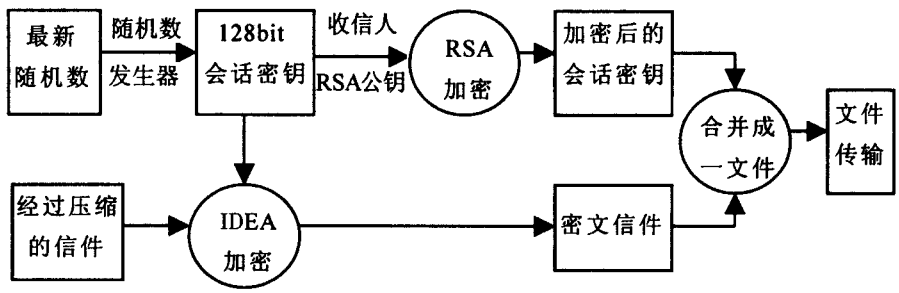

图 1 PGP 加密原理

由于 PGP 采用了上述机理,使得 PGP 高效和易于使用.在 PGP 的官方网站可以下载到 PGP 免费软件的最新版本以供使用(www.pgpi.org).

2 PGP 加密的安全性分析

PGP 的作者 Phil Zimmermann 在 PGP 文档中说到:"没有哪个数据安全系统是牢不可破的."下面对 PGP 的各个组成要素来进行安全性分析.

2.1 私钥的安全

我们知道,PGP 是基于 RSA 公钥加密的,唯一能解密密文的配对私钥就成为了攻击 PGP 的首要目标.私钥应该是惟有信息接收者才能使用的.PGP 对私钥采取了口令保护,在电脑磁盘中,私钥是根据口令的 MD5 值经 IDEA 加密存放的.因此,钥匙对的主人使用的口令是 PGP 的一道重要的防线.传统的 UNIX 仅使用 8 位口令登录,有经验的管理员通过使用尽量复杂的口令(大小写字母、数字和一些符号的混合)加强系统的安全性.而 PGP 可以使用任何长度的口令,其中可以包括空格和符号.这样,对这个口令的分析难度就大大增加了.如果用户选择尽量复杂的口令并且长度合适,那么直接对其进行分析来攻破 PGP,几乎是不可能的.

2.2 IDEA 算法的安全性

IDEA 是瑞士的 James Massey, Xuejia Lai 等人在 1990 年发表的一个数据块加密算法.Massey 被公认为世界级的密码大师.IDEA 使用长达 128 - bit 的密钥,有效地消除了任何试图穷尽搜索密钥的可能.至今为止,尚无任何采用其它方法对 IDEA 进行攻击成功的报道.该算法属于一个"强"的加密算法.

2.3 RSA 算法的安全性

RSA 算法的安全性建立在难于对大数提取因子的基础上.20 世纪 70 年代末,RSA 算法的发明人曾经提出一道 RSA - 129 挑战问题.1993 年,借助于计算机性能突飞猛进的发展,在美国 Bellcore 公司的 Arjen Lenstra、Derek Atkins、Michael Graff 和 Paul Leyland 的领导下,一个国际性的研究小组组织 600 多名志愿者,动用1 600多台工作站、大型机和超级计算机,花费了 8 个月的时间,终于分解了 RSA - 129 问题中的公开钥匙.129 位十进制数相当于 429 为二进制钥匙,而现在的 PGP 最新版提供2 048位的钥匙长度.一般我们使用1 024位的钥匙长度已经足够安全了.

RSA 的钥匙如此之长,有些人担心 IDEA 与之相比不够安全.事实上,算法的安全性除此之外还与破解的方法有着直接的关系.密码分析专家计算过,穷举 128 - bit IDEA 密匙和分解 3100 - bitRSA 密匙的工

作量相当.从密码学的角度来说,IDEA 和 RSA 都是非常"强"的算法.

2.4 MD5 的安全性

MD5 是 PGP 中被用来单向变换用户口令和对信息签名的单向散列算法.对 MD5 最有效的攻击是生日攻击[4],而即使是这样,每 s 进行1 000 000 000次的尝试,也要 500 多年,实际上是行不通的.

2.5 PGP 算法应用的其他安全因素

从以上的分析,笔者认为 PGP 是安全可靠的.当然,虽然从密码学的角度解密困难,PGP 还是面临许多的安全问题,诸如:口令或私钥的泄密、公钥被篡改、删除的文件被人恢复、特洛伊木马程序的攻击、多用户系统信息泄露以及网络流量分析等等.

3 基于 WEB 的电子邮件系统的 PGP 加密

电子邮件是计算机网络中使用最广泛的应用服务之一.TCP/IP 协议族提供了电子邮件的传输和报文格式[5].

3.1 应用于电子邮件的 PGP 加密方式的改进

PGP 的设计遵循电子邮件传输的协议标准.PGP 和电子邮件客户端应用软件(如 Outlook Express)的配合使用,使加密或者解密的过程方便和快捷.这包括:钥匙对的生成、公钥的导入、邮件的加密/解密、或者是数字签名等.

传统的 PGP 加密传输一般是配合 Outlook 等客户端软件使用,虽然现在已经有成熟的插件完成加密任务,但是在加密的时候有一定的不便之处.在很多的 PGP 软件的版本中,信件的正文加密必须放到剪切板中,给解密也带来了一定的不便.图 2 是传统的邮件加密流程.

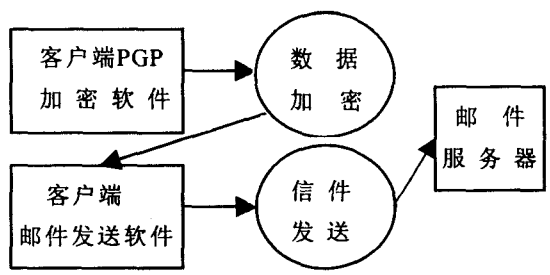

图 2　邮件系统传统 PGP 应用

这样的应用方式,在一定程度上使加密和信件的发送分离为两个过程,以用户的观点来说,还具有一定的不便.并且,这并不是基于 WEB 的加密传输.

笔者在实现 PGP 加密信件进行传输的时候,将 PGP 加密功能模块运行于客户端浏览器页面显示的后台.使用户在完成信件正文编辑之后,根据用户自己的需要,系统自动地完成加密传输的整个过程,加密的过程对于用户来说是完全透明的.这样的实现方式,使得用户在使用的时候非常地方便,实现了系统的易用性.图 3 清晰地反映出系统中 PGP 加密和邮件传输的特点[3].

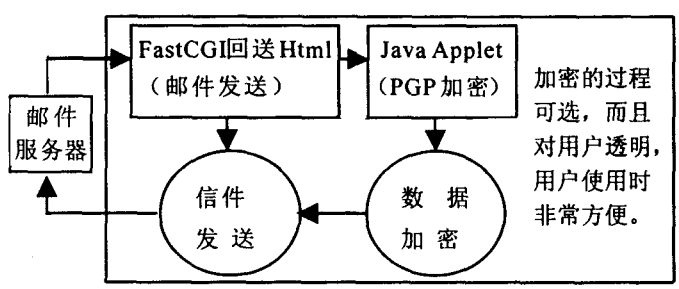

图 3　改进的邮件系统 PGP 加密和信件发送流程

3.2 具体的实现

为了防止信件在传输过程中的泄密,加密过程一定要在客户端完成.采用客户端运行的 Java Applet 程序来实现加密的功能,完全满足了这个要求.

当用户浏览器对发信页面发出请求的时候,Java Applet 程序同时下载到客户端,实现页面显示的同时,再根据用户的正文编辑和选项实现信件的加密传输或者是非加密传输.

这样的实现方式,使得信件的明文仅仅出现于客户端,进行网络传输的信息是已经经过加密的密文,实现了系统信息传输的安全性.

(下转第 94 页)

弱.

另外,从1997年建筑业总产出和增加值表中可计算出,1997年全社会总产出为1 998 442 320万元,该年建筑业总产出为173 855 000万元,占全社会总产出的8.70%.该年全社会固定资本形成总额为251 542 001万元,建筑业固定资本形成额为167 473 028万元,占全社会固定资本形成额的66.60%,反映了建筑业在固定资本形成中的重要作用.

3 结 论

以上通过对1997年国民经济投入产出表中建筑业的分析,可看到:首先,建筑业完全消耗系数和为2.013 32,其前后关联度大,对其他行业的拉动作用大;其次,建筑业影响力系数大于1,而感应度系数小于1,说明它对其他行业的影响作用大,而对其他行业的依赖性小;再者,建筑业总产值占社会总产值的8.70%,在国民经济中占据了较大的份额.这些分析数据充分表明了建筑业在经济结构和产业结构中的重要地位.

参考文献:

[1] 卢有杰.新建筑经济学[M].北京:中国水利水电出版社,2002.79~81.

[2] 中国统计年鉴2001版[OL].中国国家统计局数据网.

(上接第89页)

在系统模块划分上,加密和传输分为两个完全独立的模块.笔者按照PGP加密的标准,以Java代码实现了PGP加密算法,它能为包括邮件传输在内的许多应用提供PGP加密.这样,能够根据应用的需要,自由地安装PGP加密模块.而信件发送模块最大限度的保持了原有的完整性,这更易于对二者进行维护和开发新的功能.

3.3 应 用

我们经过综合分析而采取上述的实现方式,开发了基于WEB的PGP加密的电子邮件系统.经过在昆明理工大学信自学院电子邮件系统上的运行测试,取得了良好效果,其最大的优点就是用户使用方便和信件安全传输.在用PGP进行加密的电子邮件系统中,这是一些有效的方法.

4 结束语

PGP应用于电子邮件,是安全高效的.在邮件系统的开发中使用Java Applet程序在客户端加密,以尽量发挥其安全性和易用性.

参考文献:

[1] 樊宬丰,林东著.网络信息安全&PGP加密[M].北京:清华大学出版社,1998.

[2] RFC1991, RFC2015[OL]. http://www.ietf.org/rfc/.

[3] 于中江,车文刚,等.利用Fast CGI应用程序提高Apache Web Server性能[J].昆明工大学学报(理工版),2001,26(6):35~38.

[4] [美]Andrew S. Tanenbaum著,熊桂喜,王小虎,等译. 计算机网络(第三版)[M].北京:清华大学出版社,1998.

[5] [美]Douglas E. Comer著,林瑶,蒋慧,杜蔚轩,等译.用TCP/IP进行网际互连(第三版):第2卷[M].北京:电子工业出版社,1998.