电子邮件安全协议—PGP

钟泽秀
（西藏职业技术学院电子信息系，西藏拉萨　850000）

摘　要　首先介绍电子邮件的传输过程，引出安全电子邮件的重要性，然后介绍电子邮件安全协议 PGP，涉及到的 IDEA、RSA、MD5 加密算法以及其安全性分析。

关键词　电子邮件 ；PGP ；加密算法 ；安全性
中图分类号 ：TP393　　文献标识码 ：A　　文章编号 ：1671-7597（2014）08-0140-02

电子邮件的方便、快速、费用低廉等优点，再加上它不但能传送文字信息，还可以附上图像、声音等功能，这使得电子邮件越来越受人们的欢迎。

1 电子邮件的传输过程

电子邮件通过 SMTP 和 POP 协议来进行发送和接受，但由于互联网的开放性，邮件内容是以明文的形式在互联网上进行传递。这使得人们在使用电子邮件时不得不考虑其安全因素，因此如何保证电子邮件的机密性、完整性、真实性和不可抵赖性等方面的问题显得尤为重要。

2 PGP 介绍

为了使电子邮件在互联网上能够安全运行，开发出了一些安全电子邮件标准：PGP 和 S/MIME。其中 PGP 被广泛运用。

PGP（Pretty Good Privacy）是美国人 Phil Zimmermann 研究出来的，它是由多种加密算法（IDEA、RSA、MD5、随机数生成算法）组合而成，不但能够实现邮件的保密功能，还可以对邮件进行数字签名，使收信人能够准确判断邮件在传递过程中是否被非法篡改。

3 PGP 工作原理

3.1　IDEA 算法

IDEA 属于对称加密算法，即加密密钥和解密密钥相同，具体的算法规则是，将输入数据以每 64 为一块，对每块进行分组，分为 4 组，每组 16 位，作为第一轮的输入，进行相乘、相加、异或等运行后，形成 4 个子分组，将中间两间进行交换，作为下一轮的输入，经过 8 轮运算后，同样得到 4 个子分组，再将这 4 组重新连接到一起形成密文共 64 位。

3.2　RSA 算法

RSA 属于非对称加密算法，也称公钥算法，即加密密钥和解密密钥不同，并且加密密钥可以完全公开，但由于没有解密密钥，即使非法者窃取到了密文和发送者的加密密钥也无法查看内容，解决了对称加密中对密钥管理困难的问题，RSA 的安全性取决于对大数的因式分解，这是数学上的一个难题。

RSA 算法描述：

1）随意选择两个大的质数 p 和 q，p 不等于 q，q 和 p 保密；

2）计算 n=pq；

3）欧拉函数，φ（n）=（p-1）(q-1),n 公开，φ（n）保密；

4）选择一个小于 φ（n）的正整数 e,满足 gcd（e,φ（n））=1，e 是公开的加密密钥；

5）计算 d,满足 de ≡ 1（mod φ（n）），d 是保密的解密密钥；

6）加密变换：对明文 $m \in Z_n$，密文为 $C=m^e \bmod n$；

7）解密变换：对密文 $C \in Z_n$，明文为 $m=C^d \bmod n$；

由于 RSA 涉及的运算非常复杂，所以在运算速度上很慢，因而 RSA 算法只适合于对少量数据进行加密，如数字签名，一般情况下，如果要对大量信息进行加密，还是采用对称加密算法，因为对称加密速度比公钥加密速度快得多。

3.3　MD5 算法

MD5 属于 Hash 函数，可以将任意长度的输入压缩到固定长度的输出，具有多对一的单向特性。可以用于数字签名、完整性检测等方面。

4 PGP 提供的业务

PGP 提供的业务包括：认证、加密、压缩、与电子邮件兼容、基数 -64 变换。

4.1　认证

认证的步骤是：①发信人创建信息 M；②发信人使用 MD5 算法产生 128 位的消息摘要 H；③发信人用自己的私钥，采用 RSA 算法对 H 进行加密 ER，M‖ER 连接后进行压缩得到 Z；④将 Z 通过互联网发送出去；⑤接收者收到信息后首先进行解压 Z^{-1}，使用发信人的公开密钥采用 RSA 算法进行解密得出 H，用接收到的 M 计算消息摘要 H，将得出的两个 H 进行比较，如果相同则接收，否则表示被篡改，拒绝。

4.2　加密

加密的步骤：发信人对信息 M 进行压缩，采用 IDEA 算法对其进行加密，用接收者的公钥对密钥进行加密，与 M 进行连接后发出，接收者采用 RSA 算法进行解密得到会话密钥，将会话密钥按 IDEA 算法进行解密，并解压缩，并到原文。

在加密过程中，由于信息相对内容较多，因此对信息的加密采用的是对称加密算法 IDEA 来实现，而密钥采用的是安全强度为高的非对称加密算法 RSA 实现，通过 IDEA 和 RSA 结合，不但提高了邮件传输的安全性，而且在加解密时间上也缩短了。

4.3　压缩

PGP 采用 ZIP 算法压缩信息，这不但节省了存储空间，而且在传输过程中也节省了时间，另外，在对信息进行加密之前压缩，也相当于进行了一次变换，使其安全性增强。

4.4　与电子邮件兼容

由于电子邮件只允许使用 ASC Ⅱ字符串，而 PGP 的输出却是 8 位串，为了与电子邮件进行兼容，PGP 采用基数 -64 变换实现将输出的 8 位串转换为可以打印的 ASCII 字符串。

4.5　PGP 消息分段和重组

电子邮件中对消息内容的长度有限制的，当大于所限制的长度时要进行分段，分段是在所有处理结束之后才进行，所以

会话密钥和签名在第一个段开始位置出现。在接收端，PGP 将重新组合成原来的信息。

5 PGP 安全性分析

由于 PGP 是一种混合密码体系，它的安全性在于 IDEA、RSA、MD5 算法的安全性分析。

5.1 IDEA 的安全性

在 PGP 中采用 IDEA 的 64 位 CFB 模式，很多研究者对 IDEA 的弱点进行了分析，但也没有找到破译的方法，由此可见，IDEA 算法也是比较安全的，它的攻击方法只有“直接攻击”或者是“密钥穷举”攻击。

5.2 RSA 的安全性

RSA 算法是非对称密码体制，它的安全性基于大整数的素分解的难解性，经过长期的研究至今也未找到一个有效的解决方案，在数学上就是一个难题，因此，RSA 公钥密码体制就建立在对大数的因式分解这个数学难题上。

假设密码分析者能够通过 n 分解因子得到 p 和 q，那么他很容易就可以求出欧拉函数 φ（n）和解密密钥 d，从而破译 RSA，因此，破译 RSA 比对 n 进行因式分解难度更大。

假设密码分析者能够不对 n 进行因子分解就求出欧拉函数 φ（n），那么他可以根据 de ≡ 1（mod φ（n）），得到解密密钥 d，从而破译 RSA，因为 p+q=n-φ（n）+1，p-q=sqr（p+q）^2-4n，所以知道 φ（n）和 n 就可以容易地求得 p 和 q，从而成功地分解 n，所以不对 n 进行因子分解而直接计算 φ（n）比对 n 进行因子分解难度更大。

假如密码分析者能够即不对 n 进行因子分解也不需要求 φ（n）而是直接求得解密密钥 d，那么他就可以计算 ed-1，其中 ed-1 是欧拉函数 φ（n）的倍数，因为利用 φ（n）的倍数可以容易的分解出 n 的因子。所以，直接计算解密密钥 d 比对 n 进行因式分解更难。

虽然 n 越大其安全性越高，但由于涉及到复杂的数学运算，会影响到运行速度，那么我们实际运用中，如果来决定 n 的大小使其既安全其速度又不能太慢，目前 n 的长度为 1024 位至 2048 位比较合理。

研究人员建议，在运用 RSA 算法时，除了指定 n 的长度外，还应对 p 和 q 进行限制：① p 和 q 的大小应该相差不多；② p-1 和 q-1 都应该包含大的素因子；③ gcd（p-1，q-1）应该很小。

5.3 MD5 的安全性

MD5 是在 MD4 的基础上发展起来的，在 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。它的安全性体现在能将任意输入长度的消息转化为固定长度的输出。目前对单向散列的直接攻击包括普通直接攻击和“生日攻击”。

在密码学中，有这么一句话：永远不要低估密码分析者的能力。这也将是密码设计者与密码分析者的较量，事实上绝对不可破译的密码体制在理论上是不存在的，因此，在实际应用中，一个密码体制在使用一段时间后，会换一些新的参数，或者是更换一种新的密码体制，当然，密钥也是要经常换的。由此可见，PGP 软件虽然给我们的电子邮件带来了安全性保障，但它也不是永恒的，也许在不久的将来，由于它的弱点被攻击而被新的安全电子邮件产品所代替。

参考文献

[1]刘冰.PGP系统的设计实现与应用[J].重庆工商大学学报（自然科学版），2008（4）.
[2]吴志强.基于PGP加密技术中小企事业安全电子邮件系统的设计与实现[D].南昌大学.
[3]文远.PGP安全电子邮件系统研究与实现[D].北京邮电大学.
[4]陈鲁生，沈世镒.现代密码学（第二版）[M].科学出版社，2008.

作者简介

钟泽秀，讲师，硕士，计算机应用技术专业。

（上接第133页）

误差不超过正负 5 厘米。除此之外，也一定要加强对人为操作的控制，保证操作人员可以严格按照有关规范标准执行具体工作，确保操作的规范性与科学性，进而实现预期的测量目标，为城市建设提供可靠的数据。

在实际应用全站仪的时候，一定要加强控制，并且适当的和 GPS 技术进行配合，这样就可以有效提高测量精度，减小闭合环误差。同时，在地籍测量中，因为房屋密度大，不适合多导线点的布设，导致累计误差较大，降低了测量精度，此时，需要从不同方向进行导线布设，减少导线点，在一定程度上，提高测量精度。

3 结束语

总而言之，在城市地籍测量中，可以结合实际情况，选用恰当的测量技术。GIS 与全站仪在地籍测量中得到了普遍的应用，在一定程度上，减少了工作量，提高了工作效率，并且促进了测绘技术的进一步发展，为社会发展创造了更多的经济效益，实现了城市建设的可持续发展。

参考文献

[1]白晓东.全站仪在数字地籍测量中的应用[J].经营管理者，2010（14）.
[2]李辉.浅谈城市地籍测量中测绘技术的精度控制[J].科技创新与应用，2013（27）.
[3]鞠登磊.城镇地籍数据库的建立及其管理系统的开发[D].华中农业大学，2010.

（上接第138页）

4 结束语

数控技术在机械制造业中的作用是十分重要的，它是实现我国机械制造自动化的重要途径，有利于促进我国工业的飞速发展，提高我国的综合竞争力。在机械加工技术中应用数控技术，是我国机械设备生产未来的发展趋势。为顺应时代的发展，提高我国机械制造的水平，必须大力发展数控技术，以带动我国经济的发展，实现工业经济大国的目标。

参考文献

[1]李敬伟.数控技术在机械加工中的应用及分析[J].河南建材，2012（5）.
[2]程义.数控技术在机械加工技术中的应用研究[J].电子制作，2012（11）.
[3]栾中华.谈数控技术在机械加工中的应用与发展前景[J].科技创业家，2013（14）.
[4]贾永成.数控技术在机械加工中的应用探讨[J].中国科技投资，2013（23）.