第32卷 第1期 吉首大学学报(自然科学版) Vol. 32 No. 1
2011年1月 Journal of Jishou University (Natural Science Edition) Jan. 2011

文章编号:1007-2985(2011)01-0042-03

RSA加密算法的安全性分析*

向 进
(湘西经济贸易学校,湖南 吉首 416000)

摘 要:RSA加密算法是一种使用较多、安全性较高的非对称加密算法,分析了非对称加密体制中RSA加密算法的数学基础,讨论了其破译的可能方法,并根据目前的计算机运行速度,计算了常用的密钥长度破译时所需时间,并对RSA算法的安全性进行了定量分析.

关键词:RSA;数据加密;数据安全;密钥破解
中图分类号:TP393 **文献标志码**:A

随着网络技术的迅速发展和应用,人们已越来越依赖于计算机网络,现在人们普遍将互联网作为信息传送的平台,但在互联网上进行信息的传送存在许多不安全因素.为了确保重要信息在网上安全传输,目前采用的措施主要有3种[1]:安全信道、加密技术和信息隐藏,其中加密技术是应用最广的一种,虽然目前理论上没有不能被破解的加密算法,但只要加密后的数据在要求的时间内不被破解,数据就是安全的.目前的密码体制分为对称密码体制和非对称密码体制2种,非对称密码体制的密钥的管理和传送很方便,在通过网络传输信息时,公钥密码算法体现出了单密钥加密算法不可替代的优越性,其中公钥密码体制的算法中最著名的代表是RSA算法[2],RSA算法的安全性问题尚未得到理论上的证明[3],笔者就其安全性进行了一定的分析.

1 RSA加密算法的描述

RSA算法是一个基于初等数论定理的公钥密码体制加密算法,它的实现过程为:选取2个大素数p与q,然后算出$n=pq$,$\varphi(n)=n-p-q+1$,再选取一个正整数e,使之满足$(e,\varphi(n))=1$,$1<e<\varphi(n)$;再求出正整数d,使之满足$1<d<\varphi(n)$,且使$de\equiv 1 \bmod \varphi(n)$.RSA体制的公钥是$<n,e>$,而密钥是$<n,d>$.明文消息$m$满足$0\leqslant m<n$,加密过程为$m$的$e$次方用$n$除后所得的余数,即为密文$c$;解密过程为$c$的$d$次方用$n$除后所得的余数,即为明文$m$.

例 取2个质数$p=11$,$q=13$,p和q的乘积为$n=p\times q=143$,算出$\varphi(n)=n-p-q+1=120$;再选取一个与$\varphi(n)$互质的数,例如$e=7$,则公开密钥$=\langle n,e\rangle=\langle 143,7\rangle$.

对于这个e值,用欧几里德扩展算法可以算出其逆:$d=103$.因为$e\times d=7\times 103=721$,满足$e\times d \bmod z=1$;即$721 \bmod 120=1$成立.则秘密密钥$=\langle n,d\rangle=\langle 143,103\rangle$,

设发送方需要发送机密信息(明文)$m=85$,发送方已经从公开媒体得到了接收方的公开密钥$\langle n,e\rangle=\langle 143,7\rangle$,于是发送方算出加密后的密文$c=m^e \bmod n=857 \bmod 143=123$并发送给接收方.

接收方在收到密文$c=123$后,利用只有他自己知道的秘密密钥计算$m=cd \bmod n=123^{103} \bmod 143=85$,所以,接收方可以得到发送方发给他的真正信息$m=85$,实现了解密.

用RSA体制加密时,先将明文数字化再进行加密,在实际应用中m值的长度一般要远大于n的长度,因此实际加密消息m时,首先将它分成比n小的数据分组(采用二进制数,选取小于n的2的最大次幂),再每组单独加密和解密.比如说,选用的p和q为100位的素数,那么n将有200位,每个数据分组应小于200

* 收稿日期:2010-11-20
作者简介:向 进(1963-),男(土家族),湖南吉首人,湘西经济贸易学校讲师,主要从事信息安全及应用研究.

位长,但为保证安全性,每个数据的长度应尽量接近 n 的长度.

2　RSA 算法的加密强度与因子分解强度

目前密码的破译主要有 2 种方法. 方法之一是密钥的穷尽搜索,其破译方法是尝试所有可能的密钥组合. 虽然大多数的密钥尝试都是失败的,但最终有一个密钥让破译者得到原文,这个过程称为密钥的穷尽搜索. 方法之二是密码分析. 由于 RSA 算法在加密和解密过程都是用指数计算,其计算工作量巨大,用穷尽搜索法进行破译是根本不可能的. 因此要对 RSA 算法加密后的信息进行破译只能采用密码分析法,用密码分析法攻击RSA密码系统,途径之一是直接计算"n 的 e 次方根",但目前还没有解决这一问题的算法,这个问题是现实不可计算的问题;途径之二[4] 是想办法计算出 d,欲得到 d,可考虑从以下 3 个方面入手.

(1) 将数 n 分解因子. 密码分析员一旦分解出 n 的因子 p 和 q,就可以先后求出 $\varphi(n)$ 和 d,从而攻破 RSA 公开钥密码系统. 由此得出如下结论:破译 RSA 密码不可能比分解因子的问题更困难.

(2) 不分解 n 的因子计算 $\varphi(n)$. 显然,如果密码分析员能够求出 $\varphi(n)$,由于 e 是公开的,就可以通过 $de \equiv 1 \pmod{\varphi(n)}$ 算出 d,从而攻破 RSA 密码系统. 但是,一旦密码分析员知道了 $\varphi(n)$,他就可以很容易地分解出 n 的因子. 究其原因为

$$\varphi(n) = n - (p+q) + l,$$

所以,由 n 及 $\varphi(n)$ 可以计算出 $(p+q)$. 有了 $(p+q)$,就可以通过 $p-q=\sqrt{(p+q)^2-4n}$ 求出 $(p-q)$,因而最终解出 p 和 q. 计算 $\varphi(n)$ 的方法并不比分解 n 的因子容易,换言之,通过计算 $\varphi(n)$ 破译 RSA 密码的方法不会比通过分解 n 的因子破译 RSA 密码的方法更容易.

(3) 不分解 n 的因子或计算 $\varphi(n)$ 确定 d. 如果能够知道 d,分解 n 的因子问题也同样会变得容易起来. 因为 $\varphi(n) = (ed-1) \times k$,其中 k 为任意整数,已知 d (e 是公开的) 时,可求出 $\varphi(n)$,根据 $\varphi(n) = n-(p+q)+l$,由于 n 是已知的(公开的),在求出 $\varphi(n)$ 时可求出 $p+q$,设求出的 $p+q=r$,又由于 $n=p\times q$,从而可得 $p\times p - p\times r + n = 0$,这是一个一元二次方程,自然可非常简单求出 p,同理可求出 q,分解 n 完成.

G. L. Miller 在 1975 年指出,利用 $\varphi(n)$ 的任何倍数都可以容易地分解出 n 的因子. 因此,用 Miller 算法就可以由 $(ed-1)$ 分解出 n 的因子,也就是说计算 d 并不比分解 n 的因子更容易. 密码分析员还可能希望找到某个与 d 等价的 d',从而攻破 RSA 密码. 但是,所有这样的 d' 只相差 $(p-1)$ 和 $(q-1)$ 的最小公倍数的整数倍,因此,找到一个这样的 d' 就可以使分解 n 的因子问题变得容易起来,也即找到这样的 d' 并不比分解 n 的因子更容易.

综上所述,破译 RSA 密码系统和分解因子问题同样困难,尽管目前还不能完全证实它,即在目前状况下,如果参数 p,q 和 e 选取恰当的话,RSA 的加密强度,就取决于的抗因子分解强度.

3　大数因子分解的难度

著名数学家费马(1601—1665)和勒让德((1752—1833)都研究过分解因子的算法,现代某些更好的算法是勒让德方法的扩展. 其中,R. Schroeppel 算法是好算法中的一类,用此法分解因子仍然需要大约 $e\sqrt{\ln n \ln\ln n}$ 次运算,其中 ln 表示自然对数,可见分解 n 所需的运算次数与密钥的长度有关,随着密钥长度的增加,分解所需的时间会成指数倍增加. 对于不同长度的十进制数 n,Schroeppel 算法分解 n 的因子时所需的运算次数如表 1 所示.

表 1　用 Schroeppel 分解因子算法的运算次数表

数 n 的十进制位数	50	100	200	300	400
运算次数	1.4×10^{10}	2.3×10^{15}	1.2×10^{23}	1.5×10^{29}	2.7×10^{34}

若用 1 台 1 s 能进行 1 亿次因子分解的高速计算机来计算,分解十进制长度为 200 位的 n,其所需时间为 3 800 000 年. 由此可见,对于 RSA 系统,如果用一个长度为 200 位(十进制)的 n,认为它是比较安全的,如果 n 的长度更长,因子分解越困难,一般来说,每增加 10 位二进制数,分解的时间就要加长 1 倍. 密码就越难以破译,加密强度就越高.

不过随着计算机运算速度的提高和并行计算的发展,破解的速度也会同步提高,这时可能要求使用更长的密钥.70年代末,RSA算法的3个发明人曾经提出一道RSA129挑战问题.在其后的近20年里,该问题竟然无人敢于问津,密底似乎将永远不会揭开.1993年,在美国Bellcore公司Arjen Lenstra,Derek Atkins,Michael Graff和Paul Leyland的领导下,一个国际研究小组决定接受16年前Rivest教授等人在《科学美国人》杂志上提出的挑战.他们之所以能这样做,主要因为近20年来,计算机运算速度突飞猛进的提高,在大数分解理论上也有新的突破.该小组在国际互联网上集合来自世界各地的志愿参加者,向他们分发因数分解软件.这个分解软件可以利用计算机的空闲时间进行RSA129的公开钥匙分解工作,可以自动避免与用户工作时间的冲突.每个参加者都领取了不同的因数分解子任务,在自己的计算机上独立运算,然后把计算结果寄回MIT总部,列表归纳.到1994年4月,共有600余名志愿者参加了这项破译活动.他们总共动用了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RSA129问题中的公开钥匙.在2005年有研究人员破解了RSA640问题中的公开钥匙[5].不过破解的难度随着n长度而不断增加,因此可以根据被加密文件的重要程度及对加密时间的要求这2个因素来选择n的长度,这种选择密钥长度的灵活性(密钥长度决定保密的等级)是许多密码系统所没有的,是RSA算法的一个特点.通常选取n=512,1 024,2 048 bit.就目前的计算机水平用1 024位二进制(约340位十进制)的密钥是安全的,2 048位是绝对安全的.RSA实验室认为,n=512已不够安全,应停止使用,目前个人需要用n=668,公司要用n=1 024,极其重要的场合应该用n=2 048.

4 结语

RSA的安全性依赖于大数的因子分解,这样攻击RSA系统的难度就是大整数因子分解的难度,一般认为这是一个NPC问题,尽管尚未在理论上证明分解因子的问题一定困难,但千百年来经过众多学者的研究,迄今没有找到一种有效算法,绝大多数数论学家倾向于认为不存在大整数因子分解的多项式算法,因此目前这一破译只能依赖于现代的计算机技术,用程序进行尝试分解,从而对大数的因子分解.不过随着计算机运算速度的提高和并行计算的发展,加上因子分解方法的改进,低位数的密钥的破解已成为可能.因子分解需的时间随密钥长度的增加而成指数指增加,只要n的长度达到一定要求,并且参数p,q和e选取恰当的话,RSA系统是相当安全的.

参考文献:

[1] 夏 煜,郎荣玲,戴冠中,等.基于图像的信息隐藏分析技术综述[J].计算机工程,2003,29(7):1-3.
[2] 邱 梅,罗守山,刘 文.利用RSA密码体制解决安全多方多数据排序问题[J].电子学报,2009,27(5):1 119-1 123.
[3] 姜正涛,怀进鹏,王育民.RSA推广循环攻击实效性与弱模问题的研究与分析[J].通信学报,2009,30(6):70-74.
[4] 谢建全,阳春华.RSA算法中几种可能泄密的参数选择[J].计算机工程,2006,32(16):118-120.

Security Analysis of RSA Encryption Algorithm

XIANG Jin
(Xiangxi Economic and Trade School,Jishou 416000,Hunan China)

Abstract:Recently,RSA encryption algorithm is a widely used asymmetric encryption algorithm with high security. Mathematic basis of RSA encryption algorithm which belongs to asymmetric encryption system is analyzed. Possible methods to decrypt it are discussed as well. Then,according to recent running speed of computer,time for decryption by using a normal length of key is calculated. Besides,quantitative analysis of security of RSA algorithm is implemented.

Key words:RSA;data encryption;data security;key decryption

(责任编辑 陈炳权)