云南大学学报 (自然科学版), 2004, 26 (3): 212～215 CN 53 - 1045/ N ISSN 0258 - 7971
Journal of Yunnan University

RSA 加密体制的安全隐患*

杨维忠[1], 李 彤[2], 郝 林[1]
(1. 云南大学 计算机科学系, 云南 昆明 650091; 2. 云南大学 软件学院, 云南 昆明 650091)

摘要: 详述了 RSA 算法, 给出了 RSA 加解密的算法以及它的抗攻击能力分析表, 而且总结了常见的攻击方式, 最后分析了在实际应用中存在的一些弊端.

关键词: RSA; 公钥密码体制; 安全性
中图分类号: TP 309.7 **文献标识码**: A **文章编号**: 0258 - 7971(2004)03 - 0212 - 04

自从人类文化诞生以来, 就产生了保护敏感信息的愿望. 在现代社会, 随着 Internet 的发展, 人们越来越多地在网络上从事个人事务处理和商业活动, 如利用网络发送电子邮件进行电子购物、资金转账、发布公告、接收重要数据等. 网络已经发展成人们日常生活和工作的重要媒体, 其信息安全性随之变得越来越重要. 这个问题已经引起了各国政府的广泛重视. 而加解密技术又是最经济实用的技术, 因为好的加解密算法能在不安全的传输环境(如 Internet)中提供安全的服务.

密码算法的目的是为了确保信息的保密性、完整性和安全性. 密码学的鼻祖香农[1]提出了一些概念和基本理论, 论证了只有一种密码算法在理论上是不可解的, 那就是 One Time Padding[2]. 其它算法在理论上都是可解的. 如 DES 算法, 其密钥实际长度是 56 比特, 作 2^{56}次穷举, 就肯定能找到加密使用的密钥. 密码学在不断发展变化之中, 因为人类的计算能力也像摩尔定律提到的一样飞速发展.

1 RSA 算法

RSA 算法是第 1 个能同时用于加密和数字签名的算法, 易于理解和操作[3]. RSA 是受到最广泛研究的公钥算法, 算法的名字以发明者: Ron Rivest, AdiShamir 和 Leonard Adleman 的名字命名. 从提出到现在已 20 多年, RSA 算法经历了各种攻击的考验, 已为人们接受, 普遍认为是目前最优秀的公钥方案之一. RSA 的保密性基于一个数学假设: 对一个很大的合数进行质因数分解是不可能的. RSA 的安全性依赖于大数的因子分解, 但并没有从理论上证明破译 RSA 的难度与大数分解难度等价. RSA 用到的是 2 个非常大的质数的乘积, 目前的计算机水平无法分解, 但是这并没有"证明" RSA 的安全性, 也就是说这不能说明分解这个大数是攻击 RSA 唯一的(或者说是最佳的)途径, 也不能证明这种分解真的那么困难.

1.1 RSA 的密钥生成步骤

①找到 2 个大质数 p, q;
②做乘法 $n = p * q$;
③选择一个数 e, 满足 $e < n$ 且与 $(p - 1) * (q - 1)$ 互质;
④计算 $d = e^{-1} \bmod [(p - 1)(q - 1)]$;
⑤ e 就是公开指数, d 是私密指数;
⑥公匙就是 (n, e), 私匙是 (n, d);
⑦销毁 p 和 q.

加密算法是这样的, 把明文分成比 n 小的数据块用公开指数作乘方取模运算

$c = m^e \bmod n$ (m 是明文块(message), c 是密文块(cipher)).

解密过程正相反, 把密文数据块用私密指数作

* 收稿日期: 2003 - 09 - 09
基金项目: 云南省自然科学基金资助项目(2002F0010M); 云南省科技攻关项目(2001I710); 云南省省校省院合作项目(2001AABLA002).
作者简介: 杨维忠(1978 -), 男, 云南人, 硕士生, 主要从事计算机密码学方面的研究.

乘方取模运算

$m = c^d \bmod n$.

攻击者有公匙,就是 e 和 n,想获得私匙,换句话就是 d. 对 n 进行因数分解来获得 p, q 从而算出 d 是最好的攻击方法,直接穷举 d 或推断 $(p-1)(q-1)$ 都要慢许多[4].

1.2　几种因数分解的算法

①试探除法:最古老也是最笨拙的方法,穷举所有小于 sqrt(n) 的质数,耗时以指数率增长.

②二次筛法(QS)[5]:对 10^{110} 以内的数是最快的算法.

③MPQS:QS 的改进版本,速度要快一些.

④分区筛法(NFS)[6]:目前对大于 10^{110} 的数是最快的算法. 曾被用来成功地分解过第 9 费马数.

这些算法代表了人们对大数分解(也就是对 RSA 攻击)的探索历程. 最好的算法具有超多项式率(亚指数率)的时间复杂度,NFS 具有最接近于多项式率的表现.

大数分解仍然是困难的,但随着数论的发展和计算能力的增强而变得容易了. 1977 年, Ron Rivest 说过分解一个 125 位的数需要花费 4×10^{13} a. 在 1994 年 RSA129 被分解了,花费了 5 000 MIPS·a 的机时,是利用 Internet 上一些计算机的空闲 CPU 周期一共花了 8 个月完成的. 1995 年, Blacknet 密钥被分解,用了几十台工作站和 1 台 MarPar,共用 400 MIPS·a,历时 3 个月. 随着时间的推移,可能被分解的密钥长度还会增加. 表 1 是常用的几种 RSA 密钥长度(PGP 精选出的)与其对应的 NFS 分解算法所耗费的时间.

表 1　NFS 因数分解时间表

Tab. 1　Timetable of NFS factoring

密钥长	NFS 分解算法耗费的时间/MIPS·a
512	30 000
768	200 000 000
1 024	300 000 000 000
2 048	300 000 000 000 000 000 000

RSA 的安全性依赖于大数分解的难度. 因此需要一些产生非常大的质数的方法. 目前还没有一种迅捷的产生一个大质数的算法. 因此,实际采用的方法是产生一个大奇数,然后测试它的质数性.

1.3　大素数的选取(确定密钥)　为了测试一个数的质数性,最显而易见的方法是作试探除法:将 n 用 2 到 sqrt(n) 的每个整数来除. 如果 n 是质数,所有这些数都不能整除它. 如果 n 是质数的话,这个算法的耗时是指数方式增长的,这对需要测试的大数来说太不经济了. 从这里也可以看出,试探除法不是一条可行的 RSA 攻击道路.

实际可以采用的方法是对候选奇数做费马测试(用必要条件来代替充分条件). 费马测试并不能确定它是否质数,但通过费马测试以后的数不是质数的概率大大降低. 下面是费马测试的细节:

①待测奇数 n;

②在质数集合中依次选取一个质数 b, $b = 2, 3, 5, 7 \cdots\cdots$;

③计算 $w = b^{(n-1)} \% n$;

④如果对于所有 b, w 都为 1, n 很可能是质数. 否则 n 一定是合数.

取前 4 个质数的测试称为四阶费马测试,也是 PGP 所采用的方法. 一阶测试误判的概率是 10^{-13},二阶后为 10^{-26},完成四阶测试后是 10^{-52}. 它绝对不会漏掉一个质数,但将合数误判为质数的可能性是存在的. 这种能通过费马测试的合数被称为 Carmichael 数,如:561, 1 105, 1 729 等等. 这样的数很稀少,但它们是不安全的[7].

2　几种针对 RSA 的有效攻击方法

2.1　选择密文攻击[8]　由于 RSA 密文是通过公开渠道传播的,攻击者可以获取密文. 我们假设攻击者为 A,密文收件人为 T,A 得到了发往 T 的一份密文 c,他想不通过分解质因数的方法得到明文. 换句话说,他需要 $m = c^d$.

为了恢复 m,他找一个随机数 r, $r < n$,当然他有 T 的公匙 (e, n). 他计算

$x = r^e \% n$ (用 T 的公匙加密 r),

$y = x * c \% n$ (将临时密文 x 与 c 相乘),

$t = r^{-1} \% n$.

A 知道 RSA 具有下面的一个特性

如果 $x = r^e \% n$,那么 $r = x^d \% n$.

因此他想办法让 T 对 y 用 T 自己的私匙签名(实际上就是把 y 解密了),然后将结果 $u = y^d \% n$ 寄回给 A. A 只要简单地计算

$m = t * u \% n$.

上面结论的推导是这样的

$$t * u \%n = (r - 1) * (y^d) \%n = (r^{-1}) * (x^d) * (c^d) \%n = (c^d) \%n = m.$$

2.2 过小的加密指数 e[9] 从计算速度考虑,e 越小越好. 可是,当明文也是一个很小的数时就会出现问题. 例如我们取 $e = 3$,而且我们的明文 m 比 n 的 3 次方根要小,那么密文 $c = m^e \%n$ 就会等于 m^3. 这样只要对密文开 3 次方就可以得到明文.

2.3 RSA 的计时攻击法 这是一种另辟蹊径的方法. 不难发现,RSA 的基本运算是乘方取模,这种运算的特点是耗费时间精确,运算时间主要取决于乘方次数. 这样如果 A 能够监视到 RSA 的解密过程,并对它计时,他就能算出 d 来. 在这里提出这种攻击是因为虽然它目前还不实用,但从理论上是一个崭新的思路,值得注意.

2.4 RSA 的公共模数攻击[10] 若系统中共有一个模数,而不同的人拥有不同的 e 和 d,系统的安全性将受到威胁. 最普遍的情况是同一信息用不同的公钥加密,这些公钥共模而且互质,那么该信息无需私钥就可得到恢复. 设 P 为信息明文,2 个加密密钥为 e_1 和 e_2,公共模数是 n,则

$$C_1 = P^{e_1} \bmod n,$$

$$C_2 = P^{e_2} \bmod n.$$

密码分析者知道 n, e_1, e_2, C_1 和 C_2,就能得到 P. 因为 e_1 和 e_2 互质,故用 Euclidean 算法能找到 r 和 s,满足

$$r * e_1 + s * e_2 = 1,$$

假设 r 为负数,需再用 Euclidean 算法计算 C_1^{-1},则

$$(C^{-1})_1 - r * C_2^s = P \bmod n.$$

总之,如果知道给定模数的一对 e 和 d,一是有利于攻击者分解模数,二是有利于攻击者计算出其它成对的 e 和 d',而无需分解模数.

3 RSA 的安全性展望

如文中说所,RSA 的安全性依赖于大数分解的难度. 那么以下 3 种技术的发展会威胁到 RSA 的安全性:

(1) 分解技术. 如果因素分解技术有了突破性发展,那么 RSA 的破解将会变得非常简单,可以直接计算出私钥;

(2) 计算机能力的提高. 对于同一种攻击方法,如果计算机的计算能力提高了,那么它的攻击力必然有所提高;

(3) 计算机造价的降低及并行技术的发展. 如果并行技术进一步提高,且计算机的造价不断降低,就可以用大量的计算机组成一个网络进行并行计算,使计算能力达到超级计算机的能力,那么攻击能力将会得到巨大增长.

4 RSA 加密体制的弊端

(1) 产生密钥很麻烦,受到素数产生技术的限制,因而难以做到一次一密;

(2) 分组长度太大,为保证安全性,n 一般要在 1 024 bits 以上,不但运算代价很高,而且速度较慢,较对称密码算法慢几千倍;且随着大数分解技术的发展,这个长度还在增加;而且随着安全级别的提高,密钥的长度在急剧增加,不利于数据格式的标准化;

(3) 通信带宽要求较高,影响了它的应用价值. 为了保证安全性,它的密钥太长,在通信过程中要求的带宽较大,这特别不适用于对小数据量高频率交换的信息加密,如电话语音、网上聊天等等.

5 解决办法

(1) 可以采用新的公钥密码体制,如椭圆曲线公钥密码体制,可参考笔者近期文章;

(2) 可以进一步提高 RSA 算法的加解密效率,已达到能够在用户可以接受的时间内提供给用户更长的密钥以保证用户信息的安全.

参考文献:

[1] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28: 656—715.

[2] KAHN D. The codebreakers: the story of secrete writing [M]. New York: Macmillan Publishing Co, 1967.

[3] RIVEST R L, SHAMIR A, ADLEMAN L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120—126.

[4] WU C K, WANG X M. Determination of the true value of the euler totient function in the RSA cryptosystem from a set of possibilities[J]. Electronics Letters, 1993, 29(1): 84—85.

[5] POMERANCE C, SMITH J W, TUIER R. A piple-line

architecture for factoring large integers with the quadratic sieve algorithm[J]. Siam Journal on Computing,1988,17(2):387—403.

[6] LENSTRA A K,LENSTRA H W. Lecture notes in mathematics 1554: The development of the number field sieve[D]. New York:Springer-Verlag,1993.

[7] HULE H,MULLER W B. On the RSA cryptosystem with wrong keys[A]. Contributions to General Algebra 6[C]. Vienna: Verlag Holdeer-Pichler-Tempsky,1988. 103—109.

[8] DESMEDT Y,ODLYKZO A M. A chosen text attack on the RSA cryptosystem and some discrete logarithm problems[A]. Advances in Cryptology - CRYPTO'85 Proceedings[C]. New York: Springer-Verlag, 1986. 21—39.

[9] HASTAD J. On using RSA with low exponent in a public key network[A]. Advances in Cryptology-CRYPTO'85 Proceedings[C]. New York: Springer-Verlag,1986. 403—408.

[10] DELAURENTIS J M. A further weakness in the common modulus protocol for the RSA cryptosystem[J]. Cryptologia,1984,8(3):253—259.

Hidden security flaws of RSA encryption system

YANG Wei-zhong[1], LI Tong[2], HAO Lin[1]

(1. Department of Computer Science, Yunnan University, Kunming 650091, China;
2. School of Software, Yunnan University, Kunming 650091, China)

Abstract: It is explicated the theory of RSA, and presented the RSA algorithms. Also, it is analysed RSA's ability against attack, and summarized the ordinary ways of attack. Finally, it is explored the flaws of RSA system in practical use.

Key words: RSA; public key cryptography; security

* *

(上接第 211 页)

The application of SCM on astronomical telescope automatic tracking objects of celestial bodies

ZHOU Yan[1], SHEN Dong-ya[2]

(1. Department of Signal and Electro-engineering, Yunnan University, Kunming 650091, China;
2. Department of Communication Engineering, Yunnan University, Kunming 650091, China)

Abstract: Using SCM to control astronomical telescope automatic tracking objects of celestial bodies could replace manual running work by key-press operation. It has the characteristics of small volume, low cost and portable. The theories of automatic tracing, first of all, is manual tracking, so as to capture the rules of object movement and note down the tracks, and based on it to calculate the moving steps of step control, and finally, by controlling the running of step control which drives astronomical telescope running to reach the goal of automatic tracking.

Key words: SCM; astronomical telescope; automatic tracing