RSA算法参数的选择

覃白
(长江师范学院应用技术学院 重庆涪陵 408000)

摘 要:RSA算法由Ronald.LRivest,Adi.Shamir和Leonard.M.Adleman三人发明的,根据三人名字首字母组合来命名的。由于其既可用于加密,也可以用来做数字签名,用途比较广泛;在应用方面简单易于编程和实现,所以RSA算法在密码学领域经久不衰。但RSA算法的加密强度很大程度依赖于RSA算法中的参数。本文主要分析应该如何选择RSA算法中的参数,才能保证RSA算法的安全性。
关键词:RSA算法 参数 加密强度 安全性
中图分类号:TP3 文献标识码:A 文章编号:1672-3791(2010)10(a)-0010-01

1 RSA算法简介

RSA算法属于分组密码体制的。我们把名文用M表示,把密文用C表示,公钥参数用e表示,私钥参数用d表示,则RSA算法可以描述为如下。

加密:$C=M_e \bmod n$

解密:$M=C_d \bmod n$

其中n为两个大素数的乘积。计算出两个大素数的乘积容易,但是要分解n为两个大素数是非常困难的,这就是RSA算法安全性的核心。

参数解释如下。

(1)选取两个大素数p和q。

(2)计算n=pq。

(3)随机选取e,且满足$1<e<\Phi(n)$,$\gcd(e,\Phi(n))=1$。$\Phi(n)=(p-1)(q-1)$。得到公钥就是e和n。

(4)通过$ed=1 \bmod \Phi(n)$,计算d。那么公钥就是d和n。

2 RSA参数的选择

RSA算法的安全性主要依赖于RSA参数的选择,因此需要对这个算法中的各个参数仔细选择。

(1)p,q选择强素数,否则不能防御某些特殊的因子分解方法。

假设p,q不是强素数。可以假设p-1没有大的素因子,$p-1=p_1^{a1}\cdots\cdots p_m^{am}$,其中$p_i$为素数,$a_i$是自然数($1\leqslant i\leqslant m$)。可以设$p_i<A$($1\leqslant i\leqslant m$),A为一较小的整数,此时分解n就比较容易。我们可以设$a\geqslant a_i$($1\leqslant i\leqslant m$),可以构造$B=p_1^a\cdots\cdots p^{ma}$,此时必有$(p-1)\mid B$。由费马定理知道,$2^B=1 \bmod p$,又因为有$(p-1)\mid B$。我们如下处理$x^B=y \bmod n$,可以把xB看成是p的某整数倍加1。如果$2^B=y \bmod n$中,y=1,则把x换成3……,直到$y\neq 1$。那么,$\gcd(y-1,n)=p$,因为y应该为p的某整数倍加1。由此可以求出p与q。

(2)p与q之差要比较大,否则$n\approx(p+q)^2/4-(p-q)^2/4$。也就是说$n^{0.5}$接近$(p+q)/2$,逐个找比n0.5略大的自然数N,到使$(N^2-n)$是一个完全平方数。可以设$x^2=N^2-n$,则$n=N^2-x^2=(N+x)(N-x)$,则$p=N-x$,$q=N+x$。

(3)$p^3/1$与$q^3/1$的最大公因子应很小,否则,RSA有可能在不需要因子分解时即可被攻破,$p^3/1$与$q^3/1$都应包含大的素因子。

(4)p,q应该足够大,使得在计算上分解n是不可能的。

(5)$\gcd((p-1),(q-1))$小。否则,可以采用迭代方法。对密文$C=M^e \bmod n$反复进行e次幂的运算。c^e,c^{ee},……,到出现c的et次幂mod n为c时为止。则c的e^{t-1}次幂mod n为M,当t不是很大时,这种攻击是有效的。由Eluer定理知$e^t=1 \bmod \Phi(n)$,同样由Eluer定理,t的最小值有$t=\Phi(\Phi(n))=\Phi((p-1)(q-1))$,如果$\gcd((p-1),(q-1))$小,$\Phi(\Phi(n))$就很大,t就会很大。

(6)e不可选择过小,加密速度快但可以采用低指数攻击。在$C=M^e \bmod n$中,如果e选择过小,可能没有模n的运算,可以通过直接开平方得到。一般选择使$e^i=1 \bmod \Phi(n)$中的i尽可能大的e。

(7)密钥d的选取是最为关键的,应使$d>N^{0.25}$且越大越好,这是因为当d的长度小于N的长度的0.25倍时,攻击者可能通过连分数方法在多项式时间内求出d,而当$d>N^{0.25}$时,攻击者只能采用穷举攻击法,若d较小,则显然破译困难远比大因子分解的难度小,系统被直接攻破的可能性较大。另外,d又不能太接近e,否则RSA密钥系统较容易被攻破,因为攻击者最喜欢从比较小的数和e附近进行攻击。

(8)用户不能使用相同的模n,否则任一用户的n被分解,可通过其他用户的公钥求出其私钥。

(9)明文M的熵要尽可能大,使得在已知密文的情况下,要猜测明文的内容几乎是不可能的。

由以上所述,RSA的全部保密性依赖于$N=p\times q$的分解的难度计算,是一个大因子分解问题,但是,目前并不能从理论上证明这一点。而从实践的角度说,$N=p\times q$的分解可使系统完全被解密。再有,即使N未被分解,若参数选择不当,攻击者也完全可能在可以接受的时间内解密,主要原因是明文和密文以及N和e提供了另外一些破解信息。因此,破译RSA不可能比大因子分解更困难。

3 结语

RSA算法仍然是现在使用地比较广泛的一种算法,其安全性很大程度上依赖于参数的选择。本文主要讨论了如何合理选择RSA算法中的参数。在参数选择比较合理的情况下,破译系统的难度相当于将两个大素数之积重新分解为两个大素数的难度。

参考文献

[1] 王玉英,王昭顺.信息安全中的公钥密码软件-大整数模拟实现[J].微计算机信息,2004,20(9):121~122.
[2] 赖溪松.计算机密码学及其应用[M].北京:国法工业出版社,2001.
[3] (德)BauerF.L.密码编码和密码分析原理与方法[M].北京:机械工业出版社,2001.
[4] 景旭.基于混合加密的即时通讯系统设计与实现[J].西北农林科技大学学报,2007,(10):229~234.