文章编号:1673-0062(2018)02-0070-04

RSA 加密算法改进的研究及实现

余新宏,陈 琦,严 宇

(安徽农业大学 经济技术学院,安徽 合肥 230011)

摘 要:RSA 算法的安全性依赖于模幂和模乘运算,但是由于模幂运算太耗时间,一直使得 RSA 算法难以广泛应用,因此如何提高 RSA 运算中的模幂、模乘运算速度至关重要.对 RSA 加解密基本原理进行了相应的分析,并结合当前针对 RSA 算法的攻击手段,提出抵御这些攻击所应考虑的因素,从而对传统的 RSA 算法进行了进一步的改进.

关键词:RSA;算法研究;模乘运算

中图分类号:TP312 **文献标志码**:A

Research and Realization of the RSA Encryption Algorithm Improvment

YU Xin-hong, CHEN Qi, YAN Yu

(Economy and Technology Institute, Anhui Agricultural University, Hefei, Anhui 230011, China)

Abstract: The modular exponentiation and modular multiplication are essential elements to secure RSA algorithm. However, modular exponentiation has been so time-intensive that it impedes RSA algorithm's application. Therefore, it is paramount to enhance the efficiency of modular exponentiation and multiplication. This paper aims to improve RSA algorithm by analyzing the principle of RSA encryption, discussing attacks against RSA algorithm, and suggesting the factors to be considered when resisting attacks.

key words: RSA; algorithm research; mold by operation

0 引 言

随着信息网络的快速发展,越来越多的人利用网络共享信息、搜索资料、进行商业交易,因此信息的保密显得尤为重要.公钥密码体制的出现对现代密码体系的发展起到了十分重要的作用,而 RSA 算法是目前使用较广泛、安全性也相对较高的非对称加密算法.RSA 算法的主要能实现加密、身份验证和数字签名等功能,是一种典型的公钥密码体制.

收稿日期:2018-01-04

基金项目:安徽省高校自然科学研究重点项目资助(KJ2016A246);安徽省质量工程教学重点研究项目(2016jyxm0327);安徽省质量工程统计学教学团队项目(2017jxtd134)

作者简介:余新宏(1982-),男,副教授,硕士,主要从事数理统计方向的研究.E-mail:yxh229913@126.com

1　RSA 算法

1.1　RSA 加密算法

RSA 算法实现加密或解密变换通常有以下几个步骤.

1)密钥的产生

①选择两个保密的大素数 p 和 q.

②计算 $n=pq, t=(p-1)(q-1)$　　(1)

其中 t 是 n 的欧拉函数值.

③选择一个整数 e,满足 $l<e<t$,且

$$\gcd(t,e)=1 \tag{2}$$

(gcd 函数是求最大公约数)

④计算私钥 d(解密密钥),满足 $e\cdot d=1 \bmod t$,d 是 e 在模 t 下的乘法逆元.

⑤以 $\{e,n\}$ 为公开钥,$\{d,n\}$ 为秘密钥.

2)RSA 算法实现加密

在进行加密之前应先对明文进行分组,使每个分组的长度小于 n,在计算机中指每个分组的二进制长度小于 $\log 2n$.之后再对每个明文分组 m,作加密运算[1]:

$$C=me \bmod n \tag{3}$$

3)RSA 算法实现解密

对得到的密文分组的解密运算为:

$$m=cd \bmod n \tag{4}$$

1.2　RSA 签名算法

一般来说如果一个公开密钥体制若作为密码系统,那么他不能同时作为数字签名,反之亦然.只有很少的加密体制可以同时用于密码系统和数字签名[2],本文所讨论的 RSA 算法是其中之一.RSA 签名算法如下:

设 $n=pq$,且 p 和 q 是两个大素数[3],e 和 d 满足

$$ed=l(\bmod t). \tag{5}$$

公开密钥:n,e

私有密钥:d

进行签名:$Y=Xd \bmod n$;并将加密后的信息和签名 Y 再发送给接收方;

进行验证:接收方使用发送方的公钥 e 对收到的消息 y 进行数字签名验证变换 $X'=ye \bmod n$[1],并使用发送方的保密的私钥对收到的信息进行解密,只要得到 $X'=X$ 的结果就可以确定发送方的身份合法.

以上过程基本可以实现 RSA 算法的数字签名功能,但必须注意的是用户想要实现此功能首先必须要公开他自己的公玥,这样别的用户才能对他的签名进行验证,否则其他用户无法验证此的正确性.

通过对 RSA 算法的分析,本文将对 RSA 算法从参数的选择进行改进,阐述了 RSA 算法实现的条件,以及具体实现的程序过程.

2　RSA 参数选择

根据 RSA 算法加解密过程,它所涉及的主要参数有三个:模数 n,加密密钥 e 和解密密钥 d.

2.1　n 的选取

在 RSA 算法中,n 是由 P 和 q 的乘积,再通过运算得到密钥对.对于模数 n 的因数分解就是最直接的攻击方法,如果 n 被分解那么信息就会被窃取[4].由此看来对于模数 n 的选择十分重要,通常 n 的确定要满足以下几个条件:

1)p 和 q 之差要大.

但如果选取 p 和 q 相差很小时,在已经知道 n 的前提下,可以假设二者的平均值为 $(p+q)/2$ 为 $n/2$,然后利用 $((p+q)/2)^2-n=((p-q)/2)^2$,若等式右边可开方,则得到 $(p+q)/2$ 和 $(p-q)/2$ 即 n 被分解[6].

2)$p-1$ 和 $q-1$ 的最大公因子应很小.

3)p 和 q 必须为强素数.

素数 p 如果满足:存在两个大素数 p_1,p_2,使 $p_1/p-1$ 和 $p_2/p+1$ 同时成立或者存在四个大素数 r_1,r_2,s_1,s_2,使 $r_1/p_1-1, s_1/p_1+1, r_2/p_2-1, s_2/p_2+1$ 都成立,则此素数为强素数.只有当 n 是由两个强素数的积所构成的,它的因子分解才是难以解决的数学难题.

4)p 和 q 应该足够大到使得因子分解 n 为计算上不可能.

RSA 算法主要依靠大数的因子分解来实现其安全性,如果模数 n 能被因子分解,则相当于算法被攻破,因此模数 n 的选择一定要足够大使得 n 的因子分解在计算上是不可能实现的[5].因子分解问题是密码学中最常见的难题之一,虽然现在因子分解的算法有了很大进步,但仍没有足够的证据来证明 RSA 是可以被破解的.同时为了保证 RSA 算法有足够的安全性,则素数 p 和 q 至少应该选取 300 位以上的二进制数,故相应的模数 n 就是 600 位以上的二进制数[5].现在大多数实体采用的是 1 024 bit 的密钥,随着计算能力的提高安全密钥的长度也是随之增长的.

2.2　e 的选取

e 和 t 互素的条件比较容易满足,如果选择的 e 比较小的话,就加快了加解密运算的速度,同时也容易存储,但也降低了安全性.

一般地,e 有以下选取原则:

1)e 不可以选择太小的数.在 RSA 算法中,只要公开密钥 e 可以满足 gcd $(e,t)=1$ 即可,说明参数 e 可以任意选取,为了减少运算时间,多数人会选择比较小的 e 值[6],但低指数会大大降低整个算法的安全性.因此,一般 e 的选择应为一个 16 位的素数,这样可以有效防止安全攻击,而且运算速度也较快.

2)应使 e 在 mod t 的阶为最大.即存在 i,使得

$$ei = 1(\mathrm{mod}\ t) \tag{6}$$

其中 i 大于 $(p-1)*(q-1)/2$,可以有效抗击攻击.

2.3 d 的选取原则

私密密钥 d 不能过于小,一般至少要大于 $n/4$.这是因为:如果 d 的长度过于小,那么利用已知明文 m 加密后可以得到 $c=me \bmod n$,之后可以直接猜测出 d.求 $cd \bmod n$ 是否等于 m.若是,则 d 就是解密密钥,不是则继续猜测.如果 d 的长度过小,则猜测的范围很小,猜中的概率很大.综合以上原因 d 长度不能过小.

3 RSA 算法的实现

3.1 素数的产生

对于素性的测试通常是概率测试(结果不一定是 100%的正确),但是随着这个数测试次数的增加它测试结果的正确性也在增加.常见的检验方法有费马素性检验、米勒拉宾测试 、Solovay-Strassen 测试、卢卡斯-莱默检验法,后三种都是在费马测试的基础上建立的.

在常用的产生素数的算法中,首先是生成一个大整数,再用素性测试判断它是否为素数[6],如果不能通过素性测试判断,则令它加 2 再进行判断,直至其通过判断为止.一些特殊形式的强素数,虽然能够防止一些简单的攻击手段,但是需要花费很多的时间,因此对于 RSA 算法来说选择一个足够大的素数更加重要.

3.2 密钥的产生

RSA 算法属于公玥密码体制,拥有一对密钥(公玥和私钥).随机选择一个加密密钥 e,判断它是否与 t 互为素数.

判断两数互素的方法:首先判断两数的最大公约数(用 gcd 函数来实现)是否为 1,若是则两数互素.由欧几里得算法可知,若 $a=bn+c$ 那么 $\gcd(a,b)=\gcd(b,c)$,故可用每次操作所得余数和原本的除数做重复计算,最后所得的非零余数即为最大公约数.

产生公玥过程如图 1 所示.

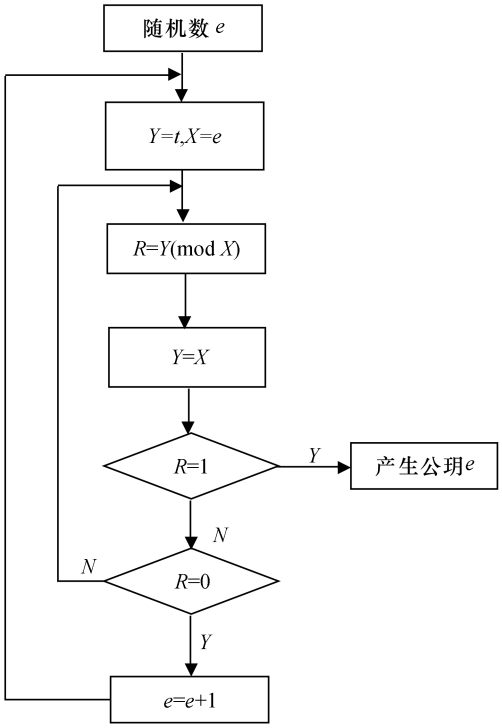

图 1 公玥流程图

Fig.1 Public key flow chart

由以上过程得出加密密钥后,根据上文中提出的 $e \cdot d=1 \bmod t$ 公式即可算出解密密钥 d.

3.3 SMM 乘模算法

在 RSA 算法中最核心的就是乘模运算,因为 RSA 算法中大部分的运算都是幂模运算,而幂模运算转化为平方模运算和乘模运算.对于 RSA 算法改进本文采用 SMM 算法主要是依据“乘同余对称特性”来减少每次操作运算的基数,从而减少了乘模运算时间提高了运算速度.

在 RSA 算法中,n 是两个大素数的积,那么 n 必然是奇数,$n-1$ 和 $n+1$ 必然是偶数,所以 $(n-1)/2$ 和 $(n+1)/2$ 肯定是整数[6].根据模运算的性质可知 $(n-i)(n-j)=n^2-ni-nj+ij=ij(\mathrm{mod}\ n)$ $(i,j \in \{0,1,2,\cdots,(n-1)/2,(n+1)/2,\cdots,n-1\})$,在 RSA 算法幂模运算中可以把较大的数转化为较小的数进行平方模运算和乘模运算,从而可以加快其运算速度.

3.4 RSA 算法改进的具体实现

实现过程中用到的计算公式和函数:

①求两数互素即两数的最大公约数为 1,利用 gcd 函数来实现.

②模运算即求余运算,

$$a = b(\bmod n) \Leftrightarrow a = b\%n \tag{7}$$

③求一个数 a 的模 n 逆元 b 的计算公式为

$$ab = 1 \bmod n \tag{8}$$

根据欧几里德算法,相当于计算 $ab = n * k + 1$ (k 为自然整数),找出满足公式的 k 和 b 即可.

首先选择两个随机大素数 p 和 q(保密),计算 $n = p * q$,$t = (p - 1)(q - 1)$,根据上文提到的 $\gcd(t,e) = 1$ 和图 1 产生公玥 e(公开的).再由 $e \cdot d = 1 \bmod t$ 计算私钥 d(保密).$\{e,n\}$ 为公开钥,$\{d,n\}$ 为秘密钥.对每个明文分组 m 做加密算法:$c = me \bmod n$,在对每个密文分组 c 做解密算法:$m = cd \bmod n$.

RSA 算法主要程序运行结果如图 2 和图 3 所示.

图 2　加密运算结果

Fig.2　Encryption operation result

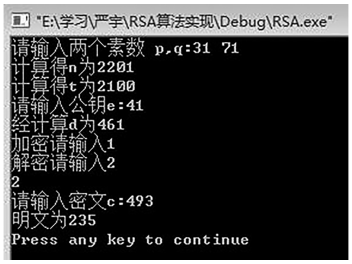

图 3　解密运算结果

Fig.3　Encryption operation result

4　结果分析及说明

通过图 2,图 3 比较可看出,RSAS 算法改进前,程序运行结果表明,第一次随机选的 e 不符合规则,实现不了对于公玥选择的纠正功能;按照上文采用的 RSA 加密算法改进的程序实现过程,加密或解密的选择以及明文和密文的输出结果,并进一步验证了 RSA 算法改进的正确性.

参考文献:

[1] 赖溪松,韩亮,张真诚.计算机密码学及其应用[M].3 版.北京:国防工业出版社,2013.

[2] 李红军,缪旭东.数据加密在网络安全中的应用[J].微型机与应用,2002,21(10):31-33.

[3] 李文峰,周晓东,戴剑勇.基于 GA-FUZZY 的投资组合满意度优化研究[J].南华大学学报(自然科学版),2009,23(2):50-54

[4] 周玉洁,冯登国.公开密钥密码算法及其快速实现[M].3 版.北京:国防工业出版社,2012:1-144.

[5] 施奈尔.应用密码学[M].4 版.北京:机械工业出版社,2013.

[6] STINSON D R.密码学原理与实践[M].冯登国,译.4 版.北京:电子工业出版社,2014.

[7] 石井,吴哲,谭璐,等.RSA 数据加密算法的分析与改进[J].济南大学学报(自然科学版),2013,27(3):283-286.

[8] 尹皓,宋晗基.于蚁群优化算法求解最大团问题的研究[J].南华大学学报(自然科学版),2017,31(3):82-86.

[9] 李云飞,柳青,李彤.对一种改进 RSA 算法的密码分析[J].应用科学学报,2013,31(6):655-660.

(责任编辑:扶文静)