三素数 RSA 算法的快速实现

徐 进
(华中师范大学数学与统计学学院,武汉 430079)

摘 要 RSA 算法的执行效率与模幂运算的实现效率有着直接的关系。该文描述及分析了运用中国剩余定理 CRT 来实现三素数 RSA 私钥运算的方法和实现步骤。结果分析表明基于 CRT 的三素数 RSA 处理速度加快,具有一定的应用价值。

关键词 RSA 算法 中国剩余定理 模幂运算

文章编号 1002-8331-(2006)11-0057-02 **文献标识码** A **中图分类号** TP309

A High-speed Algorithm for Three-prime RSA

Xu Jin
(Department of Mathematics and Statistics, Huazhong Normal University, Wuhan 430079)

Abstract: The performance of RSA algorithm implementation has direct relation with the efficiency of modular multiplication implementation. Based on Chinese Remainder Theorem this paper speeds up three-prime RSA private key operations. The result shows that three-prime RSA based on CRT is of great value.

Keywords: RSA, Chinese Remainder Theorem, modular multiplication

RSA 算法诞生于 1978 年,是第一个既能用于数据加密也能用于数字签名的算法[1]。RSA 加密原理基于单向陷门函数,其安全性依赖于大数因数分解的困难性。基于大整数分解问题的 RSA 算法是公开密钥体系的重要组成部分。

为保证 RSA 算法有足够的加密强度,就必须先取足够长的密钥。由于运用 RSA 算法对数据进行加解密运算需要进行大量的模幂运算,较长的密钥势必大大降低 RSA 处理数据的速度[6]。而 RSA 对数据的处理速度一直是其严重的缺陷。1982 年比利时的两位学者运用中国剩余定理提高了 RSA 私钥操作速度 4~8 倍[2]。因此如何提高 RSA 处理数据的速度就成为 RSA 得到普遍应用的关键问题之一。此文就三素数的 RSA 算法为基础,运用三素数的 RSA 算法及中国剩余定理来提高 RSA 算法处理数据的速度。

1 RSA 算法的基本原理[3]

步骤 1 取两个素数 p 和 q(保密)(Ron Rivest, Adi Shamir 和 Lenonard Adleman 建议取为 100 位十进制数);

步骤 2 计算 $n=pq$(公开),n 的 Euler 函数 $\varphi(n)=(p-1)(q-1)$(保密);

步骤 3 随机选取正整数 e,$1<e<\varphi(n)$ 且 $\gcd(e,\varphi(n))=1$(公开);

步骤 4 计算 d 满足同余式 $de\equiv1(\bmod\ \varphi(n))$(保密)。

由于 e 与 $\varphi(n)$ 互素,所以同余式的解 d 是唯一的,这样 RSA 算法的公钥为 e,私钥为 d。利用 RSA 加密需要将明文数字化,并取长度小于 $\log_2 n$ 位的数字作明文块。

加密过程:$C\equiv E[M]=M^e(\bmod\ n)$ (1)

解密过程:$M\equiv D[C]=C^d(\bmod\ n)$ (2)

其中 M 是明文($1<M<n$),C 是密文。

2 三素数 RSA 算法原理

在 RSA 算法中组成模 n 的素数个数可以是多于两个,在三个素数的情况下 RSA 加密与解密算法依然成立。

步骤 1 取三个素数 p,q,r(保密);

步骤 2 计算 $n=pqr$(公开),n 的 Euler 函数 $\varphi(n)=(p-1)(q-1)(r-1)$(保密);

步骤 3 随机选取正整数 e,$1<e<\varphi(n)$ 且 $\gcd(e,\varphi(n))=1$(公开);

步骤 4 计算 d,满足同余式 $de\equiv1(\bmod\ \varphi(n))$(保密)。

加密和解密过程与双素数时完全一样,仍然为:

加密过程:$C\equiv E[M]=M^e(\bmod\ n)$ (3)

解密过程:$M\equiv D[C]=C^d(\bmod\ n)$ (4)

其中 M 是明文,C 是密文。

下面对三个素数 RSA 解密过程的正确性进行证明。

证明:

$D[C]=C^d=(M^e)^d\equiv M^{ed}(\bmod\ n)$ (5)

$\Theta de\equiv1(\bmod\ \varphi(n))$ $\therefore de=1+k\varphi(n)$

这里 k 是整常数,代入公式(5)有:

$D[C]\equiv M^{ed}(\bmod\ n)=M^{1+k\varphi(n)}(\bmod\ n)=M(M^{\varphi(n)})^k(\bmod\ n)$ (6)

(1)若 $\gcd(M,n)=1$,由 Euler 定理[3,6]有 $M^{\varphi(n)}\equiv1(\bmod\ n)$ 即 $D[C]=M$;

(2)若 $\gcd(M,n)\neq1$ 又 $n=pqr$,由素数性质得 $\gcd(M,n)$ 等于 p,q,r 中之一或是 pq,pr,qr 之一。

先假设 $\gcd(M,n)=p$ 有 $M=sp$,这里 s 是正整数。

$\Theta 1<M<n$,$\therefore 1\leqslant s<qr$,又 p,q,r 都是素数。故 $(p,qr)=1$,$(s,qr)=1$,从而 $\gcd(sp,qr)=1$,即 $\gcd(M,qr)=1$。

由 Euler 定理有 $M^{\varphi(qr)}\equiv1(\bmod\ qr)$

于是 $(M^{\varphi(qr)})^{k\varphi(p)}\equiv1(\bmod\ qr)$

则 $M^{k\varphi(n)}\equiv1(\bmod\ qr)$ 或 $M^{k\varphi(n)}=1+lqr$

这里 l 是正整数。由式(6)有:

$D[C]=M(M^{\varphi(n)})^k(\bmod\ n)=M(1+lqr)=$

$M+Mlqr=M+splqr=M+snl\equiv M(\bmod\ n)$

再假设 $\gcd(M,n)=pq$,有 $M=tpq$,这里 t 是正整数。

$\Theta 1<M<n$,$\therefore 1\leqslant t<r$

由 Euler 定理有 $M^{\varphi(r)}\equiv1(\bmod\ r)$

于是$(M^{\varphi(r)})^{k\varphi(pq)} \equiv 1 (\bmod r)$

则$M^{k\varphi(n)} \equiv 1 (\bmod r)$或$M^{k\varphi(n)}=1+cr$

这里c是正整数。

同理可得：

$D[C]=M(M^{\varphi(n)})^k (\bmod n)=M(1+cr)=M+Mcr=$

$M+tpqcr=M+tnc \equiv M(\bmod n)$

这样在三个素数的情况下，$D[C]=M$成立。

3 三素数RSA对私钥操作的加速

快速实现一直是程序员追求的目标，所以任何能够加速RSA算法的事情都是受欢迎的。而RSA算法的公钥操作已经相当快了[4]，RSA私钥是由两个数n和d组成的。传统的取法是n为两个素数p和q的乘积[5]。如果p和q都是512bit，并且因为它们比n(1 024bit)小，私钥操作就会更快，那么如果p,q和r更小一些，操作速度是否会有更大的提高呢？由中国剩余定理，回答是肯定的，组成模的素数越多，私钥操作的运行就越快。

3.1 中国剩余定理简介(CRT)[5,6]

中国剩余定理又叫孙子定理。已知$n_1,n_2,\cdots,n_k$为两两互素的正整数，则同余方程组$x \equiv b_i \bmod n_i$，模N有唯一解，其中$i=1,2,\cdots,k$，b_i为正整数，$N=n_1 \times n_2 \times \cdots \times n_k$。根据高斯算法(Gauss's Algorithm)，中国剩余定理的解为$x=(b_1M_1y_1+b_2M_2y_2+\cdots+b_kM_ky_k)\bmod N$，其中$M_i=\frac{N}{n_i}=n_1n_2\cdots n_{i-1}n_{i+1}\cdots n_k$。$y_i$满足$M_iy_i \equiv 1$，由此可见中国剩余定理为对高位宽(如1 024bit)大数的模幂运算转化为对低位宽(如341bit)相对较小的数进行模幂运算提供了可能。

3.2 中国剩余定理在三素数RSA解密运算中的应用

于是这里令$k=3,n_1=p,n_2=q,n_3=r,b_1=M_p,b_2=M_q,b_3=M_r$，运用中国剩余定理：已知$p,q,r$为两两互素的正整数，正整数$N=p\times q\times r$，则同余方程组$M \equiv M_p \bmod p, M \equiv M_q \bmod q, M \equiv M_r \bmod r$，模$N$有唯一解。其解为：

$$M \equiv (M_pM_1y_1+M_qM_2y_2+M_rM_3y_3)\bmod N \tag{7}$$

其中：

$$M_1=\frac{N}{p}=qr, M_2=\frac{N}{q}=pr, M_3=\frac{N}{r}=pq$$

$M_1y_1 \equiv 1 \bmod p, M_2y_2 \equiv 1 \bmod q, M_3y_3 \equiv 1 \bmod r$

即：$qry_1 \equiv 1 \bmod p, pry_2 \equiv 1 \bmod q, pqy_3 \equiv 1 \bmod r$

根据费马小定理(Fermat's little Theorem)令p为素数，对任何不能被p整除的数A，恒满足$A^{p-1} \equiv 1 \bmod p$，可得$A^{p-2} \equiv A^{-1} \bmod p$。

则式(7)可化为：

$$\begin{aligned} M=&(M_pqr((qr)^{-1} \bmod p)+M_qpr((pr)^{-1} \bmod q)+\\ &M_rpq((pq)^{-1} \bmod r))\bmod N=(M_pqr((qr)^{p-2} \bmod p)+\\ &M_qpr((pr)^{q-2} \bmod q)+M_rpq((pq)^{r-2} \bmod r))\bmod N=\\ &(M_p(qr)^{p-1} \bmod pqr+M_q(pr)^{q-1} \bmod pqr+\\ &M_r(pq)^{r-1} \bmod pqr)\bmod N=(M_p(qr)^{p-1} \bmod N+\\ &M_q(pr)^{q-1} \bmod N+M_r(pq)^{r-1} \bmod N)\bmod N \end{aligned} \tag{8}$$

由于$M \equiv M_p \bmod p, M \equiv M_q \bmod q, M \equiv M_r \bmod r$

故$M_p \equiv M \bmod p \equiv (C^d \bmod N)\bmod p \equiv$

$(C^d \bmod pqr)\bmod p \equiv C^d \bmod p$

由费马小定理的推论：如果整数A不能被素数p整除，且$n \equiv m \bmod (p-1)$，则：

$A^n \equiv A^m \bmod p$

可得$C^d \bmod p=C^{d \bmod p-1} \bmod p$

令$d_p=d \bmod (p-1)$，则有$M_p=C^{d_p} \bmod p$。

同理令$d_q=d \bmod (q-1)$，$d_r=d \bmod (r-1)$，就有$M_q=C^{d_q} \bmod p$，$M_r=C^{d_r} \bmod r$。

若令$C_p=C \bmod p, C_q=C \bmod q, C_r=C \bmod r$，显然可知：

$$M_p=C_p^{d_p} \bmod p, M_q=C_q^{d_q} \bmod q, M_r=C_r^{d_r} \bmod r \tag{9}$$

这样利用式(9)就能将计算明文M转换成计算明文块M_p,M_q,M_r，操作位数减少成原来的三分之一，大大降低了计算强度。

根据以上的分析，基于中国剩余定理，三素数的RSA模幂运算转化为以下运算过程：

步骤1 计算$C_p=C \bmod p, C_q=C \bmod q, C_r=C \bmod r$；

步骤2 计算$M_p=C_p^{d_p} \bmod p, M_q=C_q^{d_q} \bmod q, M_r=C_r^{d_r} \bmod r$，其中$d_p=d \bmod (p-1), d_q=d \bmod (q-1), d_r=d \bmod (r-1)$；

对于给定素数p,q,r及密钥d而言是常数，可以预先计算出来；

步骤3 计算式(8)，即：

$M=(M_p(qr)^{p-1} \bmod N+M_q(pr)^{q-1} \bmod N+M_r(pq)^{r-1} \bmod N)\bmod N$

4 结论

目前虽然关于“组成各种长度的模究竟多少个素数才合适”这个论题仍在继续研究[4]，但就目前计算机的硬件速度来看，三个素数，四个素数分别对1 024bit,2 048bit的模是安全的[4]。下面就三个素数组成模为前提来讨论提高RSA私钥操作速度的原因。

由于RSA解密运算$M \equiv D[C]=C^d(\bmod n)$的复杂程度直接与模$n$和私钥$d$的长度有关。私钥的长度决定了需要做模幂乘的次数，模n决定了中间结果的长度[6]，对于三个素数RSA算法，运用中国剩余定理使得M_p,M_q,M_r的并行计算成为可能。解密过程中对1 024bit大数n的取模运算转化成对三个最大341bit,341bit,342bit素数p,q和r的取模运算，大大降低了模幂运算密度，提高了解密速度。该文在介绍三素数RSA算法实现数据解密的基础上，分析了运用中国剩余定理加快数据处理速度的实现步骤。使得运算密集的解密过程能以并行的方式来处理，显著提高了处理数据的速度。(收稿日期：2005年7月)

参考文献

1.Rivest R,Shamir A,Adleman L.A method for obtaining digital signatures and public-key cryptosystem[J].Communications of the ACM,1978;21:120~126

2.Quisquater J-J,Couvreur C.Fast decipherment algorithm for RSA public-key cryptosystem[J].IEE Electronic letters,1982;21:905~907

3.卢开澄.计算机密码学—计算机网络中的数据保密与安全[M].第3版,清华大学出版社,2003:151~162

4.Burnett S,Paine S.RSA Security's Official Guide To Cryptography[M].McGraw-Hill Education,2001:89~96

5.饶进平,冯登国.一种高效RSA模幂算法的研究[J].计算机工程与应用,2003;39(9):76~77

6.饶进平,冯登国.高速RSA处理芯片的研究和实现[J].计算机工程与应用,2003;39(5):139~141