DOI：10.15986/j.1006-7930.2015.02.0026

分布式信息管理系统混合加密优化研究

陈永锋，宋 楠

（西安建筑科技大学管理学院，陕西 西安 710055）

摘要：基于分布式信息管理系统大量高效安全的数据传输要求，针对密钥管理和认证安全的问题提出混合加密算法进行数据加密．混合加密算法使用基于 **RSA** 算法的密钥管理方式和身份认证体系，并使用二进制编码、**CRT** 定理、费马定理和小数筛选等方法进行优化．最终构造一个既满足密钥管理与消息认证，又有较高的运算效率的混合加密体系．实验结果表明优化后 **RSA** 算法效率明显提升，混合加密体系具有可靠地安全性与可行性．

关键词：分布式信息管理系统；混合加密；**RSA** 优化；中国剩余定理

中图分类号：TU45 **文献标志码**：A **文章编号**：1006-7930(2015)02-0293-04

Optimization and research on hybrid encryption of distributed information management system

CHEN Yongfeng, *SONG Nan*

(Xi'an Univ. of arch. & Tech., Xi'an 710055, china)

Abstract: Based on the requirements of efficiency and security on data transmission of distributed information management system, aiming at the key management and authentication security problem this paper put forward the hybrid encryption algorithm for data encryption. Hybrid encryption algorithm applied the key management and identity authentication system based on RSA algorithm, and optimized it by binary code, CRT theorem, Fermat theorem, decimal screening method and so on. Finally it has constructing a hybrid encryption system with satisfies key management and high operational efficiency. Experiments show that the optimized RSA algorithm efficiency improved significantly, the hybrid encryption system has reliable safety and higher practicability.

Key words: Distributed information management system; hybrid encryption; RSA optimization; CRT

随着信息技术的不断发展，信息管理系统为人们带来了很多便利．其中分布式系统更是将不同地点的系统连接起来，方便了管理也减少了投入．但是分布式信息管理系统面临大量的数据交互，其安全与效率问题一直无法兼顾．本文以多校区一卡通系统为例，提出混合加密算法从软件的角度提供一种解决思路．

保障信息安全的主要手段是进行数据加密，其由密钥种类可分为对称加密和非对称加密[1]．对称加密算法最具代表性的就是 1977 年公布实施的 DES 算法作为数据加密标准[2]，在这以后有 3DES 算法[3]、Rijndael 算法[4]、RC5 算法[5]、IDEA 算法[6]等．而非对称加密算法应用最广的是 RSA 算法[6]，它的特点是易于实现，基于大素数分解安全性高，既能加密数据又能进行数字签名身份认证．其他非对称加密算法还有 Elgamal 算法、ECC 算法(椭圆曲线算法)等．

RSA 算法由于算法效率问题不能应用与大数据量加密[7]，各国学者也对其进行了大量的研究以提升运算效率．2003 年 Sung-Ming Yen 提出牺牲存储空间以提升运算效率，瑞士科学家也解决了 768 位 RSA 算法密钥问题[8]．我国学者也取得了大量成就，王晓云教授破解 MD5[9]与 SHA-1[10]算法震惊世界，冯登国院士与陈相宁教授分别提出了运用中国剩余定理[11]和蒙哥马利算法[12]提高运算效率．

目前国内高校一卡通系统基本都采取对称加密算法进行数据加密，其加解密速度快，安全性高，适用于大数据量的数据加密与传输．其中 3DES 加密算法发展成熟，易于实现且与已有的 DES 加密应用兼容，保护已有的使用 DES 的软件和硬件投资．但是单纯的对称加密有其不足之处，校园一卡通系统的消费终端很多，分布很广．其安全性具有一定风险，对称加密无法识别消息来源．这种情况下易遭到第三方恶意篡改消息与伪造消息，同时密钥管理和密钥更换时的风险也很高．而数据签名认证消耗的时间很多，对大数据传输效率造成很大影响．

本文结合 3DES 算法与 RSA 算法以混合加密的方式解决系统数据加密面临的问题．

1 混合加密算法

1.1 两种加密算法的优劣

1) 从密钥管理方面看，3DES 算法明显不如 RSA 算法．密钥的生命周期有限，为了保证数据安全必须不断更新密钥．因为 3DES 算法是对称加密

收稿日期：2014-10-08 **修改稿日期**：2015-04-01
基金项目：国家自然科学基金项目（61271278）
作者简介：陈永锋（1962-），男，博士，教授，主要研究网络安全．E-mail: chenyf@xauat.edu.cn

算法，其密钥需要在通信前进行秘密分配，对于不同的通信对象分配不同的密钥，在密钥分配管理传递的过程中密钥泄露的风险高．所以其密钥更换困难，风险大，密钥管理难度高．而 RSA 算法公开分配加密密钥，对加密密钥的更新容易，对不同的通信对象，也只需保证自己的私钥安全即可．

2) 从加解密效率来看，3DES 算法高过 RSA 算法很多．因为 3DES 算法大多数操作是字节的位移和替换，使用计算机编程可以较快速实现，适用于大量快速的加解密运算．而 RSA 算法是基于大整数分解困难的计算进行的，加解密过程中需要进行高阶模幂运算，非常耗时．因此，RSA 算法在大量多次数据加密过程中并不适用．

3) 从身份认证和消息验证方面来看，因为 3DES 算法是对称加密算法，使用一个密钥所以无法进行数字签名．而 RSA 算法可以进行身份验证和数字签名，其签名过程也非常容易实现．

4) 安全性方面两个算法的安全性都比较高，目前没有成熟的攻击手段破解这两个算法．

1.2 混合加密算法

本文在分析了两种算法的优劣并对 RSA 算法的加解密运算进行了部分优化的基础上，结合两种算法的优势，提出一种既能快速进行大量数据加密也能进行身份验证和消息完整度验证的混合加密体制．其运行过程如下：*A* 发送方，RSA 算法公钥 *PUA*、私钥 *PRA*，3DES 算法密钥 *K*; *B* 接收方，RSA 算法公钥 *PUB*、私钥 *PRB*．

如果没有进行密钥分配或者需要更换密钥，*A* 使用 *PUB* 采用 RSA 算法加密 *K*，得到 *SK*；

1) 计算散列值 $h=H(M)$作为标识，并用 *PRA* 加密 *h*，得到签名 *S*；

2) 使用 *K* 采用 3DES 算法加密明文 *M* 和 *S*，得到需发送的消息 *D*；

3) 若没有进行密钥分配或者需要更换密钥，*A* 将 *SK* 和 *D* 发送给 *B*；否则，*A* 将 *D* 发送给 *B*；

4) 如果接收到 *SK*, *B* 使用 *PRB* 采用 RSA 算法解密 *SK*，得到 *K*；

5) 使用 *K* 采用 3DES 算法解密 *D*，得到 *M* 和 *S*；

6) 计算 $h'=H(M)$，并使用 *PUA* 采用 RSA 算法解密 *S*，得到 *h*；

7) 如果 $h'=h$，则说明消息验证成功；否则，消息可能遭到篡改．

1.3 密钥管理

密钥分配过程(没有进行密钥分配或者需要更换密钥时)：

1) 公开自己的公钥 *PUA*，*B* 公开自己的公钥 *PUB*；

2) 使用 *PUB*，采用 RSA 算法加密 3DES 算法的密钥 *K*，生成数字信封 *DK*；

3) 使用散列函数 *H*，计算散列值 $h=H(DK)$；

4) 使用私钥 *PRA* 采用 RSA 算法加密 *h*，产生数字签名 *S*；

5) 将 *S* 和 *DK* 一起发给 *B*；

6) 用 *H* 计算 $h'=H(DK)$，用 *PUA* 解密 *S*，若 $h=h'$，说明消息来自 *A* 没有被篡改；

7) 使用 *PRB* 解密 *DK*，得到 3DES 算法的密钥 *K*，完成密钥分配．

2 算法优化与数字签名

2.1 RSA 算法优化

RSA 算法是一种非常典型的公钥密码体制，具有安全性好和密钥管理方便等优点[13]．但是它也存在一些不足：一方面，计算密钥需要大量的计算，且在数据加密和解密过程中都需要计算某整数的模 *n* 整数次幂问题，这些大量计算都消耗了大量的时间，限制了 RSA 算法的效率．另一方面，大素数 *p* 和 *q* 的确定没有一个成熟的方法，一般使用繁琐的素性检测和随机生成的办法产生大素数，效率较低[14]．

本文从下列几个方面对 RSA 算法进行优化：

1) 模算术里的求幂运算：在 RSA 中，加密和解密都需要计算某整数的模 *n* 整数次幂，如果先求出整数的幂，再对 *n* 取模，那么中间结果会非常大．我们可以利用模算术的下列性质来计算

$$[(a \bmod n)\times(b \bmod n)]\bmod n = (a\times b)\bmod n \quad (1)$$

这样我们将中间结果对 *n* 取模，简化计算：

假定要计算 a^b，其中 *a* 和 *b* 是正整数，将 *b* 表示为二进制数 $b_k b_{k-1}\ldots b_0$，则：$b = \sum_{b_i\neq 0} 2^i$

$$a^b = a^{(\Sigma_{b_i\neq 0}\, 2^i)} = \prod_{b_i\neq 0} a^{(2^i)} \quad (2)$$

$$a^b \bmod n = [\prod_{b_i\neq 0} a^{(2^i)}]\bmod n = (\prod_{b_i\neq 0}[a^{(2^i)} \bmod n])\bmod \quad (3)$$

2) 用私钥进行有效运算：我们不能为了计算效率而简单地选择一个小数值的 *d*，为了简化计算，这里运用中国剩余定理来加快运算速度．

首先介绍中国剩余定理[15]，也叫孙子定理，是数论中最有用的定理之一．CRT(中国剩余定理)说明某一范围内的整数可通过它的一组剩余类数来重构，这组剩余类数是对该整数用一组两两互素的整数取模得到的[15]．令：

$$M=\prod_{i=1}^{k}m_i \tag{4}$$

其中 m_i 是两两互素的，我们可将 Z_M 中的任一整数对应一个 k 元组，该 k 元组的元素均在Z_{m_i}中，这种对应关系为：$A\leftrightarrow(a_1,a_2,\ldots,a_k)$，其中 $A\in Z_M$，对 $1\leqslant i\leqslant k$，$a_i\in Z_{m_i}$，且 $a_i=A \bmod m_i$.

定理 1：对 $1\leqslant i\leqslant k$，令 $M_i=M/m_i$，因为 $M_i=m_1\times m_2\times\cdots\times m_{i-1}\times m_{i+1}\times\cdots\times m_k$，所以对所有的 $j\neq i$，有 $M_i\equiv 0(\bmod m_j)$．令

$$c_i=M_i\times(M_i^{-1} \bmod m_i) \tag{5}$$

定理 2：根据 M_i 的定义有 M_i 与 m_i 互素，所以 M_i 有唯一的模 m_i 的乘法逆元，可以得到唯一的 c_i．计算

$$A\equiv\left(\sum_{i=1}^{k}a_ic_i\right)(\bmod M) \tag{6}$$

由于 $j\neq i$ 时，$c_j\equiv M_j\equiv 0(\bmod m_i)$，且 $c_i\equiv 1(\bmod m_i)$，故 $a_i=A \bmod m_i$，上式得证．

由上两个定理可以方便求解 $M=C^d \bmod n$，定义一些中间结果：$V_p=C^d \bmod p$, $V_q=C^d \bmod q$

运用 CRT 公式(5)～(6)，定义

$$\begin{gathered}X_p=q\times\left(q^{-1}\bmod p\right)\quad X_q=p\times\left(p^{-1}\bmod q\right)\\ M=\left(V_pX_p+V_qX_q\right)\bmod n\end{gathered} \tag{7}$$

进一步，使用费马定理来简化 V_p 和 V_q 的计算，即依据：如果 p 和 a 互素，则 $a^{p-1}\equiv 1(\bmod p)$.

$$V_p=C^d \bmod p=C^{d \bmod (p-1)} \bmod p \tag{8}$$

$$V_q=C^d \bmod q=C^{d \bmod (q-1)} \bmod q \tag{9}$$

这里的 $d \bmod(p-1)$和 $d \bmod(q-1)$可以预先计算出来，与直接计算 $M=C^d \bmod n$ 相比，上述的计算速度快了很多.

3) 大素数生成与检测：在文献[16]中已经证明随机递增搜索次数要小于随机搜索法，所以我们这里使用随机递增搜索法来产生大素数．由数论中的素数定理可知，在 N 附近平均每隔 ln$N$ 个整数就有一个素数，这样我们在找到一个素数之前，平均要测试大约 ln$N$ 个整数．由于偶数直接拒绝，所以实际上只需测试大约(ln$N$)/2 个整数[17]．在进行素性检测前，我们可以先进行预处理以提升检测效率，排除掉偶数，使用小素数整除法进一步筛选，然后使用 Miller-Rabin 算法对伪素数的素性进行检测．多次执行测试可使得一个整数是素数的概率接近 1.0．测试一个给定的数 n 是否为素数的过程涉及 n 和一个随机选择的整数 a，$a<n$．若 n 未通过测试，则 n 不是素数;若 n 通过了测试,则 n 可能是素数，也可能不是．若对许多随机选择不同的 a，n 均能通过测试，则我们几乎可以相信 n 就是素数．这个方法看似有些繁琐，但是只有在需要一对新的密钥时才会执行这个过程，所以一般不会很频繁.

2.2　数字签名过程

RSA 算法除了加解密外还可用于数字签名，进行身份认证．我们通过散列函数 H 可以生成一个散列值 h 作为消息认证码，$h=H(M)$[18]．其中 M 是需要传输的消息，$H(M)$是定长的散列值．使用散列函数作为认证码可以减少数据签名时间，增加效率．同时可以不泄露要签名的消息，提高保密度．签名过程如下：

1) 发送方将要发送的消息 M 用过散列函数计算，产生散列值 $h=H(M)$.

2) 发送方用自己的私钥加密 h，产生数字签名 $S=h^d \bmod n$.

3) 发送方将消息 M 和签名 S 一同发给接收方.

4) 接收方用发送方的公钥解密签名 S 得到 h，再用散列函数 H 计算散列值 h'．如果 h'等于 h，则说明消息来源正确，没有被篡改；否则，消息来源可能有问题．这样在消息传输过程中就避免了消息来源问题和中间人篡改消息的可能.

3　实验结果

本次实验的测试环境为：i5-4440 CPU、8G 内存，操作系统为 Windows7，开发工具是 Visual Studio 2010.

3.1　RSA 加密速率与签名效率测试

首先对素数生成效率进行测试，为了测试大量素数生成效率，素数为 512 位．改进算法与经典算法的效率对比如图 1．可以看出，五次实验随着生成素数的数量增加，消耗时间明显有所改善．通过改善生成素数时间可以提高 RSA 签名效率[19].

测试 RSA 签名速率我们生成 1 024 位素数单独测试，并对比传统 RSA 签名和只有 CRT 的 RSA 签名．如图 2 所示，本文改进的签名计算过程有非常明显的效率提升,可以大幅度提高 RSA 加解密速度，使其可以有效的应用在大数据传输的消息认证中.

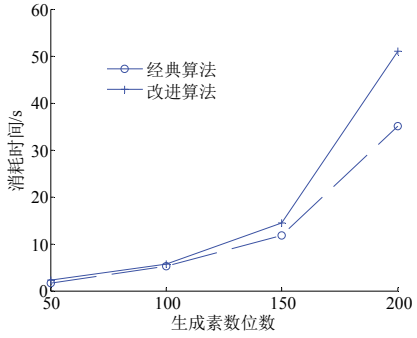

图 1　改进算法生成大素数时间对比

Fig.1　The comparison of generate large prime time

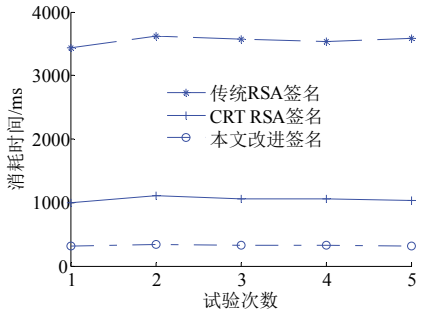

图 2 RSA 签名时间对比

Fig.2 Comparison of RSA signature time

3.2 安全性分析

混合加密体系主要的安全风险在于密钥管理与消息认证．密钥管理风险是基于 RSA 算法的安全性上的，而 RSA 算法在模数够大(大于 1 024 bits)时的安全性是有保证的．所以在体系下进行密钥分配和密钥更换时严格执行密钥管理方法，即可保证密钥管理过程中的安全．消息认证方面，我们没有直接使用消息进行数字签名，而是使用了散列函数 H 计算散列值．即使第三方攻击者获取发送方 A 的两个签名 S_1，S_2．也不能计算出 $S_3^d=((S_1^d \bmod n)(S_2^d \bmod n)) \bmod n$．因为给定一个 D 很难找到 M，使得 $H(M)=D$，这样就避免了第三者篡改、伪造签名和中间人攻击等风险．

4 结语

本文以校园一卡通系统为例，面对多校区分系统传输信息安全和密钥管理的需要，综合分析了目前主流的对称加密算法 3DES 和非对称加密算法 RSA．在对其功能过程进行分析的同时，优化部分计算过程，结合两个算法功能和运算的特点研究混合加密体系．解决系统的密钥管理与消息认证问题，提高系统运行安全性．对于分布式信息管理系统数据安全问题提出一种解决思路．

在后续的研究中，将会在实际系统中检测该体系的运行并推广到其他分布式信息管理系统．同时继续优化加密过程以提高运算速度，并在身份认证与消息认证方面做更深入的研究．

参考文献 References

[1] 杨波. 现代密码学[M]. 北京: 清华大学出版社, 2007.
YANG Bo. Modern cryptography[M]. Beijing: Tsinghua University press, 2007.

[2] 陈恭亮. 信息安全数学基础[M]. 北京: 清华大学出版社, 2011.
CHEN Gongliang. Mathematical foundations of information security[M]. Beijing: Tsinghua University press, 2011.

[3] STALLINGS W. The advanced encryption standard[J]. Cryptologia, 2010, 26(3): 165-188.

[4] JAMIL T. The rijndael algorithm[J]. Potentials, 2004, 23(2): 36-38.

[5] RIVEST R L. The RC5 encryption algorithm[J]. Springer Berlin Heidelberg, 1995: 86-96.

[6] RIVEST R L, SHAMIR A. A method for obtaining digital signatures and public key cryptosystems[J]. Communications of the Association for Computer Machinery, 1978, 21(2): 120-126.

[7] WIENER M J. Cryptanalysis of short RSA secret exponents[J]. IEEE Information Theory Society, 1990, 36(3): 553-558.

[8] BONEH D, DURFEE G. Cryptanalysis of RSA with private key d less than N0. 292[J]. IEEE Information Theory Society, 2000, 46(4): 1339-1349.

[9] WANG Xiaoyun, YU Hongbo. How to Break MD5 and Other Hash Functions[J]. Cryptologia, 2005, 251(7): 357-362.

[10] 饶进平, 冯登国. 高速 RSA 处理芯片的研究与实现[J]. 计算机工程与应用, 2003, 39(5): 139-141.
RAO Jinping, FENG Dengguo. Research and Implementation of High Speed RSA Crypto Chip[J]. Computer engineering and Applications, 2003, 39(5): 139-141.

[11] 王琴琴, 陈相宁. Montgomery 算法在RSA中的应用及其优化[J]. 计算机技术与发展, 2007, 17(6): 145-146, 150.
WANG Qinqin, CHEN Xiangning. Optimization and Application of Montgomery Algorithm in RSA[J]. Computer Technology and Development, 2007, 17(6): 145-146, 150.

[12] 王安. RSA 公钥密码算法的快速实现[D]. 济南: 山东大学, 2008.
WANG An. Fast implementation of RSA public key cryptosystem[D]. Jinan: Shandong University, 2008.

[13] 贺克英. 改进的 RSA 算法实现研究[D]. 成都: 电子科技大学, 2010.
HE Keying. Research and implementation of the improved RSA algorithm[D]. Chengdu: University of Electronic Science and technology of China, 2010.

[14] YEN Sungming, KIM Seungjoo, LIM Seongan. RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis[J]. IEEE Transactions on computers, 2003, 52(4): 461-472.

[15] 费晓飞, 胡捍英. CRT-RSA 算法安全性分析[J]. 微计算机信息, 2009, 25(3): 38, 54-55.
FEI Xiaofei, HU Hanying. Security of CRT based RSA Algorithm[J]. Micro computer information, 2009, 25(3): 38, 54-55.

[16] 张宝华, 殷新春. RSA 密码算法的安全及有效实现[J]. 中山大学学报: 自然科学版, 2008, 40(6): 22-26.
ZHANG Baohua, YIN Xinchun. The safe and efficient implementation of RSA algorithm[J]. ACTA Scientiarum Naturalium Universitatis Sunyatseni: Sci. & Tech. , 2008, 40(6): 22-26.

[17] 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.
SHI Jing, WU Zhe, TAN Lu, et al. Analysis and Improvement of RSA Data Encryption Algorithm[J]. Journal of University of Jinan: Sci. & Tech. , 2008, 40(6): 22-26.

[18] 肖振久, 胡驰, 姜正涛. AES 与 RSA 算法优化及其混合加密体制[J]. 计算机应用研究, 2014, 31(4): 1189-1194.
XIAO Zhenjiu, HU Chi, JIANG Zhengtao. Optimization of AES and RSA algorithm and its mixed encryption system[J]. Application Research of Computers, 2014, 31(4): 1189-1194.

[19] 刘学军, 邢玲玲, 林和平, 等. Miller-Rabin 素数检测优化算法研究与实现[J]. 信息技术, 2008(12): 141-143.
LIU Xuejun, XING Lingling. Research and realization of Miller-Rabin optimizing algorithm for prime testing[J]. Information Technology, 2008(12): 141-143.

(本文编辑 桂智刚)