文章编号：2095-2163(2020)03-0166-03 中图分类号：TP309 文献标志码：A

RSA 加密算法的研究

李 莹，赵 瑞，曹 宇，张天宇，刘霏凝
（吉林师范大学 计算机学院，吉林 四平 136000）

摘 要：随着互联网和通信技术的发展，信息安全问题日益受到重视，基于数据加密的信息安全技术得到了迅速的发展。数据加密就算法而言，分为对称加密和非对称加密两类。RSA 是应用最广泛的非对称算法之一，具有安全性高、易于实现等特点，但运算速度很慢，只能用于一些少量数据。针对 RSA 运算效率慢的问题，提出了中国剩余定理和蒙哥马利模乘法相结合的方法来优化模幂，用三素数代替传统的二重素数。实验结果表明，优化算法具有较高的速度和可行性。

关键词：RSA；中国剩余定理；蒙哥马利模乘法

Research on RSA encryption algorithm

LI Ying, ZHAO Rui, CAO Yu, ZHANG Tianyu, LIU Feining
(College of Computer Science, Jilin Normal University, Siping Jilin 136000, China)

【Abstract】With the development of Internet and communication technology, more and more attention has been paid to information security.In terms of algorithm, data encryption can be divided into symmetric encryption and asymmetric encryption.RSA is one of the most widely used asymmetric algorithms, and has the characteristics of high security, being easy to implement, but the operation speed is very slow, which can only be used for some small amount of data encryption. In order to solve the problem of slow arithmetic efficiency of RSA, a method combining Chinese residual theorem and Montgomery modular multiplication is proposed to optimize modular power and replace traditional double prime number with triple prime number. Experimental results show that the optimization algorithm has high speed and feasibility.

【Key words】RSA;Chinese remainder theorem; Montgomery model multiplication

0 引 言

随着计算机技术的不断发展，互联网上共享的数据量有了显著增长。处理大数据的需求也日渐增多，在安全性上就面临诸多挑战。在当今信息时代，互联网上的数据容易遭遇各种攻击，每个人都希望能够保护好自己的隐私。因此，维护用户类数据的安全性即已成为目前的研究热点。具体来说，该项研究主要包括新加密算法研发和安全系统设计。其中，加密算法通常分为 2 类，分别是对称加密和非对称加密。当下研究指出，RSA 算法是数据加密应用最广泛的一种非对称加密算法，具有安全性高、易于实现等特点，不仅可对数据进行加密，而且可以对数据进行身份验证。在 RSA 算法中，公钥的加密是已知的，而私钥的解密是私密的，因此复杂性机制的加密和解密在整体上是由密钥中需要分解[1]的质数的数量决定。而要实现安全的数据传输，就要对质数进行因数分解。此时将需要较长的计算时间和强大的计算能力，所以对于质数的解密是必不可少的。相比之下，只对 2 个质数进行因数分解，2 个质数通常很容易被打破[2]。因此，提出了使用 3 个质数来减少处理时间并提高安全性[3]。在本次研究中，主要在对非对称加密算法中的 RSA 算法原理进行分析的基础上，针对 RSA 算法的优缺点以及存在的问题，采用中国剩余定理和蒙哥马利模乘法进行优化，提出 RSA 的改进算法，并在 Java 平台上实现。

1 密码学

计算机安全在信息安全中起着重要的作用。密码学是计算机系统中保护数字数据的第一种方法，广泛应用于数字电视广播、数字货币、手机等日常生活的各个方面，以维护消息的机密性和防止信息篡改及窃听。总而言之，密码学的历史就是密码分析的历史。由于新的密码分析方法的发布，或者计算机和网络的突破性进展，即使是那些被认为绝对安全的密码，最终也会暴露在风险之中（受到危害），而这反过来又推动了加密技术的新发展。在当下研究中，RSA 非对称加密算法即是密码学常用的加密算法。

基金项目：吉林省教育厅项目（JJKH20180761KJ）；2019 年吉林省高等教育教学改革项目（JLCR611720190723010810）；基于区块链的大数据在线教育平台的关键技术与安全策略研究（研创新 201949）。

作者简介：李 莹（1994-），女，硕士研究生，主要研究方向：信息安全。

收稿日期：2019-12-24

2　RSA 算法

2.1　算法原理

RSA 算法是由 Rivest、Shamir 和 Adleman 开发的一种非对称加密算法，在此算法中公钥和私钥将会配合使用。迄今为止，RSA 算法已然成为使用最广泛的公钥算法，究其原因即在于其易于实现及良好的安全性。使用 RSA 算法来开发密钥，每条消息都被映射成整数，通常被定义为分组密码，当用户解密数据时，密钥则用于验证，该过程增强了存储数据的数据完整性，为用户提供更好的安全性。在研究工作中，用户数据在存储到服务端之前将使用 RSA 算法进行加密，继而使用 RSA 算法生成私钥，只有拥有数据的用户才知道该算法。RSA 算法中涉及的步骤分为密钥生成、加密和解密。对此拟做阐释分述如下。

2.1.1　密钥生成

在数据加密之前完成，密钥生成过程如下：

步骤 1　为保证数据的完整性，将通过考虑 2 个不同的随机素数（如具有相似位长的 g 和 h）来选择输入。

步骤 2　计算 $i = g * h$。

步骤 3　计算欧拉函数：$\emptyset(i) = (g-1) * (h-1)$。

步骤 4　选择一个整数 a，$1 < a < \emptyset(i)$ 和最大公约数，$\emptyset(i)$ 是 1。现在，将其作为公钥指数发布。

步骤 5　确定如下：$d = a - 1(mod\ \emptyset(i))$ 即 d 是 $a\ mod\ \emptyset(i)$ 乘法逆元。

步骤 6　d 作为私钥组件，$d * a = 1\ mod\ \emptyset(i)$。

步骤 7　公钥由模 i 和公钥指数 (a, i) 组成。

步骤 8　私有密匙由模 i 和私有指数 d 组成，而私有指数将被 (i, d) 保密。

2.1.2　加密

将原始数据转换为密码数据的过程被定义为加密。建议的加密程序如下：

步骤 1　公钥 (a,i) 传输给用户。

步骤 2　可逆协议用于将用户数据映射到称为填充方案的整数。

步骤 3　对所需的数据进行加密，得到的密码数据 C 由 $C = me(mod\ i)$ 给出。

2.1.3　解密

将密码数据转换为原始数据的过程被定义为解密。建议的解密程序如下：

步骤 1　向用户提出请求。

步骤 2　使用生成的私钥和加密的数据来验证用户的真实性。

步骤 3　用户将数据解密为 $m = Cd \pmod i$。

步骤 4　通过改变填充方案，为用户计算 m 提供了原始数据。

2.2　RSA 算法的改进及应用

RSA[4] 系统是在众多领域得到应用和普及的公钥密码系统之一。RSA 运算本质上是一个模指数运算。RSA 算法中大数因子分解的模指数运算是一项耗时的工作，始终制约着 RSA 算法的发展。该算法的安全级别依赖于在短时间内因式分解一个大整数。针对这一问题，许多学者提出了不同的优化算法，其中，中国剩余定理（CRT）对解密的有效性是显而易见的。证明了考虑中国剩余定理的计算代价，对偶素数 CRT-RSA 的运算速度分别是原算法的 3.32 倍（1 024 位模）和 3.47 倍（模型为 2 048 位）[5] 的运算速度。虽然速度令人满意，但存在安全问题。因此，将原有的双素数 RSA 算法改为三素数，然后进行加密操作[6-7]，这里将展开如下研究论述。

2.2.1　三素数 RSA 算法基本原理

在传统双素数 RSA 密码算法[8] 的基础上，取 3 个素数，仍建立算法，描述如下：

（1）随机选取 3 个不同的大素数 p、q、r，计算 $n = pqr$，$\phi(n) = (p-1)(q-1)(r-1)$。

（2）选取满足一定条件的加密密钥 e，计算满足 $de \equiv 1 \bmod \phi(n)$ 的私钥 d。

（3）加密和解密过程与传统算法相同。具体来说，加密算法为：$c = E(m) = me \bmod n$，解密算法为：$m = D(c) = cd \bmod n$。

2.2.2　利用蒙哥马利模乘法和中国剩余定理进行优化

RSA 算法的密码运算需要一个模指数，而模指数运算是由重复模乘法组成的。在众多计算模乘法的算法中，蒙哥马利模乘法因其在硬件实现上的显著效率而成为应用最广泛的算法之一。蒙哥马利模乘法是一种将除法运算转换为移位运算，以简化模乘法运算的方法。蒙哥马利模乘法的主要思路是模幂运算，模幂运算可以转换为模乘运算的不断重复过程。

设 A、B 和 M 是 3 个整数，其中 $0 \leqslant A, B < M$。蒙哥马利模乘法就是代替用 M 除来计算 $(AxB) \bmod M$，将所需的运算转换为用 R 除，其中 R 是 2 的幂，$R \geqslant 2^m$，并且最大公约数 $gcd(M,R) = 1$。

蒙哥马利模乘法要求预先计算 q，定义如下：

$$q = (A\ x\ B\ x\ M') \bmod R, \qquad (1)$$

其中，M' 是蒙哥马利模乘法的常数，满足：

$$(-M)\ x\ M' = 1\ mod\ R. \quad (2)$$

中国剩余定理是求解同余群的一种方法，是数论[9-10]中的一个重要定理。蒙哥马利模乘法的主要思路是模幂运算，模幂运算可以转换为模乘运算的不断重复过程[11]。在计算 N 模的情况下，就像 RSA 算法中计算模一样，$N = p \cdot q$ 是不同的素数乘积。可以看出，中国剩余定理可以将高阶大数转化为较小的低位模指数，大大提高了 RSA 加解密的效率。

3 仿真实验及其性能分析

综合前述分析可知，本文通过对 RSA 算法的仿真设计，来验证其实际的性能。本文中，需要用到的硬件环境描述见表 1。

表 1 计算机硬件指标

Tab. 1 Computer hardware indicators

指标	性能
CPU	Intel(R) Core(TM) i7-6700
内核	8 GB
操作系统	Win7
程序开发环境	Java

在 Java 的基础上，本文选用文献[12]中一种新的快速产生大素数的方法，对 2 048 bit 大数 n 的取模运算，随机生成素数。传统的双素数 RSA 算法、双素数混合 CRT 算法和三素数 CRT-RSA 算法分别对 3 个相同的消息摘要进行操作，记录各自的耗时行为。运行结果曲线如图 1 所示。实验结果见表 2。

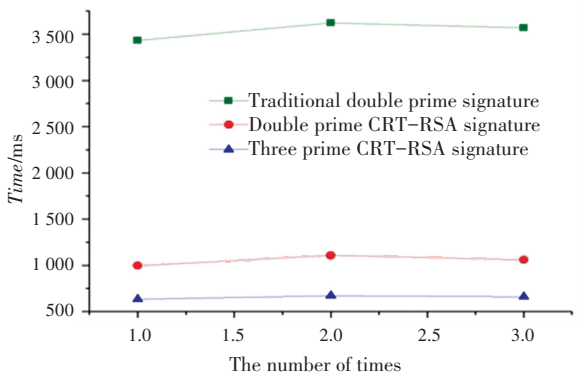

图 1 仿真实验结果

Fig. 1 Simulation experiment results

表 2 3 种算法耗时情况

Tab. 2 Time consumption of 3 algorithms ms

算法	时间			平均耗时
	第 1 次	第 2 次	第 3 次	
传统双素数	3 432	3 621	3 568	3 541
双素数 CRT-RSA	996	1 107	1 059	1 054
三素数 CRT-RSA	635	670	660	655

由表 2 可知，利用中国剩余定理进行双素数 RSA 优化的效率是传统算法的 3.36 倍，接近理论值 3.47。使用中国剩余定理和蒙哥马利模乘法的三素数 RSA 算法的效率是传统算法的 5.4 倍，是双素数 RSA 算法的 1.6 倍。结果表明，改进后的 RSA 算法可以大大提高速度。

4 结束语

本文主要研究了常用非对称加密算法 RSA。研究中，探讨分析了其研究现状，改进了算法的不足之处，通过比较 2 个素数和 3 个素数之间的运行效率，可以看出安全性能的提高，证明了改进算法的优势。

参考文献

[1] Shiota S, Furuta S, Hirokawa M, et al. Cryptographic communication system and cryptographic communication method: US, 9608818 [P]. 2017-03-28.

[2] ISWARI N M S. Key generation algorithm design combination of RSA and ElGamal algorithm [C]//2016 8th International Conference on Information Technology & Electrical Engineering. Yogyakarta, Indonesia: IEEE, 2017: 1.

[3] PATIDAR R, BHARTIYA R. Modified RSA cryptosystem based on offline storage and prime number [C]// 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). Enathi, India: IEEE, 2013: 1.

[4] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public key cryptosystems [J]. Communication of Association for Computing Machinery, 1978, 21(2): 120.

[5] BONEH D, DURFEE G. Cryptanalysis of RSA with private key d less than $N^{0.292}$ [M]// STERN J. Advances in cryptology — EUROCRYPT'99. Lecture Notes in Computer Science. Berlin/Heidelberg: Springer, 1999, 1592: 1.

[6] LIU Ping, ZHAO Huanping. Analysis and research on improved RSA algorithm[J]. Computer and Modernization, 2013(7): 84.

[7] YAN S Y. Computational number theory and modern cryptography [M]. USA: Wiley, 2012.

[8] FEI Xiaofei, HU Hanying. Security of CRT based RSA algorithm [J]. Microcomputer Information, 2009, 25(1-3): 54.

[9] SHAND M, VUILLEMIN J. Fast implementations of RSA cryptography [C]//The 11th IEEE Symposium on Computer Arithmetic. Windsor: IEEE, 1993: 252.

[10] SKORMIN V A, DELGADO-FRIAS J G, MCGEE D L, et al. BASIS: A biological approach to system information security [C]// 2001 Proceedings of Information Assurance in Computer Networks: Methods, Models and Architectures for Network Security International Workshop MMM - ACNS 2001. St. Petersburg, Russia: Springer-Verlag, 2001: 127.

[11] 薛念，潘赟，张宇弘，等. 基于 Montgomery 模乘的 RSA 加密处理器[J]. 计算机工程，2010，36(13)：125.

[12] COUVEIGNES J M, EZOME T, LERCIER R. A faster pseudo-primality test[J]. Rendiconti del Circolo Matematico di Palermo, 2012, 61(2): 261.