# RSA 算法的应用现状与研究

郭　虎
长江大学文理学院，中国·湖北 荆州 434020

【摘　要】本课题基于对小型文件加密的研究，尝试借助RSA算法进行任意文件的加密，进一步提升文件利用安全性。其工程整体主要以分层设计为主，以期为后续开发与引用提供借鉴与便利。

【关键词】RSA 算法；流程；应用

## 1　课题背景

作为当前常用数据加密技术之一，RSA 公钥加密算法还能用于数字签名算法。相较于其它算法的应用，RSA算法在操作性、理解性等方面更具优势。该算法在1978年由Leonard Adleman、Ron Rivest,Adi Shamir提出，尽管目前其领域内未对该算法安全性进行理论性验证，但是从2006年到现在，该算法历经多种攻击仍保持较高的安全性。基于算法标准化工作及其商业应用的背景下，RSA 算法的应用逐渐普及，并被世人认可。此外，在互联网身份认证中，RSA 算法的应用最为常见。

1.1 RSA 算法概述及其应用现状

本课题对 RSA 算法运行流程进行阐述，具体为：

〈密钥生成〉

取素数 p，q，令 n=p × q

取与(p-1)×(q-1)互素的整数 e，

由方程 d × e=1(mod(p-1)×(q-1))解出 d，

二元组(e,n)作为公开密钥，

二元组(d,n)作为私有密钥.

〈加密解密〉

b=aemod n，c=bdmod n.

附录中给出了证明 a=c(mod n).

正因RSA算法的安全性，使得各领域内都存在RSA算法的身影。在硬件领域方面的应用，RSA主要以IC形式在相关电子产品进行有效应用。

而针对软件方面而言，在 Internet 领域中 RSA 算法应用较为集中，包括数字证书、加密连接、数字签名等。具体应用中，以 OpenSSL 工具包为例，SSL 主要体现为安全传输协议，主要作用在于身份确认与数据保护。而OpenSSL则是基于开放源代码的加密技术工具包，主要编写人包括EricYang 等，本文对该工具不进行一一赘叙，详情介绍可参考“http://www.openssl.org/about/”网站。OpenSSL 工具包之所以可以在多种操作系统中有效应用，其原因在于应用RSA算法。此外，人们生活中常用的IE浏览器，基于SSL 协议，通过对RSA 算法与其它技术的集成，进行数字签名与数字证书的控制，进一步提升数据安全。

1.2 加密文件中 RSA 算法的应用

1.2.1RSA 在文件加密中应用的可行性

上文提及，当前数字签名以及数字证书中，RSA算法的应用较为常见。而之所以将RSA算法应用于短小的数据加密，主要在于该算法运行速度相对较慢，相较于DES 算法而言，RSA 算法的加密速度仅有DES 的千分之一。也正因此问题的存在，使得相关学者对文件加密中应用RSA算法没有过多的重视。针对常规文件而言，始终被认为是大数据块，其实不然，实际的文件资料较小，包括电话号码、银行账号、小图片、账号密码等。

本文以大数据运算程度调试为基础，进行加密消耗时间的理论性分析。事先准备一台常规配置的 PC 机，以此为载体进行幂模运算，所获取的指数因公开密钥因 e 取值较小，所以可进行小整数的获取。以 C353 为例，整数字节长度为 70（以 140 位十六进制以及线性组为主要形式，进行 RSA 算法的对应，所获取的 n 为 560bit），并进行函数测试的调试，在算法优化时借助初等数论相关知识，最终获取结果：以内存512MB、处理 AMD2800+、外频 333MHZ 的 PC 机为例，进行 RSA 算法运行所消耗的时间大约为 45ms。以上述运算速度为依据，若实际应用过程中，对大小为 1KB 的数据进行运算，按照 1024 倍的标准进行计算，可以得出 RSA 进行 1kb 数据的加密需要消耗约为 45s，并非完全不能接受。

换种角度而言，既然在数据签名中可有效应用RSA运算，意味着在普通文件中应用该算法同样具有可行性。在处理几百、几千字节文件时，运用 RSA 加密处理，其消耗的时间并不会太长。当然，RSA 加密处理所消耗的时间，与文件大小呈正比关系，结合上述所得 45ms 处理时间，换算成处理 1m 大小的文件，意味着其加密处理所消耗的时间将近 1 天。鉴于此，若想实现利用 RSA 算法进行普通文件的处理，若以常规 PC 机为前提，需要保证文件不能过大。最大处理限度为几 KB，否则会延长加密处理时间。若想实现在短时间进行大文件的有效加密处理，需要通过缩减运算量的方式来实现，这就意味着需要进行秘钥长度的缩短，增大数据出现安全隐患的几率。

本课题中，基于对完成调试软件的应用，进行 RSA 算法时间消耗的测试。测试中 PC 机配置为内存 512MB、处理 AMD2800+、外频 333MHZ，测试对象为 1KB 文件，以 560bit 的 N 进行逐字节进行处理，所测试的最终结果为 55s。而在现实生活中，重要数据文件主要包括电话号码、银行账号密码等，其大小不超过千字节，应用 RSA 算法进行数据加密，所消耗的时间约为几秒钟，所以将 RSA 加密应用于小文件处理中，具有可行性。

1.2.2RSA 应用于文件加密的意义分析

正如上文所述，RSA 算法在小文件处理中的应用，同样可以取得良好的成效。比如人们的隐私号码、银行账号、账号密码等。但是需注意，加密处理方法可行，但并不代表此算法的应用十分必要。本小节主要研究重点在于探究非对称密码在何种文件中能够有效适用，即探究采用 RSA 处理加密文件的意义。

针对带叙述且信息价值高的二进制数据、小型文件，①若此类文件在应用期间未进行加密，会提高计算机中数据管理的风险，尤其是针对公共计算机或公共机房而言。②小型文件虽然具有一定价值，但是若采用大型多用户保护程序进行文件加密，难免有点小题大做。③对称加密技术的应用并非所有文件都适用，因有相同的密钥，在某些环境条件进行交流，会存在诸多限制与影响。

## 2　结语

综上所述，进行 RSA 算法的应用，可以在解除非对称密钥应用局限性的同时，还可实现数据进行文本的有效转化，进一步提升文件传递的安全性，并达到多形式、多通道安全传递文件的目的。

**参考文献：**

[1]基于FPGA实现的AHB-Lite总线传输数据的加密IP核研究[D]柴绍杰.兰州交通大学 2020.

[2]基于加密算法的车载CAN总线安全通信研究[D].罗禹.湖南师范大学 2020.