doi:10.11830/ISSN.1000-5013.201701023

RSA融合AES算法的网络信息安全方法

冷飞,徐进华,栾仕喜

(苏州大学文正学院 信息中心,江苏 苏州 215104)

摘要: 针对网络信息的安全处理,提出一种RSA融合高级数据加密算法(AES)的加密算法.通过RSA算法配置系统密钥,降低密钥管理的复杂度.通过AES算法配合RSA密钥,完成网络信息加密.实验结果表明:RSA融合AES的加密算法充分发挥AES算法执行速度快、RSA密钥配置性能高的特点.

关键词: 网络信息;网络安全;加密速度;密钥配置

中图分类号: TP 309 **文献标志码:** A **文章编号:** 1000-5013(2017)01-0117-04

Research on Network Information Security Based on RSA Fusion AES Algorithm

LENG Fei, XU Jinhua, LUAN Shixi

(Information Centre, Wenzheng College of Soochow University, Suzhou 215104, China)

Abstract: According to the security of network information, a new encryption algorithm based on RSA fusion advanced encryption standard (AES) is proposed. Using the RSA algorithm to configure the system key, in order to reduce the complexity of key management. Using AES algorithm with the RSA key to complete the network information encryption. The experimental results show that the RSA fusion AES encryption algorithm, give full play to the AES algorithm to perform fast, RSA key configuration characteristics of high performance.

Keywords: network information; network security; encryption speed; key distribution

网络空间是一个具有高透明度的开放空间,经常会受到攻击、拦截和破坏,传输的网络信息面临巨大的安全隐患[1].有效提升网络空间中传输的网络信息安全的问题已经成为信息技术领域、网络技术领域普遍关注的焦点问题[2].当前,针对网络信息的安全保护,主要采取各种形式的加密处理[3].从技术角度看,网络信息加密可以通过信息顺序置乱和密文信息嵌入明文等手段,其加密理论和历史悠久的密码学理论极为近似[4].在密码学领域,加密处理主要针对密钥进行,根据密钥加密处理的策略不同,又可以分为对称加密和非对称加密两大类[5].数据加密算法(data encryption standard,DES)的最大缺点在于加密后的密钥长度不足,无法承受网络间的多类型、强有力攻击[6].为此,在DES加密算法的基础上,设计了高级数据加密算法(advanced encryption standard,AES)[7].AES数据加密方法不仅继承了DES加密算法加密速度快的特点,而且大幅度提高抗攻击性能[8].与对称加密不同,非对称加密在加密端和解密端使用了不同的密钥,从而使网络信息的安全程度更高.RSA加密算法是非对称加密领域的典型算法,但因为复杂的处理过程使其加密速度较慢[9].因此,作为对称加密领域中的代表性算法,AES加

收稿日期: 2016-11-25

通信作者: 冷飞(1974-),男,副教授,主要从事计算机技术,网络工程的研究.E-mail:53292999@qq.com.

基金项目: 国家自然科学基金资助项目(12ZWK01);苏州大学文正学院高等教育改革资助项目(2910312615)

密算法具有了加密速度上的优势;作为非对称加密领域中的代表性算法,RSA 加密算法具有了密钥配置上的优势[10]. 本文提出一种 RSA 融合 AES 的加密算法.

1 RSA 融合 AES 网络信息加密方案

在密钥配置方面,AES 算法属于对称加密算法,即在加密端和解密端使用相同的密钥. 对于网络信息而言,如果有 m 个用户之间进行通信,那么,每个用户至少需要设定 $m-1$ 个密钥,全网用户的密钥数量达到 $m(m-1)/2$ 个. RSA 算法则是非对称加密算法,在加密端和解密端使用不同的密钥. 对于网络用户而言,他们只需要保护好自己的解密密钥即可.

在加密时间方面,AES 算法的最大密钥宽度不超过 256 bit,RSA 算法的密钥则是大数的幂形式. 相比之下,AES 算法的加密时间要短得多. 在签名认证方面,AES 算法受到自身设计机理的限制,无法进行签名认证,RSA 算法则可以采取简便的处理完成签名认证. 在安全性能方面,AES 算法和 RSA 算法分别是对称加密和非对称加密领域中的经典方法,加密安全性都比较理想.

通过上述分析,AES 算法在加密速度上具有优势,RSA 算法在密钥配置、签名认证方面具有优势. 因此,在融合算法的设计上,尽可能地保留两种算法的优势,以更好地适应网络信息安全的需要. RSA 融合 AES 加密算法框架,如图 1 所示.

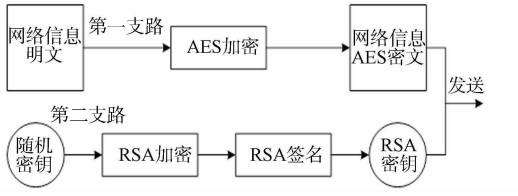

图 1 RSA 融合 AES 加密算法框架

Fig. 1 Frame of encryption algorithms fused by RSA and AES

由图 1 可知:第一条支路是对要加密的网络信息明文,执行 AES 加密处理,形成网络信息的 AES 密文;第二条支路是随机生成密钥,对密钥信息执行 RSA 算法配置密钥,再对这个配置后的密钥信息执行 RSA 签名和认证处理,形成 RSA 密钥;最后,将网络信息 AES 密文和 RSA 密钥通过网络通信通道,同时向接收端发送.

2 RSA 融合 AES 网络信息加密算法

2.1 AES 加密处理

1) 字节替换处理. 为了实现更好的加密效果,替换处理 AES 加密中的字节,针对网络明文信息中的每个字节,采用非线性变换的操作. 在这一处理开始之前,先要做一个边界设置,即"00"类的字节无法被替换. 对于其他字节,执行仿射处理,具体为

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \\ S_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} M_0 \\ M_1 \\ M_2 \\ M_3 \\ M_4 \\ M_5 \\ M_6 \\ M_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}. \tag{1}$$

根据式(1),一个字节中 8 bit 以上的字符都实现了替换处理,从而达到整个字节替换的目的.

2) 行字符移位处理. 为了使加密效果更加可靠,对于不同行上移位设置了不同的规则. 例如,以 4 行为一个移位周期,第 0 行向左移动 4 位,第 1 行向左移动 3 位,第 2 行向左移动 2 位,第 3 行向左移动 1 位. 其具体操作为

$$\mathrm{Shift(bit)} = \begin{cases} 4, & \mathrm{bit} = \text{“0”}, \\ 3, & \mathrm{bit} = \text{“1”}, \\ 2, & \mathrm{bit} = \text{“2”}, \\ 1, & \mathrm{bit} = \text{“3”}. \end{cases} \tag{2}$$

3）列字符混叠处理. 假设

$$D(c) = \lambda_1 c + \lambda_2 c + \lambda_3 c + \lambda_4. \tag{3}$$

那么，列字符的混叠处理所对应的具体数学表达式为

$$S(c) = D(c) \otimes M(c). \tag{4}$$

如果参与混叠的每一个字符列包含 4 行元素，那么混叠处理为

$$\begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_4 & \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_3 & \lambda_4 & \lambda_1 & \lambda_2 \\ \lambda_2 & \lambda_3 & \lambda_4 & \lambda_1 \end{bmatrix} \begin{bmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \end{bmatrix}. \tag{5}$$

2.2　RSA 密钥配置

对于加密算法中的密钥配置，考虑到 AES 算法密钥空间过大，故用效率更高的 RSA 算法完成密钥配置. 首先，随机形成两个大一点的素数，此处分别用 A 和 B 表示. 在此基础上，进行的配置如下，即

$$\left.\begin{aligned} x &= AB, \\ E(x) &= (A-1)(B-1). \end{aligned}\right\} \tag{6}$$

式(6)中：$E(x)$表示以 x 为自变量的欧拉函数.

其次，选取一个整数 K_p 并用它作为公钥，选取原则为

$$\gcd(K_p, E(x)) = 1. \tag{7}$$

最后，根据公钥信息再配置一个私钥 K_s，即

$$K_s = 1 (\mathrm{mod}\ E(x)). \tag{8}$$

2.3　RSA 签名认证

对于网络明文信息 M，其签名处理为

$$N = M^{K_s} (\mathrm{mod}\ x). \tag{9}$$

网络通信过程中，发送端同时将(N,M)的组合信息发送到接收端. 接收端则需要对其进行认证，认证处理为

$$M' = N^{K_p} (\mathrm{mod}\ x). \tag{10}$$

因为同时用到了签名和私钥，发送端和接收端都无法抵赖，从而确保了网络信息安全可靠的传输.

3　结果与分析

为了能够更加直观地判断 RSA 融合 AES 算法的加密性能，选择 AES 加密算法、RSA 加密算法作为比对算法. 分别从算法的密钥数量、算法的加密速度展开. 提出的算法和 AES 算法的密钥数量对比，如图 2 所示. 提出的算法和 RSA 算法的加密速度对比，如图 3 所示. 图 3 中：t 为加密时间.

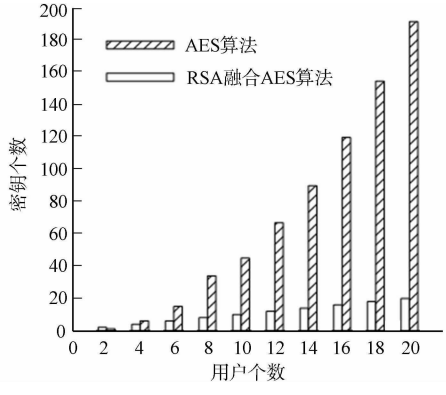

图 2　两种算法的密钥数量对比

Fig. 2　Comparison between quantities of two algorithms′ key

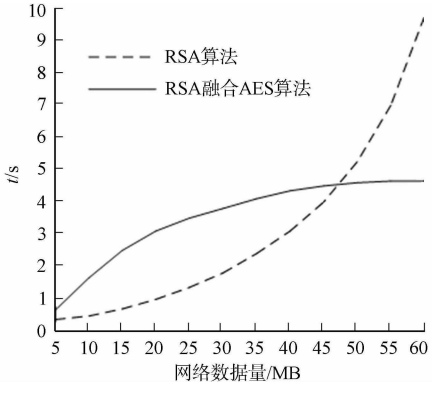

图 3　两种算法的加密时间对比

Fig. 3　Comparison between encryption time of two algorithms

由图 2 可知：随着用户数量的增大，AES 算法和 RSA 融合 AES 算法的密钥个数都在增大，但提出

的RSA融合AES算法的密钥个数增加速度大大低于AES算法.因此,RSA融合AES算法的密钥更容易管理,从密钥配置角度证实了加密算法的优势.

由图3可知:随着网络信息传输数据量的不断增大,两种算法的执行时间都有所增加;但是,RSA融合AES算法的执行时间增加到一定幅度之后,开始趋于稳定;而RSA算法的执行时间,随着网络信息传输数据量的不断增大,增加幅度持续加大,当网络信息数据量增大到一定程度,RSA算法的加密时间已经大大高于文中算法.

这组实验结果从执行时间的角度,证实了所提出的融合算法的优势.

4 结论

网络信息安全问题是信息社会必须要妥善处理的问题.针对已经应用于网络信息安全的加密算法展开研究,深入分析了AES对称加密算法和RSA非对称加密算法的优缺点.在此分析结果的基础上,构建了一种RSA融合AES算法.此算法的执行过程分为两个支路,一条支路用AES算法加密明文信息,一条支路用RSA算法配置密钥,充分发挥AES算法执行速度快、RSA算法密钥配置效果好的特点.开展了两组实验研究,实验结果证实:所提出的算法在执行速度上大大优于RSA算法,在密钥配置效果上大大优于AES算法,其加密性能满足于网络信息安全的需要.

参考文献:

[1] 赵振国.基于攻防博弈模型的网络安全测评和最优主动防范[J].电子测试,2015(2):62-64.

[2] BANDYOPADHYAY T,JACOB V,RAGHUNATHAN S. Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest[J]. Information Technology and Management,2010,11(1):7-23.

[3] 刘巧平,周斌,王文涛.基于椭圆曲线的信息加密及网络身份认真算法的研究[J].自动化与仪器仪表,2016(8):105-111.

[4] WU Yong,HU Defa. Encryption model of network information based on AES algorithm with dimension reduction chaos optization[J]. Metallurgical and Mining Industry,2015,7(4):11-17.

[5] 刘冰,潘大兵.新三维混沌映射及其在数字图像信息加密中的应用[J].华侨大学学报(自然科学版),2015,36(6):655-658.

[6] JADHAV S,MOHITE V. A data hiding techniques based on length of English text using DES and attacks[J]. International Journal of Research in Computer Science,2012,2(4):1121-1128.

[7] GANESH A R,MANIKANDAN P N,SETHU S P,*et al*. An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks[J]. International Conference on Recent Trends in Information Technology,2011:1209-1214.

[8] 蔺小梅,李国刚,张泽普.采用OHNN和M-LFSR的字序列密码加密方案[J].华侨大学学报(自然科学版),2014,35(5):519-522.

[9] KANNAMMAL A,RANI S S. DICOM image authentication and encryption based on RSA and AES algorithms[J]. Communications in Computer and Information Science,2012,330:349-360.

[10] 许柯,刘绪崇,符振艾,等.网络信息加密RSA算法的运算速度和保密性优化[J].科技通报,2015,31(7):144-147.

(**责任编辑:** 陈志贤 **英文审校:** 吴逢铁)