* 文章编号:2096-398X(2019)06-0153-07

一种结合优化后 AES 与 RSA 算法的二维码加密算法

刘海峰[1], 刘 洋[2], 梁星亮[1]

(1.陕西科技大学 文理学院, 陕西 西安 710021; 2.陕西科技大学 电子信息与人工智能学院, 陕西 西安 710021)

摘 要:针对目前的二维码信息安全发展现状,提出一种结合了改进后的 AES 和 RSA 算法的二维码加密算法。该算法在 QR 二维码编码之前实现加密,即对明文信息进行加密,利用改进后的 AES 算法先对明文信息进行对称加密,然后使用 RSA 非对称加密算法对于改进后的 AES 算法中使用到的参数进行加密生成参数密文,最后将信息密文和参数密文拼接后生成二维码并进行网络信道传输.该算法的特点是通过对 AES 算法密钥扩展和列混淆变换两方面的改进、又用中国剩余定理进行 RSA 解密算法的优化,减少了算法运行所消耗的时间,提高了安全性.该算法高效易行,结合两种算法优点,实现了对密钥的高效管理和对信息的安全保护,具有一定的推广和实用价值.

关键词:改进 AES; RSA 优化; 二维码加密算法
中图分类号:TP309.7 **文献标志码**: A
DOI:10.19481/j.cnki.issn2096-398x.2019.06.026

A QR code encryption technique combining optimized AES and RSA algorithms

LIU Hai-feng[1], LIU Yang[2], LIANG Xing-liang[1]

(1.School of Arts and Sciences, Shaanxi University of Science & Technology, Xi'an 710021, China; 2.School of Electronic Information and Artificial Intelligence, Xi'an 710021, China)

Abstract: According to the present situation of the two-dimensional code's information security, a two-dimensional code encryption algorithm based on the improved AES and RSA algorithm is proposed in this paper. The algorithm encrypts before QR code encoding, which means it encrypts the plaintext information, using the improved AES symmetrical encryption algorithm to encrypt the plaintext information, then using the RSA asymmetric encryption algorithm to encrypts the improved AES algorithm's parameters to generate the parameter ciphertext. Finally, the information ciphertext and the parameter ciphertext are spliced to generate two-dimensional code and transmit it in the network channel. This algorithm is characterized by the improvement of the key expansion and column obfuscation transformation of AES algorithm, and optimized of the RSA decryption algorithm with the Chinese remainder theorem, which reduces the running time of the algorithm and improves the algorithm's security. This algorithm is efficient and easy to implement, combined with the advantages of the

* 收稿日期:2019-07-09
基金项目:陕西省科技厅自然科学基础研究计划项目(2017JQ1026); 陕西省教育厅专项科研计划项目(17JK0102)
作者简介:刘海峰(1964-),男,陕西泾阳人,副教授,硕士生导师,研究方向:计算机网络与信息安全、代数编码与密码学

two algorithms, it can effectively manage the key and protect the security of the information. It has certain generalization and practical value.

Key words: improving AES; RSA optimization; bivariate code encryption algorithm

0 引言

二维码作为一种存储、传递和识别信息的技术现已在多个领域得到了广泛的使用，例如物流、交通、电子商务等.但随着二维码在市面上的推广，二维码的信息泄露危险也日益突出.由于二维码的生成标准是公开的，且未能在编码过程中实现信息加密，攻击者可以通过二维码截获到存储和传递的信息，存在着一定安全问题[1].对于未加密的二维码，任何获得二维码的人进行扫描后均可得到二维码中保存的信息，这对涉及个人隐私敏感信息领域造成使用上的不便.例如在追溯系统中，产品信息生成的未加密的二维码在传输过程中，若被不法分子获得，便可进行假冒印刷等一系列违法行为，使用加密后的二维码作为保存、传递产品信息的媒介，可以起到规范市场，打击假冒的目的.对于二维码信息进行加密，既保证了它的隐私性，也为使用者的个人安全提供了保障.因此，有关二维码的加解密的研究成为一个热点问题.

目前，国内对于二维码信息安全的研究取得了一些初步进展.2014 年，于英政等[2]提出结合了 DES 和 RC4 加密算法，选取 DES 和 RC4 两种算法之一，针对不同阶段的二维码信息进行加密，实现了对二维码分阶段加密；安吉旺等[3]提出对编码信息采用 RSA 和 key 口令的算法进行二维码混合加密，对明文信息分组加密后，通过 key 口令对分组明文加密，再使用 RSA 算法对 key 口令的密钥进行加密.在专用的识别软件上，如果输入正确的私钥可解密出相应的明文信息.2015 年，肖本海等[4]基于 SHA512 和 AES 两种算法对二维码信息及其密钥进行了加密，提高了对密文的保护；同年，廖镇勋等[5]提出一种针对二维码的不同阶段，探究其差异并采用不同的方法进行二维码的加密，提高了二维码加密的程度.2017 年，龙强等[6]提出一种基于非对称密码体制的二维码加密算法，该算法将非对称加密算法 RSA 与 Logistic 混沌模型相结合，对二维码中信息及密钥进行加密编码，保证了二维码中信息可以在不安全的信道中安全地传输.2018 年，张华[7]探讨了利用非对称 加密算法加密二维码的可行性和安全性；葛娅敬等[8]提出对二维码图片矩阵进行奇异值分解从而加密得到密文，解密得到明文，使基于图像处理上的二维码信息安全有了一定进展.杨康等[9]针对不同的信息权限和属性集，生成访问控制树，通过不同用户的属性分配对应的不同私钥，实现了二维码的分级加密.

综上，当前针对二维码加密的方式分为对生成的二维码图像的加密和对未进行生成二维码之前的初始明文信息的加密.在对二维码信息加密的讨论中，主要是针对二维码加密算法安全性的讨论，使用 RSA 非对称算法为例的加密算法存在着加密或解密算法时间复杂度高的问题，而使用以 DES 对称算法为例的二维码加密算法，又存在着 DES 超期服役和密钥传输是否安全的问题.

本文提出一种结合改进的 AES 算法和 RSA 优化算法的二维码加密算法.本算法在生成二维码之前，对明文信息加密，利用 AES 对称密码算法加密效率快和 RSA 非对称算法便于密钥管理的优势，基于算法安全性的基础之上实现了对密钥的安全管理.同时通过对两种算法的优化减少加解密消耗的时间，实验证明，该算法提高了二维码加密的效率.

1 算法理论

1.1 二维码

二维码，又称二维条码或 QR Code.在固定好的平面区域，二维码通过散落的黑白相间的图形按一定的规律排序，从而记录数据信息.QR 码与传统一维条码相比：数据承载量更大；属于纠错编码；可以引入加密体系；编码范围更广.QR 码的这些特性，决定了其作为载体，在信息时代会有更多的发展空间.

1.2 AES 算法

AES 算法是一种新型加密方法，具有更加可靠的加密过程和更加适合的密钥长度.AES 算法包含三大部分：密钥扩展，加密和解密.密钥长度有 128 位、192 位、256 位 3 种.密钥扩展算法的输入是一个 4 字的密钥，输出是一个 44 字的一维线性数组.每轮的密钥由种子密钥经过扩展得到.128 位的 AES 加解密算法由十轮组成(192 位 12 轮，256 位 14 轮)，每一轮有四个基本步骤：ByteSub 变换：用一个 S 盒完成分组中的按字节的代换，ShiftRow 变换：一个置换过程，MixColumn 变换：一个利用在 $GF(2^8)$ 上的算术特性的代换，AddRoundKey 变换：当前分组按位异或扩展密钥的一部分.解密算法和加密算法不同，仅仅密钥扩展形式一样，但对于加密解密中转换顺序是不同的.

1.3 AES 算法改进

1.3.1 密钥扩展改进

在传统 AES 算法密钥扩展部分，使用初始输

入的 4 字(16 字节)的密钥进行密钥扩展后,得到 44 个字(156 字节)组成的扩展密钥数组 $W=(w_0,w_1,\cdots,w_{43})$.由输入的密钥可直接先得到 W 的前 4 个字:w_0,w_1,w_2,w_3,W 剩余的字由前一字以及前面第四个字进行如下运算操作得到:当下标数字不为 4 的倍数时,直接进行异或操作,否则,先与前一字进行 g 变换,再和前第四字进行异或操作,如图 1 所示.这种密钥扩展算法面临的主要挑战是攻击者若是截取到其中一轮密钥,便可通过相应变换得到剩余所有密钥.

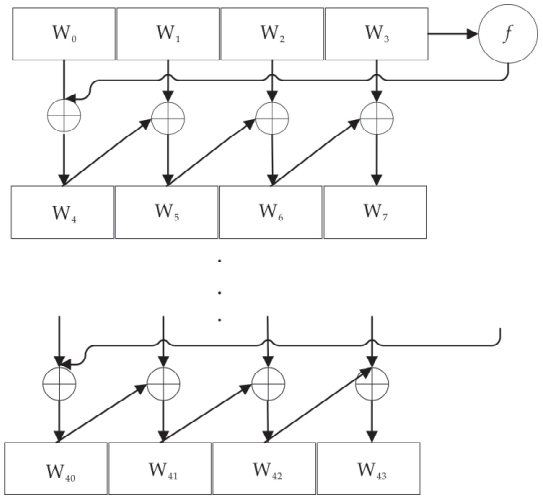

图 1　传统 AES 算法密钥扩展过程

文献[10]提出一种密钥改进算法:在密钥扩展过程中,初始密钥不变,在密钥扩展过程中,使用与初始密钥无关的一套新密钥填充为第一轮扩展密钥,求解剩余密钥则继续使用 AES 密钥扩展算法依据新密钥扩展,最终得到全部密钥.算法原理如图 2 所示.

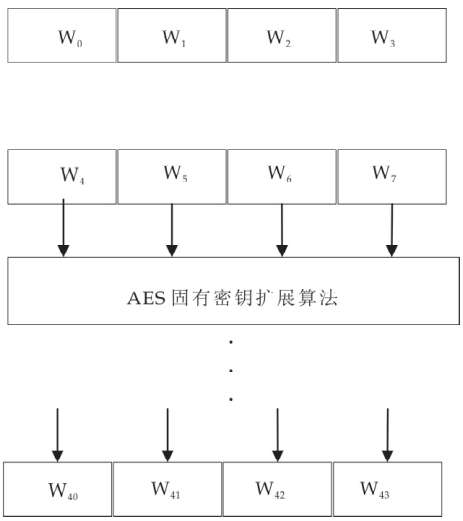

图 2　改进 AES 算法密钥扩展过程

由于扩展密钥都是由新密钥通过 AES 算法扩展得到的,与初始密钥无关,因此扩展密钥和初始密钥不存在代数关系,对于攻击者来说,截取到任一轮扩展密钥也无法推出初始密钥,反之,截取到初始密钥也无法推出扩展密钥.设种子密钥长为 k bit,采用穷尽密钥攻击平均复杂度约为 2^{k-1},以 10 轮 AES 算法来说,密钥攻击者平均需尝试 2^{127} 次可能的密钥,而改进后的密钥扩展算法使平均需尝试 2^{225} 次可能的密钥,以目前的计算能力很难破解.因此该算法在保证与程序效率不变的基础上克服了程序被截取一轮密钥即可破解全部密钥的漏洞.

在这种密钥扩展改进算法中,若攻击者已知算法密钥扩展改进过程,又成功截取到初始密钥 x_0 和其后由任一轮由新密钥或新密钥扩展得到的密钥,那么攻击者依然可根据密钥扩展过程由任一轮密钥穷尽推出新密钥,进而得到全部密钥.

面对这种挑战,本文提出一种在文献[10]密钥扩展算法上的改进算法:初始密钥不变,依照原始密钥扩展算法进行轮密钥扩展,增加随机轮数 k($1<k\leqslant 10$),在随机 k 轮时加入新密钥,加入新密钥后,剩余密钥更改为以新密钥为该轮密钥进行密钥扩展.改进后的算法原理如图 3 所示.

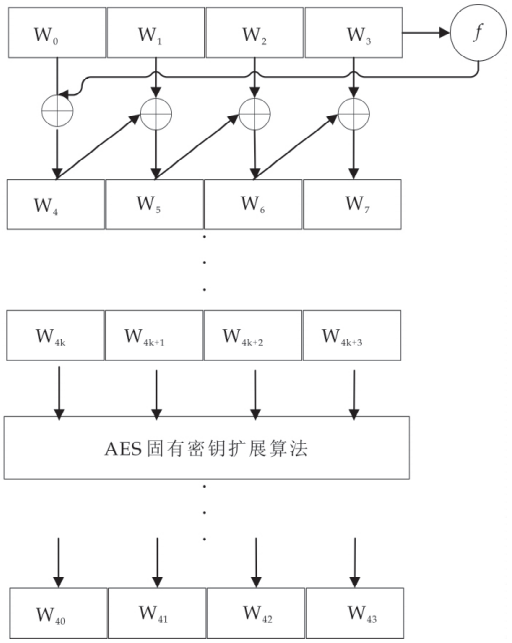

图 3　本文 AES 算法密钥扩展过程

对于之前的攻击者,攻击分为以下情况:

(1)攻击者截取到十轮中任两轮密钥,但未知随机轮数 k 情况下:①两轮密钥均由初始密钥或新密钥之一进行密钥扩展而来,由于开始选取的新密钥与初始密钥无关,则攻击者无法推得另一密钥及其扩展密钥,进而无法获得全部密钥;②两轮密钥分别由初始密钥和新密钥之一密钥扩展而来,则攻击者在未知捕获的两种密钥分别属于新密钥或初始密钥和未知分别属于两种密钥扩展的哪一轮密钥扩展情况下一共有 90 种可能的密钥组合,大大增加了破解难度.

(2)若攻击者截取到随机数 k 和初始密钥的

情况下，由于不知道新密钥，无法通过计算获得全部密钥.

(3)若攻击者截取到随机数和新密钥，情况和(2)相似.

1.3.2 列混淆变换改进

在传统 AES 加密算法中，MixColumn 变换即列混淆变换，分为正向列混淆变换和逆向列混淆变换，提供算法的扩散性.列混淆变换的正向列混淆变化对每列独立地进行操作.每列中每个字节被映射为新值.式(1)表示 $GF(2^8)$ 上正向列混淆变换，用于数据加密，式(2)表示 $GF(2^8)$ 上逆向列混淆变换，用于数据解密.

$$\begin{pmatrix} S'_{0,j} \\ S'_{1,j} \\ S'_{2,j} \\ S'_{3,j} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,j} \\ S_{1,j} \\ S_{2,j} \\ S_{3,j} \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} S_{0,j} \\ S_{1,j} \\ S_{2,j} \\ S_{3,j} \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} S'_{0,j} \\ S'_{1,j} \\ S'_{2,j} \\ S'_{3,j} \end{pmatrix} \tag{2}$$

在 AES 算法中，加密过程中，列混淆变换需要执行 4 次 xor 加法和 2 次 xtime 乘法，而解密过程中逆列混淆变换需要执行 9 次 xor 加法运算和 12 次 xtime 乘法运算[10].加密算法和解密算法因列混淆算法不同，导致加解密耗时不对等，解密算法中需要更多的时间来进行运算.

文献[10]提供了最简单形式的正向列混淆运算矩阵和逆向列混淆运算矩阵.

$$M = M^{-1} = \begin{pmatrix} 2 & 1 & 3 & 1 \\ 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \end{pmatrix} \tag{3}$$

用 M 矩阵代替原 AES 算法中正向列混淆和逆向列混淆运算中矩阵，减少了逆向列混淆运算所消耗时间，使正向列混淆运算和逆向列混淆运算消耗相同的运算资源，均为执行 4 次 xor 加法和 2 次 xtime 乘法，解决了加解密耗时不对等问题.

本文对 M 矩阵进一步改为：

$$M = M^{-1} = \begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 2 & 0 & 3 \\ 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \tag{4}$$

这样改进 M 后，正向列混淆和逆向列混淆均减少执行 2 次 xor 加法运算，加密耗时和解密耗时的共同降低使运算速度得到一定提升，章节 4.1 中的表 1 罗列了对同样数据量加密或解密所用时间的对比.

1.4 RSA 算法

RSA 是典型的非对称加密算法，它的特点是使用两个密钥的密码算法，具有方便密钥管理和传送的特点.它的基础是大数分解的困难性，它的核心是模幂运算.主要包括两个方面：密钥的产生和加密解密.

RSA 密钥的生成过程：

(1)首先选出两个大的素数 p 和 q，要求 p 不能等于 q，且 p 和 q 有一定的差距.

(2) 计算出 $n = p * q$.

(3) 计算出 $\Phi(n) = (p-1) * (q-1)$.

(4) 选择 e，使得 $1 < e < \Phi(n)$，同时 e 和 $\Phi(n)$ 要互素.

(5) 计算解密密钥参数 d 时，要求 $ed = 1 \bmod \Phi(n)$，可用扩展的欧几里得算法求解.由此得出，私钥(d,n)，然后公开 n 参数，其中 n 又被称为模，保密原始素数 p 和 q.

其中 (e,n) 是公钥，(d,n) 是私钥.d 是秘密的，而 n 是公开的.密文的解密者(或系统)将公钥公开，而将密钥和系统参数两个大素数 p、q 藏起来.

对于 RSA 算法：$D(E(M)) = (M^e)^d \bmod n = (M^d)^e \bmod n + E(D(M))$，其中 M 为明文，加密公式 $C = E(M) = M^e \bmod n$，解密公式 $M = D(C) = C^d \bmod n$.

1.5 RSA 算法优化

由于 RSA 算法中模正整数次幂的运算过程复杂，影响算法执行效率，是限制 RSA 发展的主要难题.而 RSA 算法的解密者拥有保密的系统参数 p、q 和私钥，可以在解密过程中利用中国剩余定理进行解密优化，先对中国剩余定理做简单介绍.对于同余方程组(5)：

$$\begin{cases} x = a_1 \bmod m_2 \\ x = a_2 \bmod m_2 \\ \cdots \\ x = a_r \bmod m_r \end{cases} \tag{5}$$

若满足：①$m_1, m_2, \cdots, m_r$ 为两两互素的正整数；②$a_1, a_2, \cdots, a_r$ 为整数，则同余方程组(5)的模 $M = m_1, m_2, \cdots, m_r$ 有唯一解(证明过程省略)：

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M \tag{6}$$

其中：$M_i = M/m_i$

$y_i M_i \equiv 1 \bmod m_i, 1 \leqslant i \leqslant r$

可见，中国剩余定理能够把高位宽大数的模幂运算转换为低位宽相对较小的模幂运算.下面叙述运用中国剩余定理改进 RSA 解密的方法[11].

在 RSA 算法中，存在两个互素的数 p、q，由中国剩余定理，可知求解密方程 $M = D(C) = C^d \bmod n$ 的运算，等价于求同余方程组(7)，由此，可实现由计算模 n 的数量级转化为计算模 p 和模 q 的数量级.

$$\begin{cases} M_1 = C^d \bmod p \\ M_2 = C^d \bmod q \end{cases} \tag{7}$$

(费马小定理) p 为素数,x 为满足 $x(\mathrm{mod}\ p)\neq 0$ 条件的整数,则:$x^{p-1}\equiv 1(\mathrm{mod}\ p)$.

由费马小定理,令 $r=d(\mathrm{mod}\ p-1)$,则存在 k 满足:$d=k(p-1)+r$. 故:

$$M_1=C^d(\mathrm{mod}\ p)\equiv C^{k(p-1)+r}(\mathrm{mod}\ p)\equiv (C^{(p-1)}\ \mathrm{mod}\ p)^k C^r(\mathrm{mod}\ p)\equiv 1^k C^r(\mathrm{mod}\ p)\equiv C^{d\ \mathrm{mod}(p-1)}(\mathrm{mod}\ p)\equiv (C\ \mathrm{mod}\ p)^{d\ \mathrm{mod}\ (p-1)}(\mathrm{mod}\ p)$$

同理,对同余式 $M_2=C^d(\mathrm{mod}\ q)$,有:$M_2=(C\ \mathrm{mod}\ q)^{d\ \mathrm{mod}\ (q-1)}(\mathrm{mod}\ q)$.令 $d_1=d\ \mathrm{mod}(p-1)$,$d_2=d\,\mathrm{mod}(q-1)$. 因此,同余方程组(7)转化为低指数的同余方程组(8).

$$\begin{cases}M_1=(C\mathrm{mod}p)^{d_1}\ \mathrm{mod}p\\ M_2=(C\mathrm{mod}q)^{d_2}\ \mathrm{mod}q\end{cases}\tag{8}$$

又由中国剩余定理和费马小定理可知其解:

$$M=((C\ \mathrm{mod}\ p)^{d_1}q(q^{-1}\ \mathrm{mod}\ p)+(C\ \mathrm{mod}\ q)^{d_2}p(p^{-1}\ \mathrm{mod}\ q))\mathrm{mod}\ n=((C\ \mathrm{mod}\ p)^{d_1}q(q^{p-2}\mathrm{mod}\ p)+(C\ \mathrm{mod}\ q)^{d_2}p(p^{p-2}\mathrm{mod}\ q)\mathrm{mod}\ n=((C\ \mathrm{mod}\ p)^{d_1}q(q^{p-2}\mathrm{mod}\ n)+(C\ \mathrm{mod}\ q)^{d_2}p(p^{q-2}\ \mathrm{mod}\ n)\mathrm{mod}\ n=((C\ \mathrm{mod}\ p)^{d_1}(q^{p-1}\mathrm{mod}\ n)+(C\ \mathrm{mod}\ q)^{d_2}p^{q-1}\mathrm{mod}\ n)\mathrm{mod}\ n$$

将中国剩余定理应用在 RSA 算法解密过程中,远远小于直接进行解密所需指数运算数量级,而且通过多项式运算代替逆元的求解,进一步减少运算时间,从而提高运算速度.

根据 RSA 的快速 MMRC 解密算法[12],步骤 1-5 为快速解密算法.运用这种算法共有 1 次逆元,2 次乘法,1 次加法,1 次减法和 1 次 k 比特模余,RSA 算法解密效率得到进一步提升.计算以下各式:

(1)$d_1\leftarrow d(\mathrm{mod}\ p-1)$ 与 $d_2\leftarrow d(\mathrm{mod}\ q-1)$

(2)$C_1\leftarrow C(\mathrm{mod}\ p)$ 与 $C_2\leftarrow C(\mathrm{mod}\ q)$

(3)$M_1\leftarrow {C_1}^{d_1}(\mathrm{mod}\ p)$ 与 $M_2\leftarrow {C_1}^{d_2}(\mathrm{mod}\ q)$

(4)$B\leftarrow p^{-1}(\mathrm{mod}\ p)$

(5)$m\leftarrow M_1+[(M_2-M_1)*B(\mathrm{mod}\ q)]*p$

2　结合改进后 AES 和改进后 RSA 的 QR 加密算法

方案总体思路:采用以改进后的 AES 算法为主、改进后的 RSA 算法为辅的加密算法,将改进后 AES 算法加密结果与改进后 RSA 算法加密结果结合作为 QR 码算法的输入,然后进行二维码编码.不妨设 Alice 是二维码的生成方和发送方,Bob 是二维码的接收方和验证方,明文为 M.算法主要分为以下步骤:

(1)系统建立

发送方 Alice 选择 AES 算法参数随机密钥 x_0 和第一轮密钥 y_0,系统利用 RSA 生成算法及 Bob 选择的 RSA 公钥 $K_1=(e,n)$,系统生成私钥 $K_2=(d,n)$,并反馈给 Bob,将 K_1 公开,将系统初始化系数传递给接收方 Bob.

(2)信息加密

Alice 采用改进 AES 加密算法,选定参数 $N=(x_0,y_0,z_0)$ 对明文进行加密,即利用改进后的 AES 密钥扩展算法,得到 AES 算法全部密钥,再利用全部密钥进行 AES 加密算法得到密文 M'.将参数信息 N 用 RSA 算法公钥 K_1 进行加密生成 N'.

(3)生成二维码

Alice 将明文密文 M' 和参数密文 N' 拼接在一起并进行一系列后续操作即数据分析、数据编码、纠错编码、构造最终信息、生成掩膜和格式与版本信息等,生成含有加密信息的二维码.

(4)密文解密

接收方 Bob 收到二维码信息后,扫描并通过 RSA 算法的私钥 K_2 进行解密得到二维码参数密文 N,结合改进后 AES 解密算法进而得到明文信息 M.

算法加密流程如图 4 所示,算法解密流程如图 5 所示.

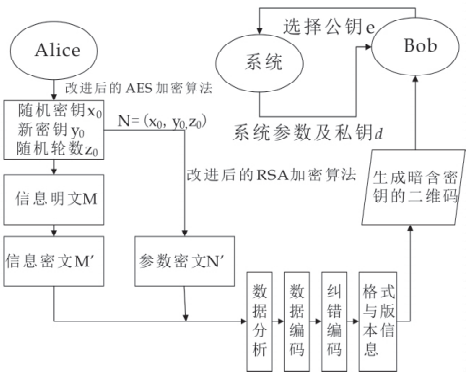

图 4　算法加密流程图

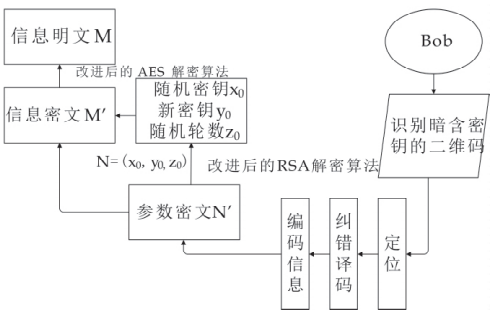

图 5　算法解密流程图

3　算法实现

算法实现基于 PyCharm 平台,编程语言为 python.QR 二维码的生成识别采用 zxing 解析库、PIL,pillow 和 qrCode 库.

Alice 在线传输明文信息给接收方 Bob.Alice

作为二维码生成以及发送方，传输 $M=$'iamgladtoseeyous'作为信息明文，进行测试运行.Alice 选择随机密钥 $x_0=2345678910111213$，新密钥 $y_0=1520251221521113$，$z_0=2$，加密之后密文 $M'=$c059e873b5a60a9104ef499f961a320B，Bob 选取 RSA 算法公钥后，由系统生成 1024 位密钥，RSA 算法加密 x_0 得到 x_0'，加密 y_0 得到 y_0'，加密 z_0 得到 z_0'，中间用'//'分隔.$x_0'=$129064168989005983496743590450297397026065405 97，$y_0'=$425420404286176275383986137492130476820305389897，$z_0'=8$，将 M' 和 N' 用'//'拼接后进行后续二维码编码.

如图 6 所示，接收方 Bob 扫描得到：由 AES 算法加密的密文 M'，由 RSA 算法加密的 AES 算法初始向量与第一轮密钥密文 N'.首先使用系统建立时的私钥 K_2 进行 RSA 解密，得到参数明文 (x_0,y_0,z_0).再利用 AES 解密算法和参数 N 解密由二维码传递的密文 M'，最终获得信息明文 $M=$'iamgladtoseeyous'.

图 6 带有密文和参数密文信息的 QR 二维码图片

4 算法测试

4.1 加密速度比较

程序运行环境为：Windows 10，CPU 2.5 GHz，RAM 4G.测试软件为 PyCharm 2018.1.2.测试采用四种算法对二维码编码前明文加密：

(1)文献[13]提出的 AES 算法.

(2)文献[14]提出的 3DES 算法.

(3)数据加密经典传输方案 AES+RSA 算法.

(4)本文提出的结合了改进后的 AES 与 RSA 优化算法的加密算法.其中 3DES 使用 3 个 56 位的密钥进行加密.AES 密钥长度均采用最广泛的 128 位，二维码存储明文字符串，四种算法对相同的 48 字节的字符串分别进行 1000 次加解密，取得加解密的平均时间，算法加密和解密时间测试结果在表 1 中列出.

表 1 算法加解密时间比较

算法	加密 Encrypt/ms	解密 Decrypt/ms
AES	0.401	0.428
3DES	16.115	16.067
AES+RSA	0.938	14.425
综合改进 AES+RSA 优化	0.889	5.297

由表 1 可以看出，由于使用了 RSA 算法对 AES 密钥参数加密，结合 AES 和 RSA 的算法比仅使用 AES 算法耗费的时间长，但依然在加密速度上优于 3DES 算法，而采用综合改进后的 AES 和 RSA 优化算法加、解密消耗时间更少.

4.2 安全性比较

3DES 算法是 DES 算法的一个安全变形，以 DES 为基本模块，通过组合分组方法设计出分组加密算法.目前，针对 3DES 算法的批评主要有：

(1)3DES 易受差分和线性密码分析攻击.

(2) 3DES 使用 64 位的块长度，不能满足大多数数据传输的要求.

(3)用软件实现该算法的速度比较慢.

针对 3DES 的缺陷[15]，AES 算法得到了解决：

(1)AES 与 3DES 相比对差分、截断差分、线性、插值和平方攻击具有很强的抵抗力.

(2)AES 最小密钥长度为 128 bits，最大密钥长度为 256 bits，目前技术不存在穷举破解的可能.并且 AES 算法的密钥长度根据不同加密级别选择不同密钥长度，而分组长度同样可变，设计的灵活性高.

(3) AES 块长度 128 位，是 3DES 块长度的两倍 .

(4)AES 具有很高的加密效率.

3DES 算法和 AES 算法两种对称密钥密码体制，密钥的分配均存在严重的缺陷，即若黑客在密钥传输过程中截取到密钥，则密文就不再保密.针对这一缺陷，RSA 非对称密码体制使用两个独立的密钥，密钥的分配问题得到了解决.

5 结论

本文提出一种结合了改进后的 AES 与 RSA 优化算法的 QR 加密算法.该算法结合两种算法优点，特别是对 AES 密钥扩展和列混淆变换两方面的改进实现了对明文的高效加密、通过 RSA 算法仅对参数信息加密，将明文信息加密后的信息密文和参数信息加密后的参数密文拼接生成二维码编码，再传送给接收方.在解密算法中，又对 RSA 解密算法使用中国剩余定理进行了优化.该算法相对

于传统二维码传送信息和密钥而言,其加解密过程兼顾了效率和安全性,安全性能得到提高,加解密时间得到减少.该算法具有一定的推广和实用价值.

参考文献

[1] 郑　君,李海霞.基于动态二维码的安全身份认证方案的研究[J].湖北理工学院学报,2015,31(2):35-38.

[2] 于英政,许宏丽.基于 QR 二维码的多级融合加密算法的设计与实现[J].计算机与数字工程,2014,42(12):2 362-2 364.

[3] 安吉旺,徐凯宏.基于 RSA 和密钥的二维码加密编码的研究[J].森林工程,2014,30(2):125-129.

[4] 肖本海,郑莹娜,龙建明,等.基于 SHA512 哈希函数和 AES 加密算法 QR 二维码信息安全设计[J].计算机系统应用,2015,24(7):149-154.

[5] 廖镇勋,王　珏.基于 QR 二维码的多重加密算法研究[J].电脑知识与技术,2015,11(30):64-65.

[6] 龙　强,刘小华.基于非对称密码体制的二维码加密算法[J].重庆师范大学学报(自然科学版),2017,34(3):91-95.

[7] 张　华.基于非对称加密算法的 QR 二维码[J].电子技术与软件工程,2018(5):29.

[8] 葛娅敬,赵礼峰.基于奇异值分解的二维码加密算法[J].计算机科学,2018,45(11A):342-343,360.

[9] 杨　康,袁海东,郭渊博.基于属性加密的二维码分级加密算法[J].计算机工程,2018,44(6):136-140.

[10] 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):1 189-1 194,1 198.

[11] 叶秀芳.RSA 算法的优化策略[J].电子设计工程,2017,25(10):83-89.

[12] 方文和,李国和,吴卫江,等.面向 Android 的 RSA 算法优化与二维码加密防伪系统设计[J].计算机科学,2017,44(1):176-182.

[13] 周佳华,李福山.基于嵌入式的 QR 二维码加密系统设计与实现[J].信息技术与网络安全,2018,37(2):37-39,50.

[14] 叶志琼,郑维清,郑　健,等.疫苗 QR 二维码加密防伪技术[J].齐齐哈尔大学学报,2015,31(4):41-44.

[15] Noura Aleisa. A comparison of the 3DES and AES encryption standards[J]. International Journal of Security and Its Applications,2015,9(7):240-246.

【责任编辑:蒋亚儒】

(上接第 141 页)

(2)通过高温质量流量计及不均匀加热方式模拟出传热设备在实际工程中存在热负荷偏差时,Z 型管组支管中流体流量偏差变化机制.通过实验发现,在低质量流速条件下,吸热较强的支管内流体质量流速较高,即吸热管的自补偿特性,通过这一发现,在管组设计时,通过合理的支管布置,可以有效的避免热负荷偏差造成的流量偏差的恶化,提高设备安全运行的能力.

(3)在相同的入口流速、压力及热流密度条件下,通过采用六头内螺纹管研究管型结构对于 Z 型并联管组支管流体流量偏差的影响规律.通过实验可知六头内螺纹管可以有效的减小支管流量偏差,但无法消除,并且从经济性角度分析,螺纹管结构复杂,造价较高,管内阻力较大,不推荐在支管设计中全部改成内螺纹管.

参考文献

[1] 车得福,庄正宁,李　军,等.锅炉[M].2 版.西安:西安交通大学出版社,2008.

[2] 杨　冬,于　辉,高　峰,等.超超临界垂直管圈锅炉水冷壁流量分配及壁温计算[J].中国电机工程学报,2008,28(17):32-38.

[3] 朱玉琴,毕勤成,陈听宽.超临界变压运行直流锅炉中间集箱分配特性的试验研究[J].热能动力工程,2009,24(1):81-84.

[4] 杨　军,朱才广.螺旋管圈直流锅炉水平混合集箱汽水分配特性的试验研究[J].动力工程,1993,13(2):43-47.

[5] Jun K, Young Lee, Sang Yong. Distribution of two-phase annular flow at header-channel junctions[J]. Experimental Thermal and Fluid Science,2004,28(2-3):217-222.

[6] Schmidt J, Giesbrecht H, Vander Geld C W. Phase and velocity distributions in vertically upward high viscosity two phase flows[J]. International Journal of Multiphase Flow,2008,34(4):363-374.

[7] Igor L P, Romney B D, Tyler J D. Hydraulic resistance of fluids flowing in channelsat supercritical pressures[J]. Nuclear Engineering and Design,2004,231(2):187-197.

[8] Sachiyo Horiki, Tomoshige Nakamura, Masahiro Osakabe. Thin flow header to distribute feed water for comapact heat exchangers[J]. International Journal of Multiphase Flow,2008,34(2):128-144.

【责任编辑:蒋亚儒】