AES 算法在 QR 二维码生成识别中的应用

李震

（四川大学锦江学院，四川 眉山 620860）

摘 要：QR 二维码因成本低、存储容量大、存储范围广等特点，已经是世界上应用最广泛的二维码之一。本文探讨了基于 AES 算法对 QR 二维码进行加密、解密的设计，并使用 Java 语言对这一设计进行了实现，以增强 QR 二维码在流通、传播过程中的安全性。

关键词：信息安全；AES 加密算法；QR 二维码；Java

中图分类号：TP391.44；TP309 **文献标识码**：A **文章编号**：2096-4706（2019）21-0144-03

Application of AES Algorithm in QR Two-dimensional Code Generation and Recognition

LI Zhen

（Sichuan University Jinjiang College，Meishan 620860，China）

Abstract：QR two-dimensional code is one of the most widely used two-dimensional codes in the world because of its low cost, large storage capacity and wide storage range. This paper discusses the design of encrypting and decrypting QR two-dimensional codes based on AES algorithm, and implements the design in Java language to enhance the security of QR two-dimensional codes in the process of circulation and transmission.

Keywords：information security；AES encryption algorithm；QR two-dimensional code；Java

1 概述

随着我国移动互联网技术的快速发展，以 QR 码为代表的二维码信息存储、传输和识别技术以其无可替代的高效性、灵活性及低成本等特点，在移动支付、信息共享等日常生活的中迅速普及。然而，利用二维码传播计算机木马、病毒，以及盗窃用户个人信息，导致隐私泄露等问题也屡见不鲜。可以看到，在很多领域中，二维码信息安全都是一个不可忽视、也无法回避的问题，二维码的安全和保密问题也越来越有研究价值[1]。本文探讨了一种通过利用 AES 加密算法对 QR 二维码进行加密的方式来提高二维码信息安全的方法。

2 QR 码简介

QR 码（Quick Response Code）是由日本 DENSO WAVE 公司于 1994 年推出的一种矩阵二维码编码方式，也是目前世界上使用最广泛的二维码编码方式之一。QR 码不仅具有存储信息量大、成本低、误码率低等一些二维码的共通特点，还具有全方位快速识别，可以对包括汉字在内的各种文字、图形、图像等几乎所有数字媒体进行编码等优点。根据 ISO 标准规定，QR 码由包含位置探测图形、分隔符、定位图形、校正图形的功能区和包含格式信息、版本信息、数据和纠错码在内的编码区两部分组成。功能图形区负责定位图像、识别特定图像等，不含有数据信息；编码区主要用于保存数据信息和版本、格式信息，也提供纠错功能[2]。QR 码版本 7 的符号结构示意图如图 1 所示[3]。

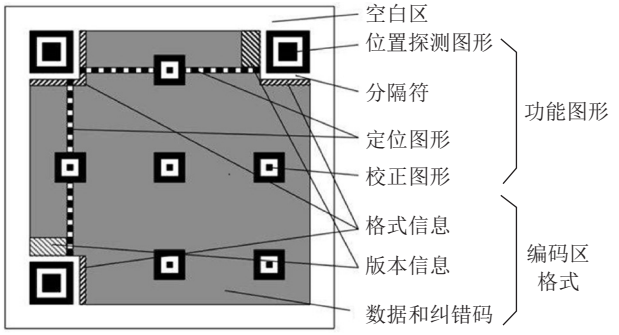

图 1 QR 码结构

如图 1 所示，QR 码的控制信息中本身并没有对数据信息进行加密，且由于 QR 码编码解码的算法本身是公开的，其所携带的信息如果被无关的组织、机构或是个人随意读取，很容易造成不必要的信息泄露、隐私曝光。在以 QR 码为媒介进行敏感信息传递时，需要有一种简单、快速、有效的加密手段。

3 AES 算法原理

作为 DES 算法的升级替代，AES 算法（Advanced Encryption Standard）自 2000 年正式公布以来，其安全、可靠、简单、快速的特性已被多方分析研究检证。作为当前最为常见的对称加密算法之一，在全世界范围内有着广泛的应用。AES 算法加密的数据块和密钥长度相同，分为 16 字节、

收稿日期：2019-08-26

24 字节和 32 字节三种。密钥越长，其加密的轮次越多，安全性也越强。下面以 16 字节密钥为例，对 AES 算法原理进行简单说明 [4]。

AES 算法在加密时的输入包括同为 16 字节的明文和密钥，输出为 16 字节的密文。明文和密钥都可以被看作是一个 4*4 的字节矩阵。算法包括密钥扩展（KeyExpansion）、轮密钥加（AddRoundKey）、字节替换（SubBYtes）、行移位（ShiftRows）、列混淆（MixColumns）等步骤。

（1）密钥扩展：通过一个混合操作将初始密钥扩展成多个 16 字节的轮密钥，供后面的轮加密使用；

（2）轮密钥加：当前状态与轮密钥进行按位 XOR 异或运算；

（3）字节替换：利用一个 S 盒完成一个状态到下一状态中字节的一一映射；

（4）行移位：将状态中的每行分别向左偏移 0，1，2，3 个字节；

（5）列混淆：将状态中的每列独立操作，与一个固定的多项式进行模乘，使每列中的每个字节都被映射为一个新的值。

加密的过程如图 2 所示。输入的密钥经过密钥扩展，与明文做第一次轮密钥加。之后按照字节替代、行移位、列混淆、轮密钥加的顺序完成一轮的加密，加密的中间结果称为状态（State）。中间状态和相对应轮的轮密钥继续进行重复的多轮次变换（16 字节密钥为 10 轮，其中最终轮不需要列混淆），最终达到高强度的加密效果，输出最终的密文。

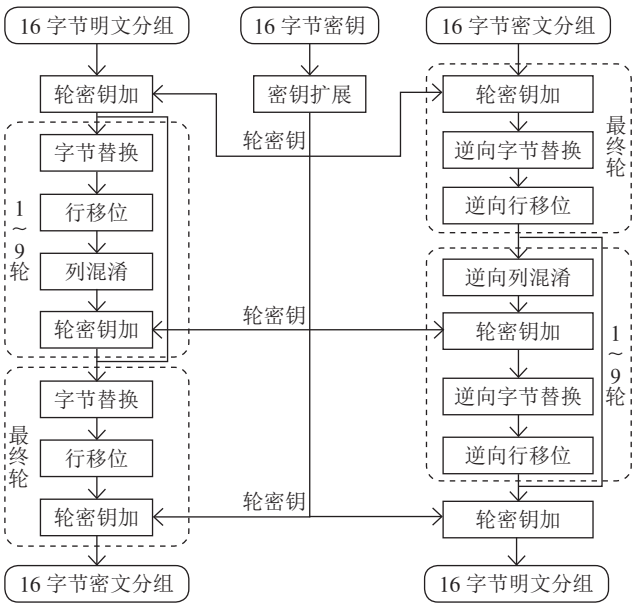

图 2　AES 算法结构

解密过程输入 16 字节密文，使用与加密过程中相同的密钥，运算过程与加密相反，如图 2 所示，其中使用的 S 盒的字节替代、线性变换的行移位和列混淆均为原运算方式的逆向运算。同样地，对应着加密的最终轮，最先进行的解密轮次也不需要进行逆向列混淆。经过总共 10 轮的变换，输出 16 字节明文，达到解密的目的。

4　应用 AES 算法对 QR 二维码加密解密

基本思路是在 QR 二维码编码前，应用 AES 算法对原始数据进行加密。再对密文进行 QR 码编码，这样即使该 QR 二维码在传播过程中被不相干的组织或者个人获取，也无法破译。需要获取该二维码信息时，在读取 QR 码前，输入与加密时相同的密钥，即可获取到原始的信息。

限于篇幅，本文只展示加密过程实现的主要代码。

4.1　加密过程的实现

（1）手动输入的密钥安全性低，且长度不容易控制，这里选择通过 KeyGenerator 类生成 128 位的随机源，再转换成 AES 算法可用的原始对称密钥的方式来创建密钥，并对该密钥进行保存，以备解密使用。

```
KeyGenerator keyGenerator;// 生成 key
keyGenerator = KeyGenerator.getInstance("AES");
keyGenerator.init(128);// 生成一个 128 位的随机源
SecretKey secretKey = keyGenerator.generateKey();
byte[] keyBytes = secretKey.getEncoded();// 产生原始对称密钥
Key key = new SecretKeySpec(keyBytes, "AES");
```

（2）以字节数组形式获取待加密的明文数据，并对明文数据进行 AES 算法加密。

```
Stingcontext = " 测试内容 ";// 待加密明文
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
cipher.init(cipher.ENCRYPT_MODE,key);// 指定加密模式，输入密钥
byte[] resultAes = cipher.doFinal(context.getBytes());
```

（3）得到的密文通过 ZXing 类库提供的编码模块进行 QR 二维码编码，并将结果以 png 格式写入指定的文件中保存。

```
Hashtable hintsAes = new Hashtable();// 创建 QR 编码参数的哈希表
hintsAes.put(EncodeHintType.CHARACTER_SET, "utf-8");
BitMatrix bitMatrixAes = new MultiFormatWriter().encode(new String(resultAes), BarcodeFormat.QR_CODE, 300, 300, hintsAes);// 输入密文，执行 QR 码编码
File outputFileAes = new File("d:" + File.separator + "QRPictureAes.png");
QRUtil.writeToFile(bitMatrixAes, "png", outputFileAes);
```

4.2　解密过程

（1）通过移动设备摄像、外部图片导入等方式，将保存的图片以比特流的形式读入系统；

（2）利用 ZXing 类库提供的解码模块，对读入的 QR 二维码进行解码，得到 AES 算法加密后的密文；

（3）输入与加密时相同的 16 字节密钥，对密文形式的 QR 二维码利用 AES 算法进行解密，得到最终的明文结果。

根据图 3 和图 4 的对比可以看出，虽然同样使用的是 QR 二维码编码，但是经过 AES 加密可形成完全不同的图形编码。对图 4 经过 AES 算法加密后的 QR 码进行识别，其结果如图 5 所示，读取到加密后的密文在不知道密钥的前提下几乎无法破译。用相应的密钥对图 4 中加密后的 QR 码进行解密，解密后的识别结果如图 6 所示，利用正确密钥对经过 AES 算法加密的 QR 码解密，则可以快速地还原出原始的数据。

图 3　未经加密生成的 QR 码

图 4　经过 AES 算法加密的 QR 码

图 5　图 4 未解密的识别结果

图 6　AES 算法对图 4 解密后的识别结果

5　结　论

本文对 QR 二维码与 AES 算法的基本原理进行了归纳总结，并提出了在 QR 二维码编码前，生成随机密钥对原始数据使用 AES 算法加密的方法，将 QR 二维码生成识别与 AES 加密算法两种技术合理有效地结合起来，是对二维码存储、传播、识别过程中存在的信息安全问题的一种快速、简单的解决方案，并且利用 Java 语言对该方案进行实现，为进一步深入研究实现更加灵活高效的 QR 二维码信息安全提供了思路，具有一定的研究价值和较强的实用性。

参考文献：

[1] 单利安 .QR 二维码水印加密及解密算法研究 [J]. 无线互联科技，2013（10）：122-123.

[2] 李逢玲，郑飞 .RSA 加密算法在 QR 二维码上的应用探讨 [J]. 中小企业管理与科技（上旬刊），2014（11）：207-208.

[3] 张定会，单俊涛，江平 .QR 码 DES 加密与解密 [J]. 数据通信，2011（3）：40-42.

[4] 陈彦龙，杨立波 .AES 算法的研究与实现 [J]. 中国科教创新导刊，2012（28）：34+36.

作者简介：李震（1985-），男，汉族，湖南隆回人，专职教师，助教，硕士研究生，研究方向：信息系统开发、软件工程。

（上接 143 页）可以由目标系统控制，限制用户在进行某项操作时只能登录指定的机器。另外，系统管理员对于可疑用户或非法登录用户可以发送指令立即终止该用户的所有操作。

4　结　论

综上所述，计算机通信网络技术越来越成熟，因为其具有访问方便的特点，所以较为容易被破解，也就极有可能在信息传输的过程中被盗取，会给系统安全带来不良影响，因此安全防护体系在计算机通信网络安全中发挥着重要的作用，技术人员应提高自身能力水平，运用先进的技术，对计算机网络进行保护，保证网络信息的安全。

参考文献：

[1] 杨建平 . 计算机通信网络安全防护体系的设计及应用探讨 [J]. 电脑知识与技术，2018，14（29）：71-72.

[2] 曹彬，黄枭 . 浅谈计算机通信网络安全防护体系的设计及应用 [J]. 中国新通信，2018，20（10）：142.

[3] 吕卫昕 . 计算机通信网络安全防护体系设计与实现 [J]. 信息与电脑（理论版），2018（4）：172-173.

作者简介：张然（1986-），女，汉族，安徽灵璧人，硕士，工程师，研究方向：信息技术；胡静静（1986-），女，汉族，安徽合肥人，硕士，讲师，研究方向：电子技术；王铁栋（1974-），男，汉族，山东济南人，博士，讲师，研究方向：信息技术。