非侵入式负荷监测系统数据隐私保护方法研究*

陈子秋[1],冯瑞珏[1],郑扬富[1],刘嘉昕[1],曾献煜[1],王智东[2]
(1.华南理工大学广州学院 电气工程学院,广东 广州 510800;
2.华南理工大学 电力学院 智慧能源工程技术研究中心,广东 广州 510640)

摘 要:非侵入式负荷监测技术有助于用电精细化管理,但细粒度的电力消费数据也导致了用户隐私信息暴露在攻击者面前。首先分析了非侵入式负荷监测数据所面临的安全风险,并从密码学角度提出了基于AES+RSA的混合加解密信息安全方案。方案采用对称算法AES加密数据、非对称算法RSA加密AES密钥来实现高效的密钥管理。利用Visio Studio 2017+Qt软件开发测试界面,通过数据总线将算法写入STM32单片机进行方案性能测试,优选出最佳的运行模式,同时验证了混合加解密方案的有效性。总结得到,方案的耗时长短取决于RSA算法的加解密或签名验签的效率。

关键词:非侵入式负荷监测系统;AES;RSA;隐私保护
中图分类号:TN606 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.201112

中文引用格式:陈子秋,冯瑞珏,郑扬富,等. 非侵入式负荷监测系统数据隐私保护方法研究[J].电子技术应用,2021,47(12):116-119,125.
英文引用格式:Chen Ziqiu,Feng Ruijue,Zheng Yangfu,et al. Research on data privacy protection method of NILM[J]. Application of Electronic Technique,2021,47(12):116-119,125.

Research on data privacy protection method of NILM

Chen Ziqiu[1],Feng Ruijue[1],Zheng Yangfu[1],Liu Jiaxin[1],Zeng Xianyu[1],Wang Zhidong[2]
(1.College of Electrical Engineering,Guangzhou College of South China University of Technology,Guangzhou 510800,China;
2.Research Center for Smart Energy Technology,School of Electric Power Engineering,South China University of Technology,Guangzhou 510640,China)

Abstract:Non-invasive load monitoring technology is helpful to fine management of electricity consumption,but the fine-grained power consumption data also leads to the exposure of users' private information to attackers. This paper firstly analyzes the security risks faced by non-intrusive load monitoring data,and proposes a mixed encryption and decryption information security scheme based on AES+RSA from the perspective of cryptography. In this scheme,symmetric algorithm AES is used to encrypt data,and asymmetric algorithm RSA encrypts AES keys to realize efficient key management. Using Visio Studio 2017+Qt software development and test interface,the algorithm was written to STM32 microcontroller through the data bus for scheme performance test,the best operation mode was optimized,and the effectiveness of the mixed encryption and decryption scheme was verified. It is concluded that the time of the scheme depends on the efficiency of RSA encryption and decryption or signature verification.

Key words:NILM;AES;RSA;privacy protection

0 引言

非侵入式负荷监测(Non-Intrusive Load Monitoring,NILM)装置为装载于智能电表的模块,通过测量并分析电力入口处的功率、电压、电流等电量信号,获取系统内各用电负荷的运行状态数据[1]。NILM装置能准确统计和呈现出各用电设备的用电量及用电时间,帮助用户改善用电习惯,节约用电,但缺乏可靠保护,极易被追踪和攻击,存在数据信息泄漏的风险[2]。国家密码局常用的加密算法是SM系列加密算法,文献[3]运用国密算法SM2与SM4加密武器装备的数据,并验证了可行性。国际上流行使用的加密算法较多,如DES、AES、RSA等,文献[4]利用其中的DES与AES算法来保障网络环境下安全通信和信息传输的安全。本文分析了NILM数据安全所面临的风险,在国内外现有的密码技术中寻找最佳的密码技术加密方案。利用STM32单片机平台进行方案测试和数据处理分析,最终验证了方案的有效性和耗时长短。

1 NILM数据安全风险分析

NILM系统结合智能电网,通过互联网进行数据传输,

*基金项目:华南理工大学广州学院杰出青年教师项目(JQ180001)

实现交互。电力信息安全性主要有完整性、有效性和机密性。完整性要求保证数据信息不被篡改，影响数据的真实性和可用性，如不法用户篡改用电数据，进行商业欺诈；有效性要求防止被伪装和接收错误指令，如冒充合法用户，导致接收方被错误引导并做出损害自身权益的行为；机密性是重中之重，若保密性无法保障，直接影响数据的完整性和有效性，会造成用户信息泄露、行为暴露，涉及隐私安全等诸多问题[5]。

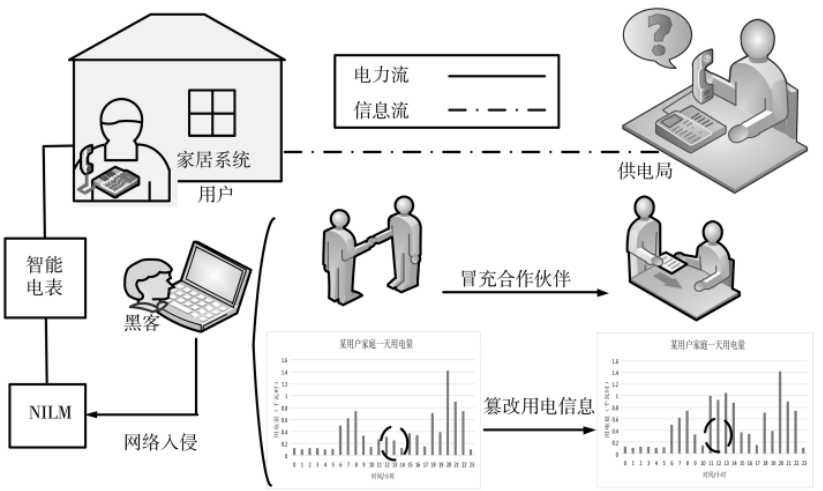


图 1 黑客攻击 NILM 系统

图 1 展示了黑客攻击 NILM 系统的途径和方式，主要包括：(1)监听攻击，黑客截取用电大数据内容，通过 NILM 负荷分解和数据分析处理，窃取用户的身份信息和活动隐私，用户像在黑客的“监听”下生活；(2)篡改攻击，不法用户篡改用电数据，进行偷电等违法行为；(3)冒充攻击，黑客利用截获的身份信息，假冒合法用户或电力公司，给对方发送有损利益的指令，造成更大的利益损失[6]。

2 数据隐私方案

常见的加密算法包括对称加密算法和非对称加密算法[7]。AES 是一种对称加密算法，其具备计算速度快、使用长密钥时难破解两方面的特点，在信息安全保护方面，广泛运用于加密敏感大数据[8]；RSA 是一种非对称加密算法，其安全性很高，且具备签名验签功能，防止信息被篡改，但 RSA 算法计算速度慢，适合加密数据长度短、有高安全性要求的信息保护场景[9]。NILM 系统信息交互频繁、数据流量大[10]，为了保证用户信息数据安全，本文提出一种 AES+RSA 混合加密数据隐私保护方案。

AES+RSA 混合加密方案如图 2 所示。发送方和接收方都会生成一对 RSA 密钥，私钥自己保留，公钥对方

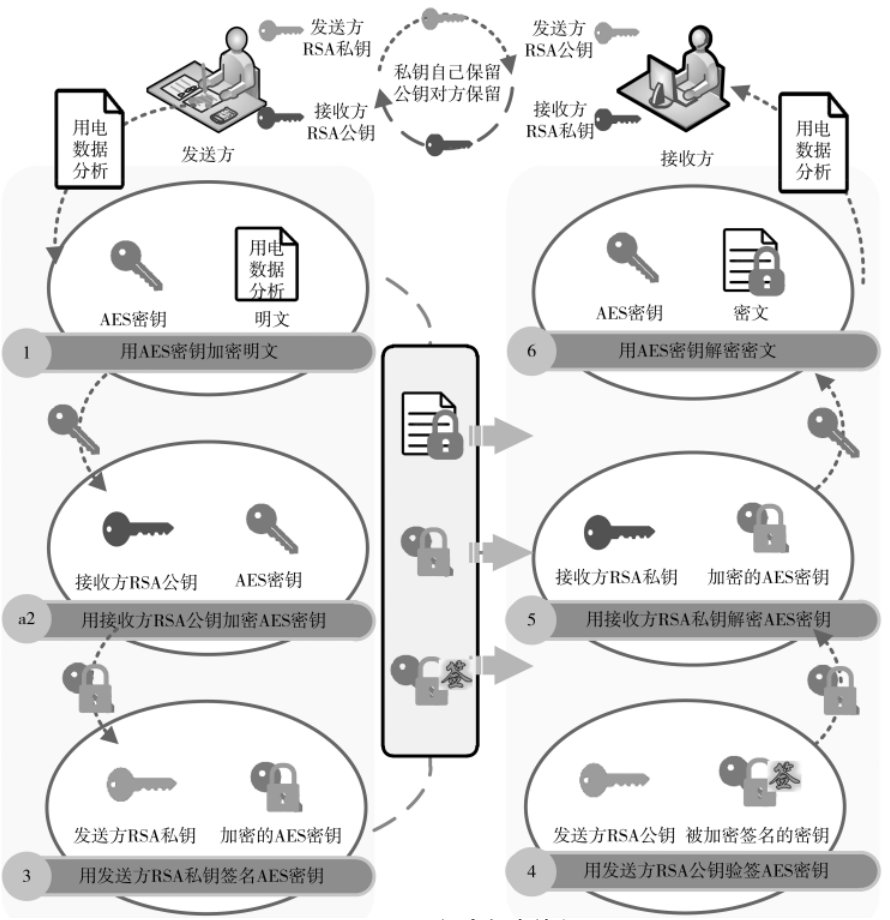


图 2 AES+RSA 混合加密流程图

保留[11]。发送方将用电数据分析(明文)发送给接收方流程如下：

(1)发送方使用 AES 密钥加密用电数据分析(明文)生成密文；

(2)发送方使用接收方 RSA 公钥加密 AES 密钥；

(3)发送方使用自己的 RSA 私钥签名 AES 密钥，并将密文和已加密签名的密钥发送给接收方；

(4)接收方使用发送方 RSA 公钥验签，判断发送方的真实身份；

(5)接收方使用自己的 RSA 私钥解密，生成 AES 密钥；

(6)接收方使用 AES 密钥解密密文，得到用电数据分析(明文)。

3 方案性能测试

混合加密算法为 NILM 系统信息安全提供了一定的保障。在主频为480 MHz、型号为 STM32H743IIT6 的 ARM 芯片搭建的平台上，实现验证混合加解密算法的效率。在计算机中利用 Visual Studio 2017+Qt5 工具开发测试界面，界面显示算法、算法模式、密钥长度、明文数据和加密后的密文。从 OpenSLL 算法开源库中抽取的 AES 和 RSA 算法通过串口下载到单片机开发板中进行耗时性能测试。

3.1 AES 性能测试

AES 分为 ECB、CBC、OFB、CFB 和 CTR 共 5 种工作模式。为了解 AES 在各种工作模式下数据长度与加解密耗时的关系，以 1 000 B 为间隔，测试了 20 组不同数据长度在不同工作模式、不同密钥长度下的加解密耗时情况，并进行分析处理。

如图 3 所示，5 个工作模式所呈现的趋势相同，加密耗时均随明文长度的增加而增加，$R^2=1$，呈正相关的关系。除 CTR 模式外，其余 4 种工作模式的回归方程斜率基本相同。而 CTR 模式回归方程的斜率稍大于其他模式，即 CTR 模式的加解密耗时相对较长。根据 AES 各模式的工作原理，ECB 和 CBC 为块加密模式，CFB、OFB 和 CTR 为流加密模式，流加密模式比块加密模式安全系数高，且 CTR 模式设置了时钟计数步骤[12]。结合安全系数和加解密效率，CTR 模式是 ARS 工作模式的最优选择。

分别测试了 CTR 模式在 128 bit、192 bit 和 256 bit 3 种密钥长度下加解密的耗时状况。从耗时比例图可得，密钥长度越长，加解密耗时越长，128 bit 的加解密速度最快，随着密钥长度的增加，加解密的时间也随之增加，从 128 bit 到 192 bit，再到 256 bit，每个阶梯耗时增幅为 13%，增幅较大。效率是选择的重要因素，综上考虑，方案采用 AES-128-CTR 加密数据。

3.2 RSA 性能测试

RSA 算法密钥长度有 1 024 bit 和 2 048 bit 两种，国际常用的是 RSA-2048 bit 算法。密钥长度越长，破解难度越大[13]。出于安全性方面考虑，选择用 RSA 密钥长度为 2 048 bit 去加解密 AES 的密钥和签名验签，测试结果如图 4 所示。

由图 4(a)和图 4(b)对比得出，RSA-2048 bit 的解密与签名耗时较长，适合加密长度较短的 AES 密钥。由于RSA 算法是块加密算法，填充模式大部分是自填充模式[14-15]。以 2 048 bit 密钥长度为例，在加密明文时若明文长度不足256 B，加密进行前会在不足256 B 的明文前面填充 0，长度填充到 256 B 才开始加密，经过填充后都为相同的明文长度，所以加密的时间都不受明文长度变化而影响，同理，签名验签和加解密的算法原理一样。

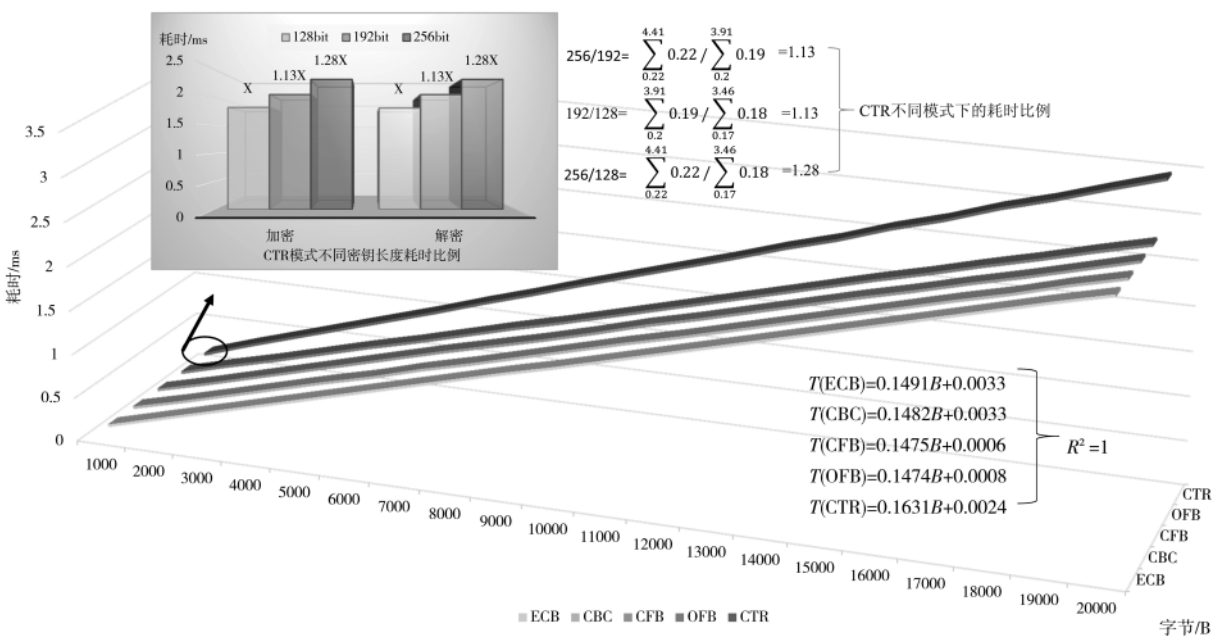
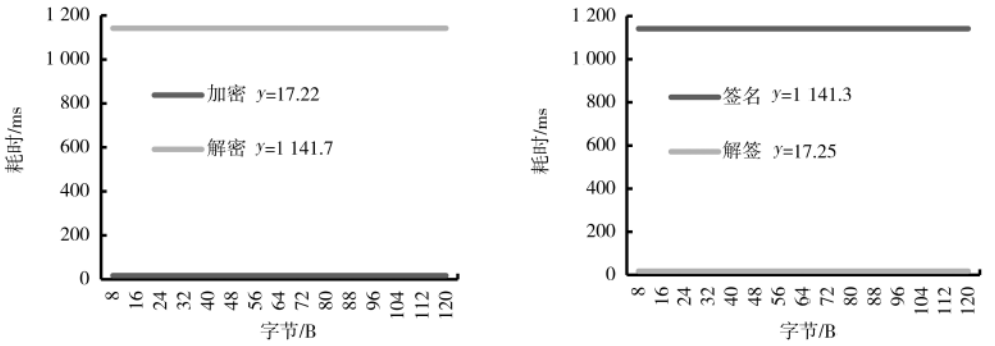


图 3 AES 各模式下明文长度对加密时间的影响



(a)RSA 加解密时间特性图　　(b)RSA 签名验签时间特性图

图 4　2 048 bit 密钥长度的加解密和签名验签效率

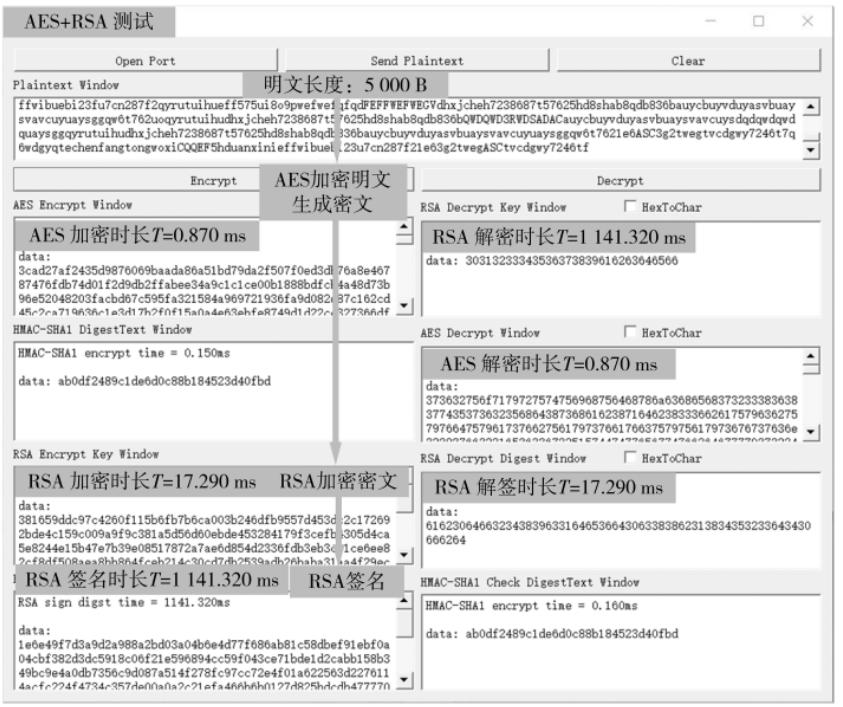


图 5　混合加密方案测试

两者在作用层面上不一样，加密是为了保证信息安全，签名是为了防止信息被篡改，签名和验签相当于多了一道防御系统，让整个系统更完善。

3.3 总方案性能测试

如图 5 所示，以明文长度5 000 B 为例，对 AES-128-CTR+RSA-2048 的混合加解密方案进行了耗时性能测试，软件左边的框图为测试的 AES 加密明文时长、RSA 加密密钥时长以及签名的时长，右边的框图为解密的过程以及时长。加密的明文与解密所得的明文完全一致，没有明显误差，证明 NILM 组合密码方案有效。

4 结论

本文针对非侵入式负荷监测数据存在用户隐私泄露的安全问题，提出了一种基于 AES+RSA 的混合加解密方案，并对方案进行了耗时性能测试，测试结果如下：

(1)AES 的耗时性能测试表明：AES 各模式的耗时与明文长度呈线性关系。CTR 模式在相同明文长度下，密钥长度越长，耗时呈阶梯式上升。本方案选择 AES-128-CRT 模式对用电数据进行加密。

(2)RSA-2048 bit 的耗时性能测试表明：RSA 解密和签名时间耗时较长，且加解密和签名验签时间都不受明文长度变化而影响，适合加密长度较短的 AES 密钥。

(3)AES-RSA 混合加解密方案测试表明：RSA 在组合加解密耗时中占主导地位，经过加解密和签名验签前后明文不失真，数据完整，本方案有效可行。

参考文献

[1] 邓晓平，张桂青，魏庆来，等.非侵入式负荷监测综述[J/OL].自动化学报：1-21[2021-02-24].https://doi.org/10.16383/j.aas.c200270.

[2] 王文丽，解绍锋，王谷城，等.基于非侵入式负荷监测的

(下转第 125 页)

Signal Processing, 2014, 80(2): 233-241.
[9] WANG Y, ZHU Z, YAO J, et al. A 0.45-V, 14.6-nW CMOS subthreshold voltage reference with no resistors and no BJTs[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2015, 62(7): 621-625.
[10] 辛晓宁, 张雷. 一种宽输入电压范围高 PSRR 线性稳压器[J]. 电子设计工程, 2016, 24(17): 185-187.
[11] LU T, ZHANG J, ZONG Y. A Low-quiescent current low-dropout regulator with wide input range[J]. International Journal of Electronics and Electrical Engineering, 2015, 3(3): 182-186.
[12] HENG S, PHAM C K. A low-power high-PSRR low-dropout regulator with bulk-gate controlled circuit[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2010, 57(4): 245-249.
[13] LEUNG K N, MOK P K T, KI W H. A novel frequency compensation technique for low-voltage low-dropout regulator[C]//IEEE International Symposium on Circuits and Systems, IEEE, 1999: 102-105.
[14] RAZAVI B. The bandgap reference a circuit for all seasons[J]. IEEE Solid-State Circuits Magazine, 2016, 8(3): 9-12.
[15] CHONG S S, CHAN P K. A 0.9-μA a quiescent current output-capacitorless LDO regulator with adaptive power transistors in 65-nm CMOS[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2013, 60(4): 1072-1081.
[16] HENG S, PHAM C K. A low-power high-PSRR low-dropout regulator with bulk-gate controlled circuit[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2010, 57(4): 245-249.
[17] KEIKHOSRAVY K, MIRABBASI S. A 0.13 μm CMOS low-power capacitor-less LDO regulator using bulk-modulation technique[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2014, 61(11): 3105-3114.
[18] KWOK K C, MOK P K T. Pole-zero tracking frequency compensation for low dropout regulator[C]//IEEE International Symposium on Circuits and Systems, 2002, ISCAS 2002. IEEE, 2002: 735-738.

(收稿日期: 2020-11-12)

作者简介:
吴霞(1974-), 女, 硕士, 实验师, 主要研究方向: 电子电路设计与应用。
鲍言锋(1992-), 男, 硕士研究生, 主要研究方向: 模拟集成电路设计。
邓婉玲(1980-), 女, 副教授, 硕士生导师, 主要研究方向: 新型半导体器件与模拟集成电路设计。

扫码下载电子文档

(上接第 119 页)

日常活动监测[J]. 电工技术, 2020(12): 52-55.
[3] 方轶, 丛林虎, 邓建球. 基于国密算法的武器装备数据混合加密方案[J]. 探测与控制学报, 2020, 42(1): 121-126.
[4] 李晶, 宋小明. 密码技术在网络安全中的应用研究[J]. 内蒙古科技与经济, 2020(1): 58-59.
[5] 赵磊. 智能电网中电力用户隐私安全研究[D]. 长沙: 长沙理工大学, 2018.
[6] 温伟强. 网络攻击技术与网络安全探析[J]. 网络安全技术与应用, 2015(1): 79-81.
[7] 李彬. 浅谈非对称加密方式及其应用[J]. 信息记录材料, 2021, 22(1): 214-215.
[8] 姚华桢. 一种基于 AES 算法的流媒体加密方法[J]. 中国有线电视, 2006(2): 153-157.
[9] 鲍海燕, 芦彩林. 基于改进 RSA 算法的隐私数据集同态加密方法[J]. 太赫兹科学与电子信息学报, 2020, 18(5): 929-933.
[10] 张露. 非侵入式负荷监测算法研究[D]. 广州: 华南理工大学, 2019.
[11] 李淑敬, 李林国. RAS 算法在 VFP 中数字签名的实现[J]. 西安文理学院学报(自然科学版), 2013, 16(4): 58-61.
[12] 乐丁惕. 基于 CTR 操作模式的 AES 算法加密组件的研究[J]. 长春工程学院学报(自然科学版), 2012, 13(4): 117-118, 122.
[13] 张乐星. 基于 AES 和 RSA 的网络数据加密方案[J]. 科技通报, 2004(6): 539-541.
[14] 李学锋, 陈丹. 公开密钥密码体制与 RSA 算法[J]. 襄阳师专学报, 1998, 19(2): 62-64.
[15] 陈刚. 基于数据加密算法的计算机通信安全技术[J]. 九江学院学报(自然科学版), 2020, 35(4): 68-70, 74.

(收稿日期: 2020-11-14)

作者简介:
陈子秋(1997-), 男, 本科, 主要研究方向: 信息技术安全与应用。
冯瑞珏(1985-), 通信作者, 女, 硕士, 讲师, 主要研究方向: 信息技术安全与应用, E-mail: fengrj@gcu.edu.cn。

扫码下载电子文档

版权声明