一种煤矿安全监控系统数据加密算法

朱 沙 沙
(天地(常州)自动化股份有限公司 江苏 常州 213000)

摘 要 近年,国家颁布了《煤矿安全监控系统升级改造技术方案》,方案中说明对于敏感数据需做加密处理。研究常用的加密算法,其中包括 DES、3DES、RSA 三种加密算法方案,并且结合煤矿安全监控系统数据的特殊性,兼顾安全和高效,提出一种 3DES-RSA 混合加密算法。经分析该混合算法综合了 3DES 和 RSA 的优点,是一种适合煤矿安全监控系统的加密算法。

关键词 DES 3DES RSA 煤矿安全监控 加密 解密

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.11.052

A DATA ENCRYPTION ALGORITHM IN COAL MINE SAFETY MONITORING SYSTEM

Zhu Shasha
(*Tiandi(Changzhou) Automation Co., Ltd., Changzhou 213000, Jiangsu, China*)

Abstract It is stated that the sensitive data should be encrypted in Technology schemes of upgrading of coal mine safety monitoring and control system. This paper deeply analyzes common encryption algorithm (such as DES、3DES、RSA). According to the particularity of coal mine monitoring control system, a hybrid algorithm called 3DES-RSA is proposed combining safety and high efficiency. After analysis, the hybrid algorithm integrates the advantages of 3DES and RSA, and is a suitable encryption algorithm for coal mine monitoring control system.

Keywords DES 3DES RSA Coal mine safety monitoring Encryption Decryption

0 引 言

煤矿安全监控系统主要是对井下环境参数的监测[1-2],并根据监测出的数据做出相应的控制命令策略。在国家安全标准 6201 - 2006《煤矿安全监控系统通用技术要求》[3] 中明确规定,对于敏感数据,软件必须保证其不可以被篡改。2015 年底,《煤矿安全监控系统升级改造技术方案(征求意见稿)》[4] 发布并将“增加加密存储要求”这一规则正式纳入方案中。本文在煤矿安全监控系统数据特殊性基础上,经过对 DES、3DES、RSA 三种加密算法的深入研究比较,提出一种适用于煤矿安全监测系统的 3DES-RSA 混合算法,并对该算法性能做实验测试,证明该混合算法适用于煤矿安全监测系统。

1 常用数据加密方法

1.1 DES

DES 属于一种分组加密算法。加解密使用相同的 8 字节密钥,明文和密钥进行一系列的置换等复杂运算后最终加密数据。

DES 的优点:密钥较短,加密处理简单,速度快,且密文和明文长度大致相同,适合煤矿安全监控系统海量数据加密的场景。DES 的缺点:密钥安全性不足,且如果通信方是多个,每个通信方发送一个密钥,密钥的管理成本较高。

3DES,即三重 DES 加密,和 DES 算法没有本质区别。DES 面临的主要问题是密钥长度短,容易被穷举攻击,随着芯片计算能力的提升,DES 更容易被暴力破

收稿日期:2019 - 06 - 05。监控类软件平台、框架研究及示范项目(2018GY003)。朱沙沙,硕士生,主研领域:计算机软件技术。

解。而 3DES 密钥长度是 DES 的 3 倍,弥补了 DES 安全性能不足的情形。

1.2 RSA

RSA 是非对称算法,加解密使用不同的密钥。两个密钥都可以用于加密,解密时需要使用另一个密钥。但是,通常用公钥加密,私钥解密,而公钥是公开的,持有公钥的用户均可以对私钥加密后的数据进行解密。

理论上 A 和 B 之间要通过 RSA 实现保密通信,需要 A 和 B 各自生成一组密钥,同时保存好自己的密钥;用对方的公钥加密要发送的消息,用自己的私钥解密对方发送过来的消息。RSA 加密时,对要加密数据的大小有限制,最大不大于密钥长度。

例如在使用 1 024 bit 的密钥时,最大可以加密 1 024/8 = 128 Bytes 的数据。数据大于 128 Bytes 时,需要对数据进行分组加密,分组加密后的加密串拼接成一个字符串后发送给客户端。如果 RSA 加密过程中使用的填充方式为 RSA_PKCS1_PADDING[5],则明文长度最多只能是 128 - 11 = 117 Bytes,如果超出,必须切割分组加密。

1.3 比较总结

根据上述分析,从三个方面总结可得[6]:

(1) 加密速度。DES 加密速度最快,3DES 由于采用三重加密,速率是 DES 的三分之一,RSA 最致命的缺点就是加解密速度很慢。

(2) 安全性。3DES 密钥长度是 DES 的三倍,弥补了 DES 安全性的弱点。RSA 算法的安全性和大素数的位数有关,当素数位数够大时,RSA 安全性最高。

(3) 密文长度。DES 加密后的密文长度是 8 字节的整数倍,如果明文长度不够 8 字节,则自动补全。3DES 和 DES 的密文长度相同。而 RSA 的密文长度由密钥的长度决定,通常为了保证安全性,RSA 的密钥长度不能低于 1 024 位,即 128 字节,除去 7 字节保留位,RSA 的密文长度至少为 121 字节。

2 煤矿安全监控系统数据特点

安全监控系统所采集的数据主要是一些有害气体和设备的实时数据,按照国家煤炭安全的标准,每个传感器设备平均每秒产生 1 条实时离散数据,并且在现实煤矿部署中,通常情况下会有几百甚至几千个传感器设备。以瓦斯传感器为例,如果按照一年 1 000 个传感器计算,每个传感器一年产生数据约 3 000 万条,1 000 个传感器产生数据总量约为 300 亿条,每条数据由瓦斯传感器编号、瓦斯值、数据发送时间三个属性组成。由此可知,安全监控系统中数据具有总量大、发送速率快和数据值小三个特点。

基于以上分析结论并结合煤矿安全监控系统数据特殊性综合考虑,本文提出采用 3DES-RSA 混合加密算法的存储方案。3DES-RSA 混合加密算法的优势如下:

(1) 3DES-RSA 加解密速度介于 RSA 和 DES 之间,稍弱于 DES 算法,解决了 RSA 加解密算法慢的致命弱点。

(2) 3DES-RSA 产生的密文长度和明文大致相当,大大节省数据库文件存储空间。

(3) 3DES-RSA 较 DES 加长了密钥长度,增强了安全性。

所以,从理论上来说,采用 3DES-RSA 混合算法,可以弥补各自的缺点,更好地提高数据存储的加密性能和安全性,是一种适合煤矿安全监控系统的数据混合加密算法。

3 3DES-RSA 算法设计

3DES-RSA 混合算法原理如图 1 所示。该算法用 DES 算法加密明文数据,同时对 DES 算法所用的密钥进行 RSA 算法加密。将密文和加密之后的密钥一起打包发送给接收方。接收方在接收到数据包之后,先对密钥密文进行解密,获取 DES 算法的加密密钥。因为 DES 算法的加密和解密用的相同密钥,所以获取密钥之后就可以对密文进行解密。

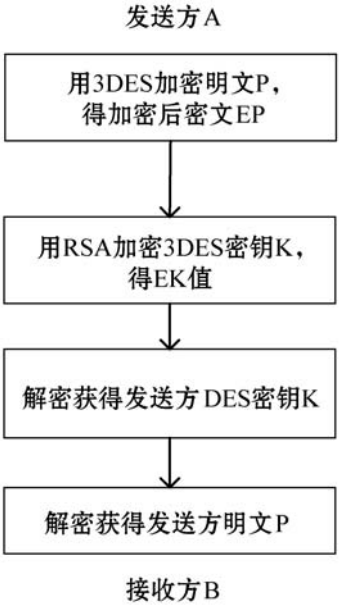

图 1　3DES-RSA 混合加密算法原理

3DES-RSA 混合加密算法实现流程如下：

（1）由素数生成算法可以得到多个素数[7]，选择其中较大的两个大素数 p 和 q。通过前面所述 RSA 加密算法可以得到公开密钥和私有密钥，并将公开密钥公布出去，保存私有密钥。

（2）由 3DES 算法产生的 128 位随机数，即密钥，对明文信息进行加密。

（3）用 RSA 算法的公钥对 3DES 算法的密钥进行加密并经过网络传输给接收方。接收方对接收的密文信息用 RSA 生成的密钥进行解密得到 3DES 算法的加密密钥，然后再对 DES 算法的密文进行解密。

4 实验测试

分别对 RSA 和 3DES-RSA 两种加密算法的存储和查询性能进行测试。

4.1 测试要求和环境配置

（1）1 000 个传感器同时产生数据，每个传感器平均每年产生数据 3 000 万条，要求一张表存储一个传感器的数据，1 000 个传感器即对应 1 000 张表，每张表一年存储约 3 000 万条记录。

（2）存储性能大于每秒 10 000 条记录。

（3）数据库文件不得大于 2 TB。

（4）为了便于恢复数据，日志模式设置成完整模式，并且日志文件大小不得大于 2 GB。

（5）数据库内存最大值设置成服务器内存的四分之一（本文是 4 GB）。

（6）在查询测试的流程中，需边执行插入操作边查询数据。

测试软硬件环境配置如表 1 所示。

表 1 测试环境配置

硬件	操作系统：Windows server 2012 R2
	处理器：i7-7700K CPU
	内存：16 GB
	硬盘：1.8 TB 机械硬盘
软件	Sqlserver 2012 标准企业版
	Visual Studio 2017

4.2 数据构造

在安全监控系统中，传感器测点的数据值为核心数据，比如瓦斯值，本文以瓦斯传感器为例，构造瓦斯值主数据[8-9]如表 2 所示。

表 2 构造数据结构

属性	类型	说明
ItemID	Bigint	传感器编号，如 123456
ItemValue	Decimal	瓦斯值，如 90.64
Sendtime	Datetime	数据上传时间

说明：出于加密安全性考虑，且 3DES 是对字符串进行加密，故规定对应的表字段 ItemID、Itemvalue 类型设置为 varchar（50），ItemSendTime datetime 数据类型转换成 int 类型入库存储。

4.3 RSA 加解密算法测试

1）编写加密算法。

（1）设置密钥长度 KEYSIZE 为 1 024 位。

（2）以 KEYSIZE 为参数，生成 RSA 加密服务实例 RSACryptoServiceProvider。

（3）RSACryptoServiceProvider 生成私钥 PrivateKey 和公钥 PublicKey。

（4）将所需加密的明文转换成字节型数组 BPlainText。将公钥导入到 RSACryptoServiceProvider。

（5）通过 RSACryptoServiceProvider 的 Encrypt（）方法加密明文，并将密文转换成字符串。

2）编写解密算法。

（1）设置密钥长度 KEYSIZE 为 1 024 位。

（2）以 KEYSIZE 为参数，生成 RSA 加密服务实例 RSACryptoServiceProvider。

（3）RSACryptoServiceProvider 生成私钥 PrivateKey 和公钥 PublicKey。

（4）将所需解密的密文转换成字节型数组 EncryptText。将私钥导入到 RSACryptoServiceProvider。

（5）通过 RSACryptoServiceProvider 的 Decrypt（）方法解密密文，并将解密后的明文转换成字符串。

3）构造 20 个线程，同时往 1 000 张表里面插入加密后的数据，统计平均存储速率。

4）加密存储性能数据如表 3 所示。

表 3 加密存储的性能实验数据

线程数	表数据量/万	平均存储速度/（条·s^{-1}）
20	200	2 400

5）查询和解密性能数据如表 4 所示。

表 4 解密性能实验数据

查询数量	耗时/ms
5 000	16 400
8 000	33 781

4.4　3DES-RSA 加解密算法性能测试

1）编写加密算法。

（1）设置 64 ×3 位密钥长度 KEYSIZE,并自定义公共密钥值_PKEY 和初始向量_*IV*。

（2）将需要加密的明文 plainText 转换成字节型数组 BPlainText。

（3）实例化 3DESCryptoServiceProvider 类,并通过 CreateEncryptor( )方法加密明文 plainText。

（4）将加密后的明文 BPlainText 转换成字符串。

2）编写解密算法。

（1）设置 64 ×3 位密钥长度 KEYSIZE,并自定义公共密钥值_PKEY 和初始向量_*IV*。

（2）将需要加密的明文 EplainText 转换成字节型数组 BElainText。

（3）实例化 3DESCryptoServiceProvider 类,并通过 CreateDecryptor( )方法解密密文 EplainText。

（4）将解密后的明文 PlainText 转换成字符串。

3）构造 20 个线程,同时往 1 000 张表里面依次插入加密后的数据,统计平均存储速率。

4）加密存储性能数据如表 5 所示。

表 5　加密性能实验数据

线程数	表数据量/万	平均存储速度/(条·s^{-1})
20	20	18 000
20	1 000	15 600

5）查询和解密性能数据如表 6 所示。

表 6　解密性能实验数据

查询数量	耗时/ms
10 000	1 363
5 000	730

4.5　结果分析

根据上面对 RSA 和 3DES-RSA 的加解密性能实验测试结果,下面从存储(速率、MDF 文件大小、LOG 文件大小)和查询两个方面作比较分析。

1）存储:

（1）速率。在硬件条件相同的情况下,同样往 1 000 张表里面插入数据,RSA 的平均存储速率约为 2 400 条/s,而 3DES-RSA 的平均存储速率为 16 000 条/s,由此可知,3DES-RSA 的存储速率是 RSA 的 8 ~10 倍,存储性能远远高于 RSA。

（2）MDF 数据库文件大小。1 000 张表,3DES-RSA 算法每张表插入 1 000 万数据,此时 MDF 文件大小为 681 GB。反观 RSA 算法,每张表在插入 200 万数据的情况下,MDF 数据库文件大小已经高达 2.5 TB。由此可推算,在 1 000 张表插入同样数据的情况下,在 MDF 数据库文件大小上 RSA 算法是 3DES-RSA 的 20 倍左右,而煤矿现场部署不可能提供如此海量的硬盘空间。

（3）LOG 日志文件大小。1 000 张表,对于 3DES-RSA 算法,每张表插入 1 000 万条数据的情况下,LOG 日志文件大小约为 600 MB。反观 RSA 算法,每张表插入 200 万数据的情况下,LOG 日志文件大小已经达到 600 MB。由此可推算,在 1 000 张表插入同样数据的情况下,LOG 文件大小 RSA 是 3DES-RSA 的 3 ~5 倍。

2）查询:由测试结果可知,对于 RSA 算法,每秒可查询数据量约为 240 条,而 3DES-RSA 算法,每秒可查询数据量约为 7 500 条,查询性能是 RSA 算法的 30 倍左右。

综上,从理论分析到实验测试(存储和查询性能),3DES-RSA 算法不管在性能还是安全上更能满足煤矿安全监控系统的现实需求,是一种合适的混合算法。

5　结　语

本文首先对 DES、3DES 和 RSA 三种加密算法从理论上进行分析比较,并结合煤矿安全监控系统数据的特殊性提出一种 3DES-RSA 的混合加密算法。通过实验数据分析证明,该混合算法充分发挥 3DES 和 RSA 的不同优点,加密效率和安全性能满足安全监控系统需求,是一种适合煤矿安全监控系统应用需求的混合算法。

参　考　文　献

[1] 仲丽云. 煤矿安全监控系统存在的问题及其改进探讨[J]. 工矿自动化,2010,36(6):92 -94.

[2] 宋泊东,张立臣,江其洲. 基于 Spark 的分布式大数据分析算法研究[J]. 计算机应用与软件,2019,36(1):39 -44.

[3] 国家安全生产监督管理总局. 煤矿安全监控系统通用技术要求:AQ 6201—2006[S]. 北京:煤矿工业出版社,2006.

[4] 国家煤矿安监局科技装备司关于征求《煤矿安全监控系统升级改造技术方案(征求意见稿)》意见的通知[EB/OL]. [2016 -11 -05]. https://www.mem.gov.cn/gk/gwgg/agwzlfl/tz_01/201701/t20170103_235131.shtml.

[5] 李彬,温蜜,齐钰. 智能电网 AMI 系统中一种新型密钥管理方案[J]. 计算机应用与软件,2016,33(1):321 -325.

(下转第 333 页)

-85.
[8] 蔡晶晶,宗汝,蔡辉. 基于空域平滑稀疏重构的 DOA 估计算法[J]. 电子与信息学报,2016,38(1):168-173.
[9] Mohimani H, Babaie-Zadeh M, Jutten C. A fast approach for overcomplete sparse decomposition based on smoothed L0 norm[J]. IEEE Transactions on Signal Processing,2009,57(1): 289-301.
[10] 赵瑞珍,林婉娟,李浩,等. 基于光滑 l_0 范数和修正牛顿法的压缩感知重建算法[J]. 计算机辅助设计与图形学学报, 2012,24(4):478-484.
[11] 孙娜,刘继文,肖东亮. 基于 BFGS 拟牛顿法的压缩感知 SL0 重构算法[J]. 电子与信息学报,2018,40(10):2408-2414.
[12] 伍飞云,周跃海,童峰. 基于似零范数和混合优化的压缩感知信号快速重构算法[J]. 自动化学报,2014,40(10): 2145-2150.
[13] 陈金立,李伟,朱筱嵘,等. 基于修正近似双曲正切函数的平滑 l_0 范数算法[J]. 计算机工程与设计,2018,39(12): 3717-3721,3754.
[14] Ma W K, Hsieh T H, Chi C Y. DOA estimation of quasi-Stationary signals with less sensors than sources and unknown spatial noise covariance: a Khatri-Rao subspace approach [J]. IEEE Transactions on Signal Processing,2010,58(4): 2168-2180.

(上接第 285 页)

[21] 陈湘川. 信息缺乏网络中的通信算法研究[D]. 合肥:中国科学技术大学,2000.
[22] 肖琳琳,陈杰,马冬妍,等. 中国工业企业两化融合现状实证研究[J]. 中国科技论坛,2016(9):71-77.
[23] 曾文献,张淑青,孟庆林,等. 基于改进 BP 神经网络的网络入侵检测研究[J]. 石家庄学院学报,2019,21(3): 23-30.
[24] 逯玉婧. 基于深度信念网络的入侵检测算法研究[D]. 石家庄:河北师范大学,2016.
[25] 王明. 基于卷积神经网络的网络入侵检测系统[D]. 北京:北京邮电大学,2018.
[26] 陈万志,李东哲. 结合白名单过滤和神经网络的工业控制网络入侵检测方法[J]. 计算机应用,2018,38(2):363-369.

(上接第 303 页)

[9] 秦靖辉. 安全电子商务 SET 协议的研究与改进[D]. 广州: 广东工业大学,2016.
[10] 韩炼冰. 椭圆曲线密码算法的 FPGA 设计与实现[D]. 成都: 电子科技大学,2018.
[11] Kavitha S, Alphonse P J A, Reddy Y V. An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system[J]. Journal of medical systems,2019,43(8):260.
[12] 卢闻捷. 改进椭圆曲线密码体制在 SET 协议中的应用[J]. 计算机系统应用,2018,27(4):34-38.
[13] 李尚泽. 椭圆曲线标量乘算法改进及应用[D]. 北京: 北京化工大学,2017.
[14] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS[J]. Telematics and Informatics, 2019, 38: 100-117.
[15] 吴旦. 椭圆曲线加密算法在卫星通信中的应用[J]. 数字通信世界,2018,165(9):160.
[16] Toughi S, Fathi M H, Sekhavat Y A. An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System[J]. Signal Processing,2017,141(12): 217-227.
[17] Beelen P, Datta M. Generalized hamming weights of affine cartesian codes[J]. Finite Fields and Their Applications, 2018,51(5):130-145.
[18] 王子青. 移动支付系统加密认证算法及安全协议的研究与实现[D]. 南京: 南京邮电大学,2016.
[19] 魏娟. SET 加密技术在 B2C 电子商务中的应用研究[J]. 赤峰学院学报(自然科学版),2017,33(5):109-110.
[20] Mehta E, Solanki A. Minimization of mean square error for improved euler elliptic curve secure hash cryptography for textual data[J]. Journal of Information and Optimization Sciences,2017,38(6):813-826.
[21] 魏南强. 基于 SET 协议的电子商务安全问题[J]. 山东工业技术,2017(4):137.

(上接第 315 页)

[15] Liu R, Chen P Y, Peng X, et al. X-Point PUF: Exploiting sneak paths for a strong physical unclonable function design [J]. IEEE Transactions on Circuits and Systems I: Regular Papers,2018,65(10):3459-3468.
[16] Liu W Q, Zhang L, Zhang Z R, et al. XOR-based low-cost reconfigurable PUFs for IoT security[J]. ACM Transactions on Embedded Computing Systems,2019,18(3):25.

(上接第 327 页)

[6] 李校南,王雪瑞,戴紫彬,等. 可重构分簇式分组密码处理架构[J]. 计算机应用与软件,2014,31(1):315-318,326.
[7] 陈侨川. 一种基于 DES 和 RSA 算法的混合加密算法[D]. 昆明:云南大学,2015.
[8] 陈运启,张翼. 煤矿瓦斯监控系统关键数据加密算法的研究与实现[J]. 工矿自动化,2012(7):7-10.
[9] 马汝超,赵亮. 煤矿安全监控系统数据加密技术[J]. 工矿自动化,2017,43(2):15-18.