

一种基于 DES, RSA 的随机加密算法

王印明, 李 阳

(兰州交通大学 电子与信息工程学院, 甘肃 兰州 730070)

摘 要:随着 Internet 的快速发展,对网络中信息传输的安全性要求越来越高。加密技术是网络安全技术的基石。目前典型的加密算法各有优缺点,如 DES 算法速度快,但安全性较低且密钥长度固定;RSA 算法安全性高,密钥长度不固定,但运算速度较慢。文中提出基于 DES, RSA 的随机加密算法,可根据选取规则来选择 DES 或 RSA 算法来加密信息,然后将算法标记、密钥长度、密钥及密文信息组织成新的信息进行传输。这样既能快速地对数据进行加解密,又能很好地解决密钥分配问题,在保证安全性的前提下,也提高了算法效率。

关键词:数据加密;加密算法;DES 算法;RSA 算法;随机加密算法

中图分类号:TP311

文献标识码:A

文章编号:1673-629X(2012)04-0235-03

A Random Encryption Algorithm Based on DES, RSA Algorithm

WANG Yin-ming, LI Yang

(School of Electronics and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China)

Abstract: With the rapid development of Internet, the security of information transformation in the network has become more and more important. Encryption technology is the cornerstone of network security technology. At present, the typical encryption algorithms have advantages and disadvantages, such as, DES algorithm is fast, but its security is low and the length of key is fixed. RSA algorithm is safer, and its length of key is not fixed, but it is slower. In this paper, the random encryption algorithm based on DES, RSA algorithm chooses DES or RSA algorithm to encrypt information according to the selection rules, and then organizes the flag of algorithm, the length of key, key and the ciphertext information into the new information to transmit. This can not only encrypt and decrypt the data rapidly, but also be a good solution to key distribution problem, and improve the efficiency of the algorithm under the promise of security.

Key words: data encryption; encryption algorithm; DES algorithm; RSA algorithm; random encryption algorithm

0 引 言

在当今信息化的时代里,数据是信息的载体,信息的交流依赖于数据的传输,并且随着 Internet 的广泛应用,网络中信息传输的安全性越来越受到人们的重视。数据加密、数字签名、身份验证等技术应运而生,特别是数据加密技术给网络中数据传输安全带来了希望。加密算法为数据的加密传输提供了很好的解决方法^[1,2]。

安全性和运算效率是衡量一种加密算法好坏的重要指标,并且在不同的应用场合,对两者的具体要求也是有差异的,例如对实时性要求较高的场合,运算效率就比较重要;而对于重要的机密信息而言,安全性就显得极为重要。

1 常用的加密算法

数据加密是对可读的信息(即明文)经过某一种(或某几种)加密算法处理后使其成为一段不可读的信息(即密文),而且只有在经过对应的密钥处理后才能得出原来的信息(即明文)^[3]。将密文转换成明文的过程称作解密。加密算法是对数据进行加密处理的核心,故其性能的好坏直接影响对数据加密的安全性和效率性。

基于密钥的加密算法常分为两类:对称加密算法和非对称加密算法(即公开密钥加密算法)^[4,5]。

1.1 DES 加密算法

DES(Data Encryption Standard, 数据加密标准)是一种对称加密算法,既可用于加密也可用于解密。该算法加密时将明文分为固定长度的块,用同一密钥对每一块进行加密,输出的密文也是固定长度的^[4]。加密过程是使用 64 位密钥(包括 56 位的密钥以及附加的 8 位奇偶校验位)来对 64 位明文输入块进行加密的方法,通过对 64 位的明文数据块进行 16 轮迭代运算后,得到 64 位密文输出块^[6]。并且密钥是任意的 56

收稿日期:2011-08-30;修回日期:2011-12-02

基金项目:兰州市科技计划项目(2010-1-6)

作者简介:王印明(1987-),男,山东滕州人,硕士研究生,研究方向为信息服务集成、软件工程。

位数,并可随意改变。

DES 算法加密速度快、效率高,已被广泛应用于数据加密,但是当使用的人数比较多时,密钥比较容易泄露,并且因其密钥长度为 56 位,目前在特定领域已不能提供很好的安全性。

1.2 RSA 加密算法

RSA 加密算法既能用于加解密,也可用于数字签名,基于大数分解的难度决定了其可靠性。公钥和私钥是 2 个大素数的函数。由一个密钥和密文破解出明文的难度相当于分解两个大素数的积^[7]。且解密是加密的逆转换,正是由于这种逆转换,才使其具有了数字签名的功能。

RSA 加密算法的过程:给定明文 $M < n$,随机选择两个不同的大素数 p 和 q ,计算 $n = p * q$,计算 $m = (p - 1) * (q - 1)$,然后随机选择一个整数 $e (0 < e < m)$,要求满足 e 与 m 互为质数。最后计算私钥 d ,要求满足 $d = e^{-1} \bmod m$ (保密)。确定:公钥 $K_{pub} = \{e, n\}$,私钥 $K_{pri} = \{d, n\}$,密文 $C = M^e \bmod n$ ^[8,9]。由此可见,RSA 加密算法的安全性高,但是计算时间长、加密速度慢。

2 基于 DES, RSA 的随机加密算法

2.1 算法思想

该算法不再是始终运用同一种加密算法对数据加密,而是根据一定的随机选取规则来确定某种算法对数据进行加密^[10,11],加密后将算法标记、密钥信息及密文信息按照一定的组织方式合成新的密文信息进行传输。

解密时将密文信息根据事先的信息组织方式来分解出算法标记、密钥信息及原始密文信息,然后根据算法标记和所用的随机选取规则来确定出该密文信息所用的加密算法,最后运用密钥信息将原始密文信息解密,得到明文信息。算法流程图如图 1 所示。

2.2 算法实现

加密时,明文信息按照特定的随机加密规则来选择加密算法^[12],若为 DES 算法,首先设置算法标记 f ,然后根据 DES 算法原理生成密钥 k ,运用此密钥对数据加密,得到密文 $d1$,最后将算法标记 f 、密钥 k 、密文 $d1$ 按照一定的组织方式合成为新的密文 $d2 = \{f, k, d1\}$, DES 密钥长度都为 64 位,因此无需保存密钥长度;若为 RSA 算法,首先设置算法标记位,然后随机生成密钥长度 l (512 ~ 1024, 并且为 8 的倍数),根据密钥长度 l 生成密钥对(公钥 $k1$, 私钥 $k2$),运用公钥 $k1$ 对数据加密,得到密文 $d1$,最后将算法标记 f 、密钥长度 l 、私钥 $k2$ 、密

文 $d1$ 按照一定的组织方式合成为新的密文 $d2 = \{f, l, k2, d1\}$ 。程序流程图如图 2 所示。

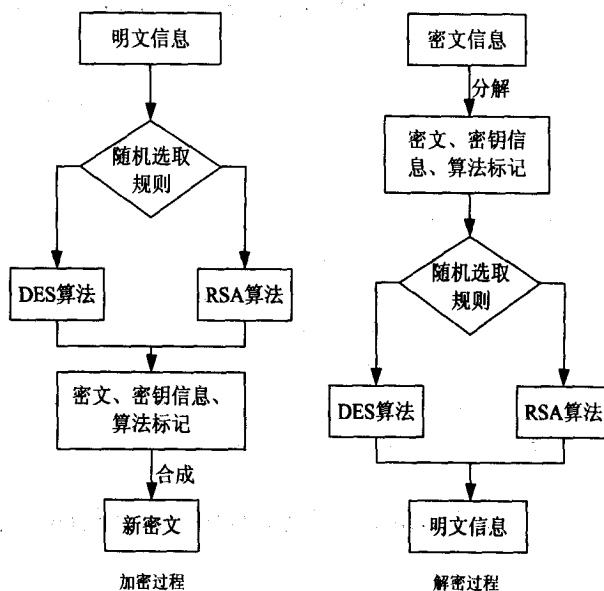


图1 算法流程图

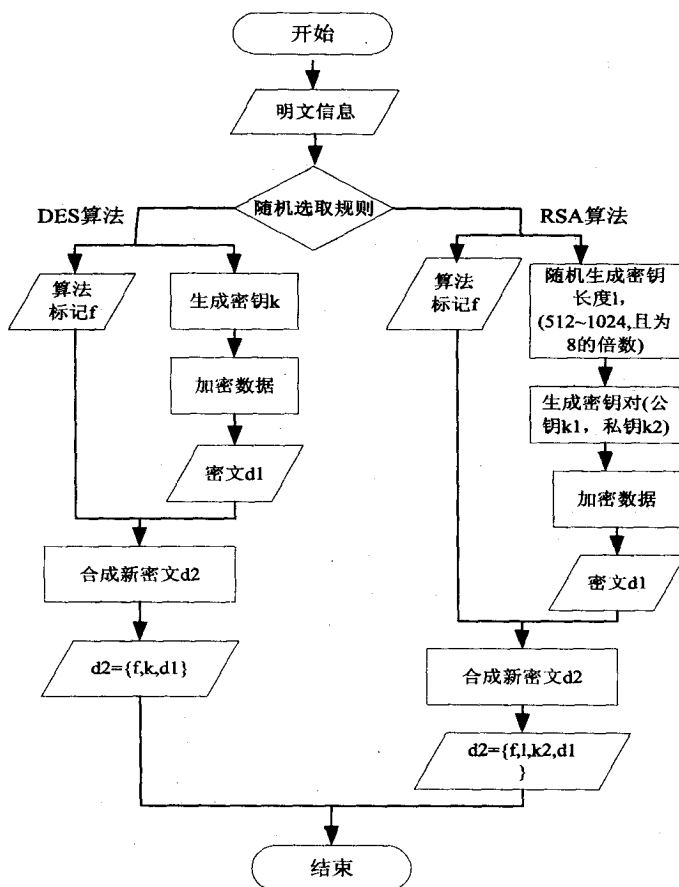


图2 加密程序流程图

解密时,把密文信息按照加密时的组织方式分解出算法标记 f 、密钥信息和原始密文信息 $d1$,然后根据随机选取规则确定加密算法,若为 DES 算法,通过分解出的密钥 k 和原始密文信息 $d1$ 就可以解密为明文信息;若为 RSA 算法,需通过分解出的密钥长度 l 得到

私钥 k , 然后将原始密文信息 $d1$ 解密为明文信息。程序流程图如图 3 所示:



图3 解密程序流程图

本算法中, 随机选取规则为等概率选取的方式, 即选取 DES 和 RSA 算法的概率相同。具体实现方式为根据产生的随机数, 奇数时选取 DES 算法, 偶数时选取 RSA 算法; 密文的组织方式如图 4 所示:

| | | | |
|--------|-------------|--------------|-------|
| 算法标记 F | 密钥长度 l (可无) | 密钥 K (或私钥 k) | 密文 d1 |
|--------|-------------|--------------|-------|

图4 密文组织方式



图5 程序运行结果

算法以 Java 语言实现, 假设需加密的数据为字符串“基于 DES, RSA 的随机加密算法”, 程序运行结果如图 5 所示。

2.3 性能测试

测试本算法的速度和安全性, 测试环境为 PC 机, CPU: Intel (R) Pentium (R) Dual E2200, 内存: 1GB, JDK 版本: 1.6.0_22。测试加密数据为字符串“加密算法”, 运行次数: 1000, 测试结果如表 1 所示:

表1 测试结果

| 性能 | 运行次数 | 加密时间 (ms) | 解密时间 (ms) | 平均时间 (ms) | 安全性 |
|--------|------|-----------|-----------|-----------|-----|
| DES 算法 | 1000 | 3756 | 254 | 2005 | 低 |
| RSA 算法 | 1000 | 161723 | 20627 | 91175 | 高 |
| 随机加密算法 | 1000 | 88128 | 14992 | 51560 | 高 |

由表 1 数据可以看出, 本算法的安全性比 DES 算法高, 同时运算速度与 RSA 算法相比有了很大提高。

3 结束语

数据加密是保证信息安全的重要手段, 选择合适的加密算法可以使数据的安全性和实时性得到很大的提高^[12]。文中在 DES, RSA 算法的基础上提出了一种随机加密算法, 可根据不同的随机选取规则选择不同的加密算法, 在安全性和加密速度方面有良好的表现, 且具有很好的扩展性, 可根据需要将不同的加密算法集成进来。笔者在这方面只是做了一点探索, 对于算法可能存在的缺陷和如何将算法更实用化还需做进一步的研究工作。

参考文献:

- [1] 孙国梓, 林清秀, 陈丹伟. 密钥加密实验平台的研究与实现[J]. 计算机技术与发展, 2009, 19(8): 144-147.
- [2] 陈雪兆, 杨杰. 计算机网络的加密算法研究[J]. 教育技术导刊, 2009(9): 68-70.
- [3] Ashrafi M Z, Ng S K. Privacy-preserving e-payments using one-time payment details[J]. Computer Standards & Interface, 2009, 31(2): 321-328.
- [4] 段钢. 加密与解密[M]. 北京: 电子工业出版社, 2004.
- [5] 李迈勇. 网络安全: 加密原理、算法与协议[M]. 北京: 清华大学出版社, 2007.
- [6] 李海泉, 李健. 计算机网络安全与加密技术[M]. 北京: 科学出版社, 2001.
- [7] 王茜, 倪建伟. 一种基于 RSA 的加密算法[J]. 重庆大学学报, 2005, 28(1): 68-72.
- [8] 陈兴波, 王晓明. 一种快速 RSA 算法的改进[J]. 计算机工程与设计, 2006, 27(22):

(下转第 241 页)

格式分区的操作系统中,进行文件的操作,结果表明系统可以在 FAT 分区和 NTFS 分区很好的工作,对所有 txt 类型文件都进行了加密存储,写入的明文如图 3 所示。

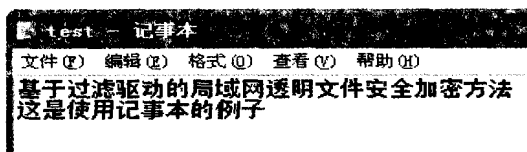


图3 文件保存的明文

当在另外一台没有加密方法的电脑上看这些文件都是乱码,看不到真实信息,如图 4 所示:

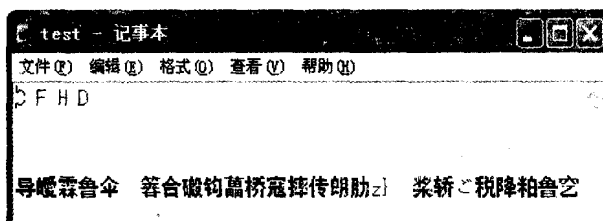


图4 文件实际存储的密文

并且还对加密过程使用 DebugView 进行了检测,通过使用 DebugView 的检测可以对内核态程序的运行过程有一个大致的了解,如图 5 所示:

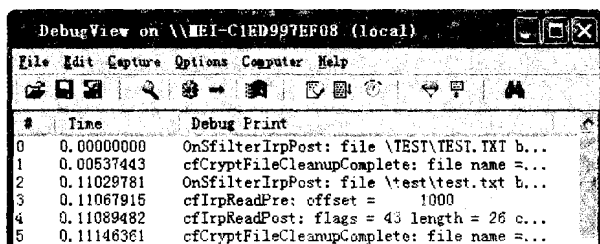


图5 文件加密过程

实验结果表明基于过滤驱动的文件加密方法可以在不改变用户的使用习惯的情况下很好地提供加密与解密操作。

4 结束语

利用文件系统过滤驱动技术进行文件透明加密和解密是一种在 Windows 内核里实现的底层开发技术,

开发实施起来相对较繁琐,但是它可以在不改变用户的习惯的情况下有效保护局域网内各种电子文件信息安全,在安全性方面也有了很大改善,具有较高的商业价值和较好的社会效益。

文中实现的局域网文件加密技术对局域网内部的信息安全有一定的保障,但是还有许多需要完善的地方。

参考文献:

- [1] Sun Qindong, Guan Xiaohong, Zhou Yadong. A Survey of Network Information Content Audit[J]. Journal of Computer Research and Development, 2009, 46(8): 1241-1250.
- [2] Zhao Mingwei, Mao Rui, Jiang Rongan. Transparent Encryption File System Model Based on Filter Driver[J]. Computer Engineering, 2009, 35(1): 150-152.
- [3] Shen Wei, Wang Lei, Chen Jiajie. Design and Implementation of Encryption System Based on File System Filtering Drive[J]. Computer Engineering, 2009, 35(20): 157-159.
- [4] Liu Haiyan, Yang Zhaohong, Huo Jinghe. On the Detection and Analysis Techniques of the Intranet Security[J]. Computer Engineering & Science, 2009, 31(9): 11-12.
- [5] 胡宏银,姚峰,何成万.一种基于文件过滤驱动的 Windows 文件安全保护方案[J]. 计算机应用, 2009, 29(1): 168-171.
- [6] 王全民,周清,刘宇明,等.文件透明加密技术研究[J]. 计算机技术与发展, 2010, 20(3): 147-150.
- [7] 吴慧玲,贺广生.一种基于系统驱动的文件透明加密系统的实现[J]. 计算机与现代化, 2010, 5(4): 156-158.
- [8] 顾正义,黄皓.新加密文件系统的研究与实现[J]. 计算机工程与设计, 2009, 30(4): 3271-3277.
- [9] 赵晓峰,叶振.几种数据库加密方法的研究与比较[J]. 计算机技术与发展, 2007, 17(2): 219-223.
- [10] 徐翔.文件保护系统中透明加解密技术的设计与实现[D]. 北京:北京化工大学, 2009.
- [11] 李民.基于 Windows 文件系统过滤驱动的文件加/解密技术研究与实现[D]. 成都:四川大学, 2006.
- [12] 谭文,杨潇,邵坚磊.寒江独钓-Windows 内核安全编程[M]. 北京:电子工业出版社, 2009.

(上接第 237 页)

4243-4248.

- [9] Castagnos G. An efficient probabilistic public-key cryptosystem over quadratic fields quotients[J]. Finite Fields and Their Applications, 2007, 13(3): 563-576.
- [10] 汪祥莉,李腊元,王文波.一种基于网络安全的复合加密算法的研究[J]. 武汉理工大学学报, 2008, 32(5): 845-848.

- [11] Bao Feng, Lee Chengchi, Hwang Min-Shiang. Cryptanalysis and improvement on batch verifying multiple RSA digital signature[J]. Applied Mathematics and Computation, 2006, 172(2): 1195-1200.
- [12] 佟晓筠,姜伟.基于混合加密技术的电子商务安全体系研究[J]. 微处理机, 2006, 4(2): 45-47.