

基于扰乱器对 DES 加密算法安全性提高的论证

王建华¹, 李 金²

(江苏科技大学 电子信息学院, 江苏 镇江 212003)

摘 要: DES 是一种应用非常广泛和成熟的数据加密算法。在深入剖析 DES 加密算法原理基础上, 提出了一种改进的 DES 加密方案, 该方案通过对 64 位密钥变换后的结果进行扰乱, 使得设计后的加密体系安全性更高; 同时对扰乱器的原理进行了数学验证, 证明了改进方案的可靠性; 而软件设计结果, 进一步论证了改进方案的可行性。

关键词: 加密算法; DES; 扰乱器; 3DES

中图分类号: IP301.6

文献标识码: A

文章编号: 1000-7180(2012)10-0198-04

Scrambler Based on the DES Encryption Algorithm to Improve the Security Argument

WANG Jian-hua¹, LI Jin²

(Institute of Electronic information, Jiangsu University of Science and Technology, Zhenjiang 212003, China)

Abstract: DES is a widely used and mature data encryption algorithm. This paper analysis the principle of DES algorithm and its advantages and disadvantages and propose a DES improvement program, which the 64-bit key transformation by the results after the disruption, making the system more secure. Also on the design principle of Scrambler having mathematical proof, and gives the results of software design, and further proof s its feasibility.

Key words: Encryption algorithm; DES; Scrambler; 3DES

1 引言

随着信息技术迅猛发展^[1], 采用密码技术对信息加密是最常用和最有效的安全保护手段^[2-4]。

本文在分析 DES 加密算法的基础上, 提出了一种在密钥处理过程中加入扰乱器的改进 DES 加密方案。重点介绍了扰乱器的特点, 以及其实现的原理并进行了数学理论以及实际传输过程中加解密输入输出的验证, 同时分析了其比传统 DES 加密算法安全性更高的原因, 进一步得出置信的研究结论。

2 DES 算法介绍

2.1 DES 算法的原理

当前广泛使用的密码体制有公钥密码和对称密码两类^[5-7]。公钥密码不需要对密钥进行秘密分配, 可实现密钥交换、数字签名和认证等, 但是其运算复

杂, 需要传送大量数据; 而对称密码加密速度快, 适合加密大块数据^[8]。比较典型对称加密算法是 DES 算法^[1,8]。

在 DES 算法中, 首先把数据报文分成报文段, 每个报文段包含 64 位, 不足补零, 64 位的明文经过初始置换, 被分成左、右两半部分 L_0 和 R_0 , 各 32 位长; 然后左右部分均进行 16 轮完全相同的运算, 在运算过程中, 数据与密钥相结合, 16 轮运算完毕后, 左右部分合在一起经过一个末置换(初始置换的逆置换), 就完成了整个加密过程^[1]。

尽管引入 DES 算法之后涌现了一大批对称加密算法, 尽管它注定被高级加密标准 AES 所取代, 但是 DES 依然是一个极其重要的算法。

DES 加密算法包括 5 个函数: 初始置换(IP); 复杂函数 f_k , 它包含置换和代换两个部分, 而且它依赖于输入的密钥; 用以转换数据两个部分的简单

置换函数(SW);再一次运用函数 f_k ;最后的一个置换函数是 IP 的逆,记为 IP^{-1} 。

f_k 的输入不仅包括通过加密算法的数据,而且包括一个 8 位的密钥。算法可以设计成 16 位密钥的工作模型,包括两个 8 位的子密钥,分别用在 f_k 的两次出现中。另一种方法是将 8 位密钥在算法中使用两次。如图 1 所示为 DES 加密过程流程图。

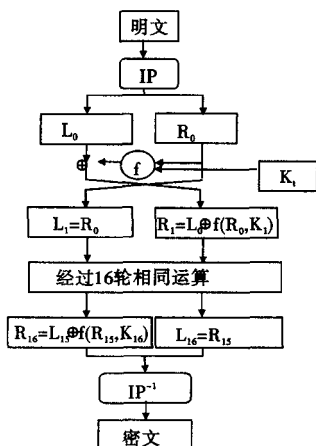


图 1 DES 加密过程流程图

不管是 DES 加密方案,还是任意改进的 DES 加密方案,总有明文和密钥两个输入。DES 算法的明文长度为 64 位,密钥长度为 56 位。从图 1 可见,明文的处理经过了三个阶段。首先,64 位的明文经过初始置换(IP)而被重新排列。然后进行 16 轮的相同函数的作用,每轮的作用中都有置换和代换。最后一轮迭代的输出有 64 位,它是输入明文和密钥的函数。将其左半部分和右半部分互换产生预输出。最后,预输出再被与初始置换(IP)互逆的逆初始置换(IP^{-1})作用产生 64 位的密文。

DES 密钥太短以及各次迭代密钥具有相关性等缺点使得后续学者研究了大量的 DES 变种和改进算法,如 3DES,以及结合硬件电路实施的改进 DES 加密算法方案等。

DES 加密算法密钥中用到了 64 位中的 56 位,具有较高的安全性。但是密钥仅有 56 位太短,各次迭代中使用的密钥 $K(i)$ 是递推产生,这种相关性必然降低了密码体制的安全性。在现有的技术条件下用穷举搜索法进行攻击来获取正确密钥已趋于可行;其次,DES 算法实现替代函数 Si 所用的 S 盒的设计原理未公开,其中可能有隐患,它是 DES 算法的核心,易被差分密码攻击^[1]。

2.2 DES 算法存在的问题

虽然,DES 算法自出现以来一直作为非常安全

的加密算法被广泛用于各种数据的保护,DES 加密算法的密钥用到了 64 位中的 56 位,具有较高的安全性。但是,学术界对它进行了深入的研究后,发现了它的诸多缺点,主要集中在^[2]。

(1) DES 的加密单元仅有 64 位太小,而且 64 位被分为 8 组后,每个分组只有 8 个字符,去掉其中用于奇偶校验位的第 8 位,实际参与加密过程的也就只有 7 位。

(2) 密钥仅为 56 位太短,而且发收信双方都共同使用 1 个密钥对数据进行加解密,计算量小;而且每一次迭代产生的密钥都与上一次迭代相关,这种特性导致了密码系统的安全性降低。由于 DES 算法的公开性,在现有的技术条件下用穷举搜索法来对密文进行攻击以获取正确密钥已趋于可行^[3,4,9]。

(3) DES 算法实现替代函数 Si 所用的 S 盒的设计是 DES 算法的核心,其设计原理的未公开性,其中可能有隐患,易被差分密码攻击。

为了克服以上的各种缺点,后续学者应用了存在多种算法的改进方法,如:

(1) 具有独立不相关的子密钥的 DES 算法

每一轮迭代使用的密钥不是由一个 56 位二进制密钥产生,而是 16 个不同的子密钥,这种算法看似安全性更高,但是密码界权威已经证明,DES 的变形可被 261 个选择明文破解^[8]。

(2) 带有交换 S 盒的 DES 算法

改变盒的次序虽然能够降低抵御差分密码分析的能力,但同时也降低了算法的安全性,不仅对选择明文的攻击也提升不了,而且使差分密码法更容易攻击该算法^[1]。

(3) 三重 DES 算法

用三个不同且不相关的密钥对数据进行三重加密,即为

$$C = Ek_3(Dk_2(Ek_1P)),$$

$$P = Dk_1(Ek_2(Dk_3C)).$$

这种方法虽然提高了数据的安全程度,可以有效地抵抗来穷举搜索法的攻击^[10],但却增加了传统 DES 计算时间的 $n-1$ 倍,降低了其运行效率。

3 改进的 DES 数据加密算法

以往密码学家的种种 DES 算法的改进方案都存在不同的问题。针对用户对数据安全性更高地要求,提出了一种 DES 的改进方案。在改进的 DES 数据加密算法中,主要在 16 轮迭代过程中加入了扰乱器,扰乱后的密钥序列不可用穷举攻击的方法破解,

虽然 16 轮密钥是由 56 位密钥递推产生的,但每个 48 位的子密钥在加入迭代前进行了物理意义上的干扰,则就不可利用其以往地规律性去推导出密钥,那么必然提高了数据传输中的安全性.主程序流程图.见图 3.

3.1 改进的 DES 加密算法流程示意图

改进的 DES 加密算法流程如图 2 所示.



图 2 加(解)密模块流程图

传统的 DES 加密算法中,当生成 16 个 48 位子密钥后,密钥直接进行 16 轮迭代变换,而改进的 DES 加密算法则主要在生成的 16 个 48 位子密钥后引入了物理电路扰乱器,使得密钥的规律性更加隐秘,从而提高了数据的安全性.主程序流程图见图 3.

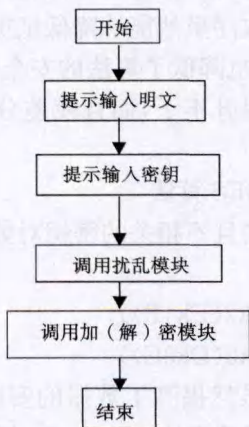


图 3 主程序流程图

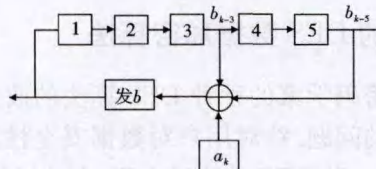


图 4 扰乱示意图

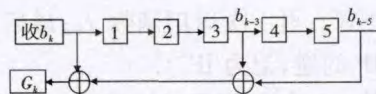


图 5 扰乱恢复示意图

3.2 扰乱器设计

扰乱与扰乱恢复分别如图 4 和图 5 所示.在图 4 和图 5 中,方框中的 1、2、3、4、5 分别为移位寄存器,圆形中的加号表示异或运算符,每一个都表示分别左移一位,当 48 位子密钥进入扰乱器后则重新生成 48 位的子密钥 b_k ,再进行 16 轮加密变换得出密文,而 DES 的特点是对称加密体制,扰乱器符合了这一特点.解密过程是加密过程的反过程,直接应用扰乱恢复即可恢复最初的 48 位的子密钥.

3.3 扰乱实现的数学证明

结合图 4 和图 5,可以列出下面两个算数表达式:

$$b_k = a_k \wedge b_{k-3} \wedge b_{k-5} \quad (1)$$

$$c_k = b_k \wedge b_{k-3} \wedge b_{k-5} \quad (2)$$

由式(1)和(2)联立求解得

$$c_k = a_k \wedge b_{k-3} \wedge b_{k-5} \wedge b_{k-3} \wedge b_{k-5} \quad (3)$$

结合异或运算法则 $b_{k-3} \wedge b_{k-5} = b_{k-5} \wedge b_{k-3}$,式(3)等价于

$$c_k = a_k \wedge b_{k-3} \wedge b_{k-5} \wedge b_{k-3} \wedge b_{k-5} = a_k \wedge b_{k-3} \wedge b_{k-5} \wedge b_{k-5} \wedge b_{k-3} = a_k \quad (4)$$

由此可见,扰乱器是对称性的器件,具有可逆性.

4 改进的 DES 算法性能验证和分析

对比 DES 和改进后的 DES 加密算法性能测试结果如图 6 所示.

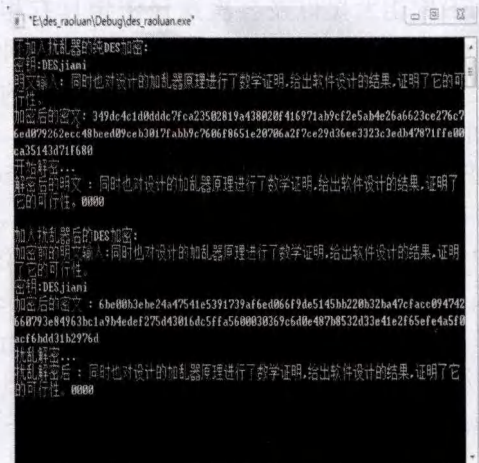


图 6 DES 与 DES 改进算法测试结果

对比 DES 加密与加入扰乱后的 DES 加密可以

看出:

(1) 在加密相同的明文情况下,加入扰乱后的DES加密后的密文与传统的DES加密后的密文明显不同.则说明了引入扰乱后密文不具有明显的DES加密后的规律性;

(2) 扰乱解密后仍然恢复了准确的发方消息,则扰乱后的DES加密算法具有正确性和可靠性;

(3) 若有非法用户篡改信息,则必然解密后不可能得到加密相同的消息,又根据扰乱器和DES加密算法的对称性,则说明了改进后的DES加密算法具有有效性;

(4) 在加密时,由于子密钥顺序被扰乱器扰乱进而发生变化,攻击的难度和复杂度也就相应上升了,则必然增加穷举攻击法破解的难度.

综上所述,软件运行结果证明了改进的DES算法的正确性和可靠性.但是由于DES加密算法公开,攻击者可以利用穷举搜索法对密钥进行攻击,从而使得DES加密的安全性能难以保证;而加入电路结构组成的扰乱器后,在改进的DES加密算法中,攻击者即使找到了正确的密钥,由于并不知道扰乱器的具体电路结构,从而攻击者很难正确解密,加密的安全性能就得到了明显提高.

5 结束语

本文引入的扰乱器结构并不复杂,而且扰乱和恢复扰乱器的特点本身也符合了解密对称机制,这一特点使得软件实现上更加的方便,同时扰乱后的DES加密算法弥补了传统的DES加密算法的不足,使其安全性得到进一步的提高,可用于重要数据和信息传输等方面,应用范围也极广.

参考文献:

- [1] 杨宏志. 对称密码算法簇设计及其仿真[D]. 郑州:解放军信息工程大学,2010.
- [2] 邹应双,陈风,陈铮. 一种基于DES的加密方法[P]. 中国专利:CN101707521A. 2009-12-1.
- [3] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol [M]. Peking: Tsinghua University Press, 2007.
- [4] Xu Chen, Wenpin Guo, Design of secure instant Messaging system based on RSA and TDES[J]. Microcomputer Applications, 2009, 25(9), 39-40.
- [5] Dong Xiaolei, Qian Haifeng, Cao, Zhenfu. Provably secure RSA-type signature based on coniccurve[J]. Wireless Communications and Mobile Computing, 2009(2): 217-225.
- [6] Tang Shaohua. Simple secret sharing and threshold RSA signature schemes [J]. Journal of Information and Computational Science, 2004(1): 259-262.
- [7] Xu Qiu-Liang, Chen Tzer-Shyong. An efficient threshold RSA digital signature scheme[J]. Applied Mathematics and Computation, 2005(6): 25-34.
- [8] 张春晖. DES算法原理及改进[J]. 电脑知识与技术, 2009(22): 1-10.
- [9] 盛苏英,吴新华. 一种新的图像加密算法研究与应用[J]. 微电子学与计算机, 2011, 28(2): 124-128.
- [10] 郭华,丁国良,刘昌杰,等. DES加密算法的差分电磁攻击实现[J]. 微电子学与计算机, 2009, 26(12): 35-37.

作者简介:

王建华 男,(1956—),副教授,硕士研究生导师.研究方向为雷达信号处理和智能控制.

李金女,(1985—),硕士研究生.研究方向为多层次密钥管理系统下的DES加密.