基于一次密钥的数据加密算法优化①

房祥超, 李兴保

(曲阜师范大学 信息技术与传播学院, 日照 276800)

摘 要: 介绍了关于DES算法的一些研究情况, 分析了DES了算法的加密原理以及实现过程, 通过内容分析, 简单介绍了 DES 算法的几种改进方案, 通过分析它的加密过程以及几种改进方案, 进而提出了自己的一个改进思想即一次密钥的加密方案, 通过这个方案为 DES 算法的优化作一个参考.

关键词: DES 算法; 一次密钥; 加密原理; 算法优化

Optimization of Data Encryption Based on a Key

FANG Xiang-Chao, LI Xing-Bao

(School of Information Technology and Communication, Qufu Normal University, Rizhao 276800, China)

Abstract: This paper introduces some research about DES algorithm, analyzes the encryption principle of DES algorithm and implementation process, through content analysis, introduces the improvement of DES algorithm, improved scheme through the analysis of the encryption process it and several, puts forward an improved thought his is a key encryption scheme, a reference through this scheme optimization for DES algorithm.

Key words: DES algorithm; key; encryption principle; algorithm to optimize

1 引言

随着计算机技术的发展, 计算机网络也得到了长足的发展, 比如电子商务, 网络产品经营管理等, 同时, 由于计算机网络在传输中缺乏足够的安全性, 网络上的信息在传输过程中随时都受到被窃听, 篡改等的威胁, 为了保证网络数据传输的安全性, DES 数据加密算法应运而生.

DES 算法为密码体制中的对称密码体制, 又被成为美国数据加密标准, 是1972年美国IBM公司研制的对称密码体制加密算法. 作为数据加密标准形式的DES 数据加密算法虽然有许多年的历史,但是仍在数据加密领域占据着重要地位,并且被各个领域广泛采用,包括ATM柜员机,收费站以及银行身份验证等领域. 加密过程如图 1 所示.

DES是一个分组加密算法, 它以64位为分组对数据进行加密, 同时它也是一种对称数据加密算法: 加密和解密使用同一个密钥. 它的密钥长度为64位, 其中56位为有效数据位, 另外8位为奇偶校验位. 虽然其中有几个弱密钥, 但是由于数量少, 所以很容易避开它们.

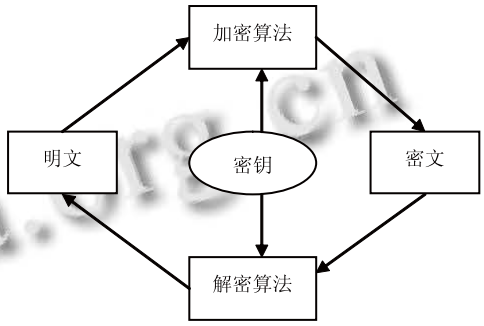

图 1 数据加密过程

2 DES算法的加密过程

DES 算法把 64 位的明文输入块变为 64 位的密文输出块, 它所使用的密钥也是64位, 由于是64位分组加密,所以首先要对数据进行分组,分组完成后就需要用函数进行加密操作, 其中最核心的加密函数是 F 函数, 分组后的数据经过 F 函数的迭代操作形成密文数据, 操作过程如图 2 所示.

① 收稿时间:2013-02-06;收到修改稿时间:2013-03-06

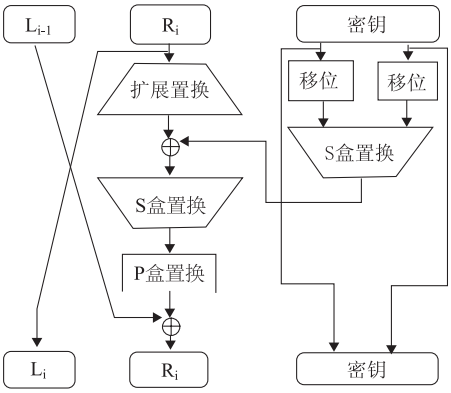

图 2 DES 加密核心过程(F 函数)[2]

其中扩展置换即是把分组后的 32 位通过一种规则扩展为 48 位, 同样的, S 盒置换以及 P 盒置换也是根据一定的 S 盒以及 P 盒数据位置换表进行置换, 由于 F 函数中涉及的各种置换表已经比较通用, 本文就不一一列举置换表了.

此 F 函数需要经过 16 迭代操作, 完成后进行最终置换, 形成密文数据.

DES 加密过程密钥是其中加密的关键, 算法的安全性依赖于密钥, 而实际的加密过程中并不是直接使用密钥, 而是通过 16 次迭代运行形成 16 个 48 位子密钥, 下面将介绍子密钥的生成过程.

3 DES算法的缺陷

多年来,DES 算法一直作为数据加密标准被应用于许多行业各种数据的保护, 但随着计算机性能的提升, 它的缺陷也日益显露出来.

(1) DES 算法的密钥长度过短, 只有 56 位数据有效位, 现在计算机的运行速度已经可以使用穷举攻击来破译密码, 并且花费的时间并不是很多, 例如, 1997 年 1 月 28 日, 美国的 RSA 数据安全公司悬赏 1000 美金破译 DES 的 56 位密钥, 其目的是调查 internet 上的分布式计算能力, 并测试密钥长度为 56 位的 DES 算法的相对强度, 美国程序员 Vesor 在 internet 上万名自愿者的帮助下花费 96 天成功破译了 DES 密钥, Vesor 说:“对于一个坚定的攻击者来说, 56 位密钥已经不再安全了,”后来随着计算机速度的提升, 仅用几个小时就可以破译, 所以用 DES 来保护很长时间的数据已经是不可行的.

(2) DES 加密算法不能很好的抵抗选择明文攻击, 选择明文攻击是一种破译密码的方式, 通过选择一定的明文通过 DES 加密算法进行加密, 用以观察密文的以及和目标密文进行对比, 从而找到加密的规律, 最坏的情况下, 攻击者可以直接得到密钥,选择明文攻击的一个特点是根据明文与得出的密文之间的联系来进行判断, 当然为了安全加密方可以每次更换密钥, 这样虽然可以相当程度上避免选择明文攻击, 但是会造成密钥管理上的压力, 而且密钥更换过于频繁而且会造成安全隐患.

(3) DES 算法加密过程中并没有加入随机密钥, 所用到的密钥都是通过初始密钥生成, 这样容易受到线性攻击.

4 改进措施

由于 DES 固有的短密钥缺陷以及密钥传输的安全性等问题, 导致这个经典的数据加密算法的相对没落, 笔者通过观察和分析 DES 的加密过程, 以及浏览各加密方案得知很难有一种加密方法能够达到所谓的绝对安全, 任何长度的密钥随着计算机的发展也会被暴力破译, 任何类型的密钥传输都可能被获取破解, 另外笔者发现自从密码学诞生以来, 最安全的加密算法就是每次更换密钥的算法, 密钥只使用一次,而且这样就从来不会被破译, 基于这些缺点, 笔者提出一种基于一次密钥的 DES 算法改进方案, 下面详细介绍一下该方案.

分析 DES 加密算法的加密过程得知: DES 算法需要先把明文进行分组, 分组后的明文以 64 位数据为一组, 然后对 64 位进行异或操作,之后再把 64 位数据进行左右分组, 分组后右部分 32 位数据进行扩展以及与密钥合成 48 位子密钥, 然后进行 Sbox 置换和 P 盒置换, 然后再和原来的左边 32 交换, 变成新的左边 32 位, 在算法实现的直观过程中, 左边的 32 位数据并没有在实现过程参与什么操作, 纵观整个加密过程都没有涉及到随机数据的问题, 这给算法造成很大的安全隐患, 所以笔者设计通过随机函数, 每次生成 64 位随机子密钥, 全部通过随机函数生成, 64 位子密钥进行 s 盒压缩置换, 压缩成 32 位数据,然后与左边的 32 位数据进行异或操作, 这样就加入了随机函数在过程里面, 之后再按照 DES 加密过程进行下一步的操作, 这样每次迭代都会经过这个过程, 也就是说要经过 16 次的随机密钥生成算法, 每次的密钥长度为 64 位, 也就是 DES 算

法密钥的长度增加了 16*64 位即 1024 位, 这样算法的总密钥长度为 1088 位, 而且每次加密一个数据后, 这种密钥就会作废, 下次运行加密程序将会得到另一组加密数据, 这样就形成了一次密钥的算法, 密钥只使用一次, 大大增加了数据的安全性. 下图为该改进算法的核心部分.

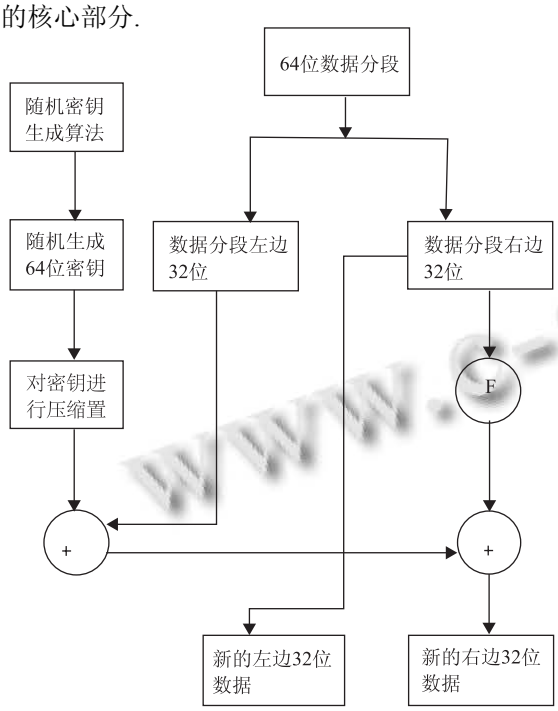

图 3　基于一次密钥的 DES 算法改进核心部分

5　改进后的优点

(1) 首先, 在每次的迭代过程中加入 64 位的随机密钥, 增加了总密钥的长度,基本上避免了暴力破解的可能性, 因为优化后的总密码长度是 1088 位, 也就是包含 21088 密钥空间, 已经超过了 RSA 的密钥长度, 暴力破解的方法已经基本不可能破译它.

(2) 其次, 因为里面加入了随机函数, 每次的加密子密钥都是随机的, 这种优化方案的密钥是一次性的, 也就是说, 本次加密完成后密钥就会失去作用, 下次加密的密钥是另外随机生成的, 这种随机密钥, 有比较好的抵抗线性攻击和差分攻击的能力.

(3) 这个优化方案最大的特点就是它是一次性的加密方案, 事实证明唯一不能被破译的加密方法就是一次性的密钥.

6　算法的缺点分析

当然, 这个优化算法也有自己的缺点.

(1) 由于密钥长度过长, 达到 1088 位, 给密钥管理带来了难度, 容易带来安全隐患, 当然, 现在的移动存储技术发达, 这个问题已经不是什么大问题.

(2) 因为这是基于一次密钥的加密算法, 所以它的密钥是一次性的, 跟上面一样, 密钥管理上有难度, 另外, 它每次都需要更换新的密钥, 密钥传输中会有一定的安全隐患, 笔者建议在应用中密钥需要用非对称加密算法来加密传输比如 RSA 等算法.

(3) 由于在 16 次迭代过程中加入了随机的 64 位密钥, 所以算法的速度降低了. 该方案在实现过程中也比较灵活, 可以根据需要减少随机密钥的位数以及去除掉数据位压缩置换操作. 这样能在一定程度上提高它的执行效率.

7　结语

笔者通过阅读 DES 改进方案相关文献, 分析各个改进方案的优缺点, 提出基于一次密钥的方案, 改进后的 DES 算法具有更好的抵抗攻击的能力, 使得 DES 算法有更广阔的前景.

参考文献

1 吕莉,赵嘉.DES 加密算法及其实现的改进.南昌工程学院学报,2006,25(5).
2 谢志强,高鹏飞,杨静.基于前缀码的算法改进研究.计算机工程与应用,2009,45(9):92–94.
3 邓悦恒.3DES 算法原理与设计.电脑知识与技术,2005,20(7):.
4 王静,蒋国平.基于无理数的 DES 加密算法.南京邮电大学学报,2009,29:6.
5 赵风光.算数编码与数据加密.通信学报,1999,20:4.
6 龚蓬,邱凤娇,刘猛.用 cscw 的一种数据加密算法.计算机集成制造系统.2003(9)专刊.
7 顾超.动态 DES 算法.计算机应用与软件,2007,24:7.
8 陈良.一种优化 DES 算法.计算机计算机工程与应用,2004.