文章编号：2095-4980(2013)01-0131-05

基于密钥长度的数据加密标准算法改进

李红芳，杨领军，曹三省

(中国传媒大学 信息工程学院，北京 100024)

摘　要：数据加密标准(DES)算法是典型的分组对称式私钥密码机制，在加密学研究领域中占据着十分重要的地位，且对于以融合网络和物联网为代表的下一代网络中各类嵌入式加密应用而言具有很好的适用性。本文简单介绍了 DES 算法原理及其安全性，主要针对 DES 算法易受穷举攻击法的不足，依据 DES 算法本身的特点提出了改进措施，采用双密钥交叉加密，提高加密过程中密钥的复杂度，增强抵抗攻击的能力，达到对 DES 算法安全性的改善。

关键词：数据加密标准算法；安全；双密钥；交叉加密

中图分类号：TN391；TP309.7　　**文献标识码：**A

Improved Data Encryption Standard algorithm based on the length of key

LI Hong-fang，YANG Ling-jun，CAO San-xing

(School of Information and Engineering, Communication University of China，Beijing 100024，China)

Abstract: Data Encryption Standard(DES) algorithm is a typical private password mechanism，and its group is symmetric. The algorithm is very important in the field of encryption study. It is adaptive to the applications for encryption in many different systems, especially in the embedded system of Internet of Things(IOT) and Convergence Networks in the next generation. This article simply introduces the principle and the safety of DES algorithm. According to the characteristics of the DES algorithm，an improved scheme is put forward in order to overcome its easily attacked shortcomings. This method adopts two keys to crosswise encrypt. It can improve the complexity of encryption key in the process and enhance the ability of resisting attack, therefore, the safety of DES algorithm is improved.

Key words: Data Encryption Standard；safety；double-key；cross-encryption

美国国家标准局(NBS)于 20 世纪 70 年代初，向公众发出了征求加密算法的公告，在 70 年代末美国政府宣布采用 IBM 公司设计的方案作为加密算法，并命名为 DES 算法。在当时的技术条件下，利用有效的 56 bit 密钥的 DES 算法完全可以满足 NBS 对加密算法提出的要求。该算法的设计目标是加密保护静态的存储和在信道中传输的数据，因此 DES 算法曾在磁卡、ATM 机及智能 IC 卡、加油站、高速公路收费站等领域被广泛应用，以此来实现关键数据的保密。信用卡持卡人的 PIN 的加密传输，IC 卡的双向认证等，都用到了 DES 算法，并且 DES 在电子商务中也得到了广泛的应用[1]。随着计算机技术的飞速发展，数据加密技术也得到了极大的发展，然而 DES 加密算法的不足也不断凸显，密钥较短，迭代次数少，分组较短，S 盒存在隐患等[2]，但是它作为加密算法的开端，在数据加密领域中发挥着重要作用，因此对 DES 分组密码的改进是有意义的工作。

1　DES 算法的基本原理

1.1 原理

DES 算法是一种典型的分组对称式加密算法。每次以 64 bit 数据块为加密对象，密钥 K 的长度也是 64 bit，但实际有效的只有 56 bit，第 8 bit、第 16 bit、第 24 bit、第 32 bit、第 40 bit、第 48 bit、第 56 bit、第 64 bit 作为校验位。数据块需要经过 16 轮加密运算，每轮使用不同的子密钥 $K(i)$，每轮子密钥由初始密钥 K 按照置换表生成，加密后的密文长度也是 64 bit。解密过程与加密过程互逆。

收稿日期：2012-03-31；修回日期：2012-05-15

DES 算法结构紧凑，条理清楚，综合运用了多种加密技术，如代替、置换、代数等[3]。其中算法的主要部分为 Feistel 网络结构，也可以认为 DES 是 Feistel 结构的一种实现。DES 加密过程大致可以分为 3 个阶段：初始置换；16 次迭代变换(圈变换)；末置换。加密示意图如图 1 所示，基本过程概述如下：

首先，给定 64 bit 明文，经过初始置换 IP 表变换，将明文重新排列，前 32 bit 作为 $L0$，后 32 bit 作为 $R0$，再将 64 bit 密钥经过固有的密钥算法得到 16 个子密钥，用 $K1,K2,K3,\cdots,K16$ 表示，分别供 16 次迭代使用，进行 16 轮完全相同的变换，得到 $L16$ 和 $R16$，最后将 $R16,L16$ 进行 IP 逆置换得到密文，即 $IP^{-1}R16L16$。其中对明文右半部分等进行的 f 变换为非线性变换，包括扩展置换、与子密钥异或、S 盒代替和 P 置换，f 的输出结果与上一轮的左半部分异或作为下一轮的输入。DES 的解密过程是加密过程的逆过程，其运算与加密相似，只是子密钥的输入顺序与加密时的顺序相反。

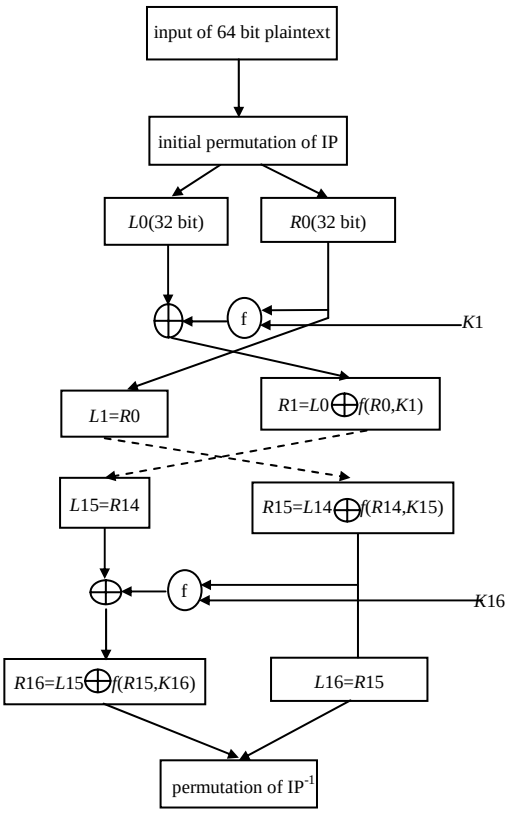

Fig.1 Encryption process of DES
图 1 DES 加密过程

1.2 安全性

DES 算法的主要目的是为加密保护存储的静态数据和在信道中传输的数据，自公布以来，成为了计算机通信和国际上商用保密通信最常用的加密算法。随着计算机技术的突飞猛进，DES 算法的不足也逐渐暴露出来，人们对 DES 的安全性持怀疑态度，对它的抗攻击强度非常关注。其中主要针对 DES 加密算法的密钥长度、S 盒的设计、分组长度和迭代次数等[4]。

1) 密钥长度较短，仅有 56 bit，密钥空间的大小为 2^{56}，在现有技术条件下用穷举攻击法进行攻击来获取正确密钥已趋于可行，并且随着计算速度的提高，为此所付出的代价越来越小，所以不宜用 DES 算法保护重要的数据信息。又由于在子密钥产生的过程中，16 个子密钥至少首尾相同，或者会出现更多的子密钥重合现象，从而会有半弱密钥和弱密钥现象，同样降低了 DES 的安全性。

2) S 盒的设计也被质疑，DES 算法中的非线性变换采用的是 8 个 S 盒，S 盒作为 DES 算法中惟一的非线性部分，也是整个算法安全性所在，它的设计原则与过程是保密的，从而被很多人认为其可能存在隐患，易被差分密码攻击[5]。

3) DES 算法中明文、密钥与密文之间存在着互补的特性，即密钥对明文加密后产生的密文，与密钥的补对明文的补加密后产生的密文是互补的，利用 DES 的互补性来找出密钥，破解算法会花费更少的时间。

4) 选择明文攻击也会破坏 DES 算法的安全性[6]。DES 算法的分组数据块较短，攻击者可以事先任意选择一段明文让被攻击的加密算法加密，并得到相应的密文，攻击者通过该过程获得关于加密算法的一些信息，以利于在将来更有效地破解由同样加密算法加密的数据。

1.3 DES 改进相关研究综述

当前，人们为了加强 DES 算法的加密强度以及提高加密的效率，针对前文提到的 DES 算法中存在的安全性等问题提出了一些改良方法，如改变 S 盒，增加分组的长度，采用 N 重 DES 加密，增加迭代次数等，但是也会因为算法中的一些改变出现一些新的问题：如 S 盒被改变，作为加密算法的核心，改变了算法中唯一的非线性变换，整个算法的安全性无法预知，或许会削弱算法的加密能力；又如 N 重 DES 加密算法，虽然多次进行的加密解密间接地增加了密钥的长度，但也同样多花费了 N–1 倍的时间[7]，从而降低了运行效率，对于较长文件的加密，该方法存在明显不足。

2 基于密钥长度的 DES 算法改进

2.1 算法的理论分析

虽然 DES 已经成了如今主要的被分析或攻击的算法，但是人们对于算法的结构仍然无可挑剔，并未发现它

的不足。从 DES 算法发展到多重加密算法，如 3DES 等，再到如今的 AES 算法，其中的关键是密钥的长度问题，被加密的数据的安全性依赖于密钥，DES 算法密钥的长度有待更深入的研究[8]。

本文在基于密钥长度进行 DES 改进的研究中，为改善密钥较简短的现象，提出了一种改进方法，即通过适当加大密钥长度，提高加密的复杂度。3DES 及 *N* 重 DES 加密的思想是进行了多次的 DES 加/解密，来增加密钥的长度，从而增长加密时间，降低加密的效率，换取加密的安全性。Shannon 证明了一次一密密码体制是不可破的，这给研究和改进加密算法带来了很大启发。鉴于此，本文欲采用 2 个密钥对明文进行加密[9]，改变算法的整体框架结构，在进行 16 轮迭代时使用的 16 个子密钥分别由 2 个密钥各产生 8 个，该想法将 DES 算法的密钥长度由 64 bit(实际密钥长度是 56 bit)延长到 128 bit(实际密钥长度是 112 bit)，提高了 DES 算法加密效果。理论分析可知，该改进算法并未降低算法的效率，加密效率明显高于 3DES 加密[10]。

如图 2 所示，由 *K*1 按照子密钥的生成方式分别产生第 1，第 3，第 5 到第 15 个奇数位的子密钥，同样，第 2，第 4，第 6 到第 16 个偶数位的子密钥由 *K*2 产生，子密钥交叉式的加密方式，增加了相邻密钥间的非线性，相当于增加了除 *S* 盒之外的一些非线性部件，从而增强了加密效果。

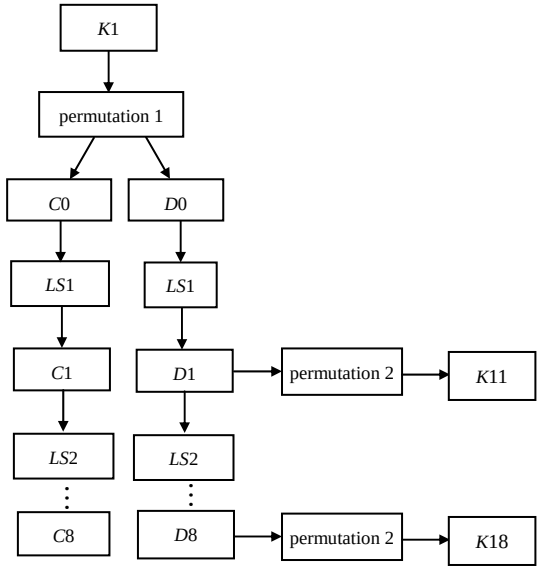

Fig.2 Produce of sub-key
图 2 子密钥的生成

2.2 改进算法的验证

本文采用人们较易理解和接受的 C/C++语言实现 DES 算法对文件的加密，加密过程中可以人为输入加密所需要的密钥以及被加密的文件。在对算法的改进中，主要针对子密钥的生成函数部分进行改进：

```
int DES_MakeSubKeys(char key1[64],char key2[64],char subKeys[16][48])
{
    char temp1[56],temp2[56];
    int cnt;
    DES_PC1_Transform(key1,temp1);//PC1 置换
    DES_PC1_Transform(key2,temp2);
    for(cnt = 0; cnt < 16; cnt=cnt+2){//产生奇数轮加密的 8 个子密钥
        DES_ROL(temp1,MOVE_TIMES[cnt]);//循环左移
        DES_PC2_Transform(temp1,subKeys[cnt]);//PC2 置换，产生子密钥
    }
for(cnt = 1; cnt < 16; cnt=cnt+2){
        DES_ROL(temp2,MOVE_TIMES[cnt]);
        DES_PC2_Transform(temp2,subKeys[cnt]);
    }
    return 0;
}
```

文件的解密过程即为加密的逆过程，解密文件时只需按照逆序调用子密钥，就可以正确地解密文件。

2.3 验证结果对比

下面通过一些简单的实例进行对比说明。选取的明文文件为：87654321hongfang9j8h7g6f1234wertdd6937ss13love1411111111wwwwwwwwaaccddff99661155youmissi20121221，如图 3 所示。选取原 DES 算法的密钥为 desmiyue，取改进后的双密钥分别为：desmiyue,lkjhgfds，通过对比相同文件加密后生成的密文位数的变化引起的密文复杂度以及所需的时间来比较原 DES 算法与改进的 DES 算法的加密效果。为了对比明显，将明文每 8 bit 分为一个数据块，相关文件的截图如图 3~图 6 所示。改变位数的对比如表 1 所示。

表 1 对比结果

Table1 Comparison of results

algorithm	change of number											
original DES	33	27	33	30	33	33	37	29	31	30	30	29
improved DES	32	31	32	26	26	40	37	34	39	34	33	33

Fig.3 Plaintext file
图 3 明文文件

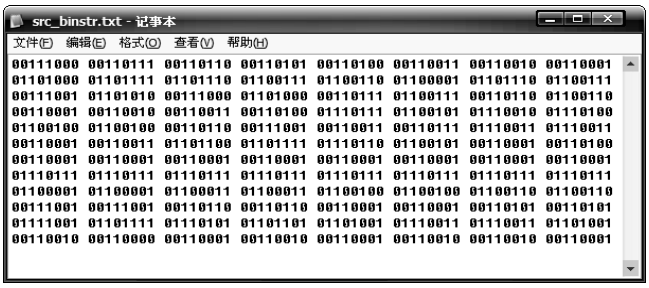

Fig.4 Binary representation of plaintext
图 4 明文二进制表示

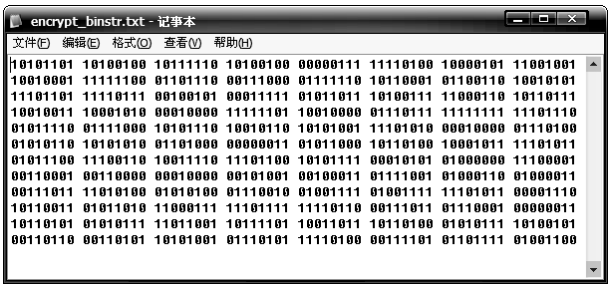

Fig.5 Binary representation of the original DES
图 5 原 DES 加密文件的二进制表示

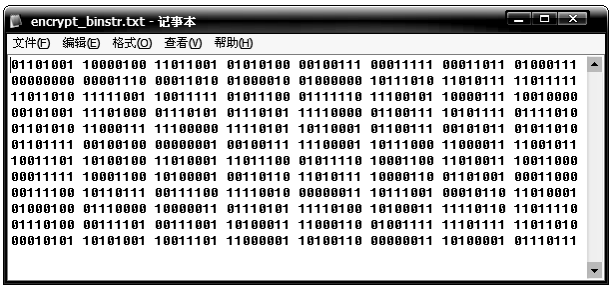

Fig.6 Binary representation of the improved DES
图 6 改进算法的 DES 加密文件的二进制表示

表 1 中 12 组数据简单对比了原 DES 算法和改进的 DES 算法对数据加密后密文的位数改变。可以看出，有的数据加密后变得相对简单些或是与原算法的加密效果差不多，还有稍多些数据改进后的算法可以使加密后的数据变得更复杂些。若要证明整个算法的优越性，需要大量的统计结果对比实现，由于时间等原因，文中没有进行大量数据的加密对比，但是通过上文的理论分析可知，该改进算法有一定的可行性。

加密过程的对比见图 7、图 8。

本例中，从少量的数据加/解密运行结果中可以看出，加解密过程所消耗的时间几乎一样。文件加解密效率相当，所以改进后的算法对加密的效率并无太大的影响。

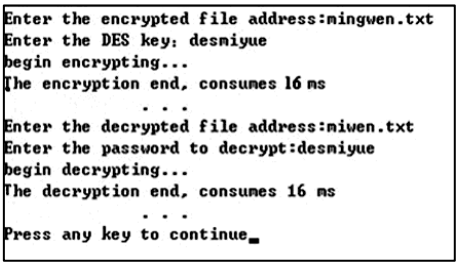

Fig.7 Encryption process of the original DES
图 7 原 DES 加密过程

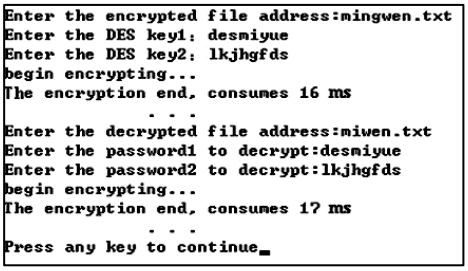

Fig.8 Encryption process of the improved DES
图 8 改进后 DES 加密过程

3 结论

DES 算法中密钥长度一直是被人质疑的一个不足点。本文通过改变原 DES 算法的密钥长度来改进 DES 算法，采用双密钥加密，延长了密钥长度，交叉式地对明文进行加密，增加了明文加密后的复杂度，提高了攻击难度，文中通过理论分析以及实例也进行了说明。

参考文献：

[1] 刘晓星,胡畅霞,刘明生. 安全加密算法 DES 的分析与改进[J]. 微计算机与信息, 2006,22(4):32-33. (LIU Xiaoxing, HU Changxia,LIU mingsheng. The Analysis and Improvement of DES Encryption Algorithm[J]. Micro computer and information, 2006,22(4):32-33.)

[2] 周建钦,何凌云. DES 加密算法的密钥扩展[J]. 科技通报, 2011,27(2):263-267. (ZHOU Jianqin,HE Lingyun. Key Expansion of DES Encryption Algorithm[J]. Bulletin of Science and Technology, 2011,127(2):263-267.)

[3] 吕莉,赵嘉. DES 加密算法的分析及其实现的改进[J]. 南昌工程学院学报, 2006,25(5):28–31. (LV Li,ZHAO Jia. Analysis and Research of DES Encryption Algorithm[J]. Journal of Nanchang Institute of Technology. 2006,25(5):28–31.)
[4] 佟丽亚. 关于对 DES 加密算法进行改进的构想[J]. 邢台职业技术学院学报, 2004,21(3):70–71. (TONG Liya. Improvement about DES Encryption Algorithm[J]. Journal of Xingtai Vocational and Technical College, 2004,21(3):70–71.)
[5] 邱伟星,肖克芝,倪昉,等. 一种 DES 密钥延长方法[J]. 计算机工程, 2011,37(5):167–168. (QIU Weixing,XIAO Kezhi,NI Fang,et al. DES Key Extension Method[J]. Computer Engineering, 2011,37(5):167–168.)
[6] 张清华,邓亚平. 基于一种 DES 算法改进体制的研究[J]. 计算机应用与软件, 2003,20(8):49–51. (ZHANG Qinghua, DENG Yaping. An ameliorative system based on DES algorithm. Computer applications and software, 2003,20(8):49–51.)
[7] Young Won Lim. EFFICIENT 8-CYCLE DES IMPLEMENTATION[C]// The Second IEEE Asia Pacific Conference on ASICs. Cheju,Korea:[s.n.], 2000:175–178.
[8] Jee Sung-ho,Paul Montague. A Secure DES Implementation for Real-time Embedded Applications[C]// 1999 Third International Conference on Knowledge-Based Intelligent Information Engineeing Systems. Adelaide:[s.n.], 1999:496–500.
[9] 肖丰霞,刘嘉勇,李国勇,等. 基于电子钥匙的双向身份鉴别方案[J]. 信息与电子工程, 2007,5(6):473–475. (XIAO Fengxia,LIU Jiayong,LI GuoYong,et al. Mutual Authentication Scheme Using USB KEY[J]. Ineformation and Electronic Engineerinc, 2007, 5(6):473–475.)
[10] 周斌,彭应宁,汤俊. 雷达系统超精简流式 AES 加密器设计和优化[J]. 信息与电子工程, 2010,8(3):276–280. (ZHOU Bin, PENG Yingning,TANG Jun. Design and optimization of compact AES as stream cipher in radar system[J]. Information and Electronic Engineering, 2010,8(3):276–280.)

作者简介:

李红芳(1987–),女,河北省沧州市人,在读硕士研究生,研究方向为新媒体、无线监控.email:840459384@qq.com.

杨领军(1968–),男,山东省东营市人,博士,副教授,研究方向为数字信号处理、多媒体技术、集成电路设计、无线监控等.

曹三省(1977–),男,北京市人,博士,副教授,研究方向为智能媒体系统、移动新媒体、互动媒体关键技术等.