DOI:10.16039/j.cnki.cn22-1249.2012.11.007

文章编号:1007-2853(2012)11-0127-03

基于DES算法的系统优化设计

付秀伟
(吉林化工学院 信息与控制工程学院,吉林 吉林 132022)

摘要:随着密码分析方法技术的进步,使得DES算法的安全受到严重的威胁,改进DES算法是提高其安全性的有效途径.分析了DES安全性的相关公式,提出一种简单实用的改进方案.该体制扩充了密钥长度,增强了密码分析攻击难度.

关 键 词:DES算法;安全性;改进方案;密钥长度
中图分类号:TP 332.3 **文献标志码**:A

随着Internet和科技的发展,人们使用计算机网络传递安全敏感信息的情况越来越普遍,如网上银行业务、商业数据交换、政府秘密信息传递、网上交易电子支付系统等.信息安全问题日趋突出,信息泄密、篡改、伪造等案件日益上升,因此如何消除数据安全隐患已成为人们十分关心和重视的问题,信息安全也成为信息科学领域的热门学科,这一学科的研究不但具有重要的理论研究价值,而且具有广泛的实际应用价值[1].在这种情况下,数据加密是保证信息机密性的唯一方法[2].

数据加密标准(Data Encryption Standard,DES),作为ANSI的数据加密算法(Data Encryption Algorithm)和ISO的DEAI,成为一个世界范围内标准已经20多年了.它很好地抵抗多年密码分析,但目前穷举攻击法及差分攻击对其已可以破译,所以加强DES算法安全性已迫在眉睫.DES算法中起混乱作用的其他运算都是线性的,易于分析和破解,除了S盒是非线性的,所以S-BOX是DES算法中重要步骤,它为DES的安全性提供了保障[3].

1 DES算法原理

DES是一种对称分组密码算法,也可以说是块加密法,既可用于加密,又可用于解密,每次分组数据按64位块长进行加密或解密.它的密钥有效长度是56位,密钥是保密的,它可以是任意的56位的二进制数,也可以任意时候改变.64位的明文进行分组,明文分组后与有效的56位密钥按替代或交换的方法形成密文组.对于度量分组密码安全性,Shannon从理论上给出了表达式,而且提出了两种原则:混乱与扩散性原则,用于隐蔽明文消息中的冗余度[4].

明文先通过一个初始置换(IP),将明文分组分成左半部分(L)和右半部分(R),各32位长,R_0与子密钥K_1进行F函数的运算,输出32位的数,然后与L_0执行异或操作得到R_1,L_1则是上一轮的R_0,经过16轮后,左、右半部分合在一起,经过一个末置换(初始置换的逆置换),完成整个DES算法流程.另外,DES解密过程与加密算法流程是一模一样的,但解密过程中16轮的子密钥序列由$K_1,K_2,\cdots,K_{16}$的顺序倒过来,即第一轮子密钥为加密算法第16个子密钥K16.第2轮子密钥为原有密钥K_{15},依此类推,即DES算法的流程,如图1所示.

其中,图中⊕表示以2为模的逻辑异或运算.IP表示初始置换,而IP-1表示逆置换,初始置换和逆置换是相反的两种操作.F是R和Kn的非线性函数[5],F函数包括S-BOX非线性运算,即DES算法中关键部分.DES算法中所有其它的运算均是线性的,对外界来说是易于分析的,而S盒是整个算法中唯一非线性的部分.由S盒来实现的非线性运算为DES提供了更好的安全性.

收稿日期:2012-09-12
作者简介:付秀伟(1983-),男,山东泰安人,吉林化工学院助教,硕士,主要从事嵌入式方面的研究.

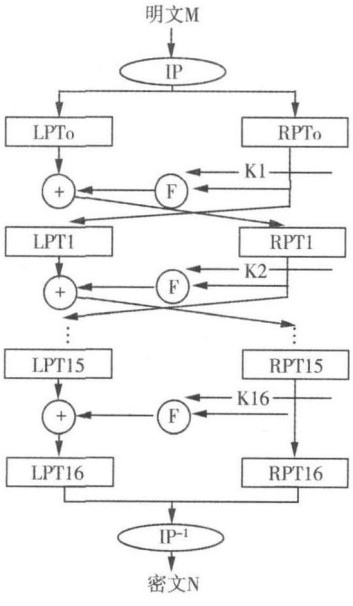

图1 DES算法的流程图

2 DES算法安全性分析及改进

2.1 算法安全性分析

理论上DES算法具有较好的安全性,到目前为止,除了用穷举搜索法对DES算法进行攻击外,还没有发现更有效的办法.但随着科学技术的发展[6],超高速计算机面世以后,现在DES加密算法的安全性受到威胁,因为它的密钥仅为56位,以现代计算能力,24小时内即可能被破解.解决的办法有两个,一则考虑把DES密钥的长度再增长一些,二则提高DES算法的安全强度,以此来达到更高的保密程度.对应DES的安全性能可以通过定理了解.

定理1:设DES的密钥扩展法为$K=e(k)$,其中k为密钥种子,K为所生成的加密密钥.则$\overline{K}=e(\overline{k})$,即当密钥种子取补时,加密密钥全部取补.

引理1:对于DES轮函数的钥控非线性函数,k为轮子密钥,有$F(\overline{x},\overline{k})=F(x,k)$.

定理2:设DES的加密算法为$y=DES(x,k)$,其中k为密钥种子,则$\overline{y}=DES(\overline{x},\overline{k})$.

对于密钥种子k,如果$DES^{-1}(g,k)=DES(g,k)$,则称k为一个弱密钥.根据DES的密钥扩展算法,有4个弱密钥:$k=(0,\cdots,0)$;$k=(1,\cdots,0)$;$k=(0,\cdots,0,1,\cdots1)$;$k=(1,\cdots,1,0,\cdots0)$.

由上述DES算法介绍可以看到:DES算法中只用到64位密钥中的其中56位,而第8,16,24,……,64位8个奇偶校验位并未参与DES运算,即DES的安全性是基于除了8,16,24,……,64位外的其余56位的组合变化2^{56}才得以保证的,但由于除去8位奇偶校验,也使得整个算法密钥短,易受到线性攻击加以破解,无法保证信息安全.

2.2 算法改进方法

针对于选择函数组S-BOX的位置,设定不再固定为从S1到S8[7-8].原有的S-BOX共8个BOX,放置仅一种模式,针对具体差分分析和线性分析攻击方法,令S-BOX排列具有随机化.其原理利用排列组合实现.

正整数P可以利用$(P_{n-1},P_{n-2},L\,p_2,p_1)$来表示,其中$0\leqslant p_i\leqslant i$,而且,$(p_{n-1},p_{n-2},L\,p_2,p_1)$可以表示一组数1,2……$n$的排列组合.令$p_i$表示排列$1,Q_2,\cdots,Q_n$中在$i-1$位置前面且比$i-1$大的数个数.举例说明:$(p_4,p_3,p_2)=(1,2,3)$其中$p_4=0$,表示3前面有1个比3大的数字,$p_3=2$表示2前面有2个比2大的数字2,$p_2=3$表示数字1前面有3个比1大的数字(即数字1在最后面),所以(1,2,3)对应的排列组合为4,3,2,1,所以利用7个数字就可以表示8个S-BOX的顺序.同时,从DES算法密钥变换中,可知,最初64位密钥通过放弃8位而得到56位密钥.这样,每一轮有56位密钥,而每一轮从56位密钥产生不同的48位子密钥,称为密钥变换.压缩置换如表1所示.

表1 压缩置换

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

从表格中观察,可以得知,其中舍弃的8位数字分别为9,18,22,25,35,38,43,54.与最初密钥放弃的8位奇偶校验位加和为16位.而DES算法共16轮,在每一轮均要产生一个子密钥,由于DES算法固有的轮号有固定的左移位数,而使破译较为简单,所以,通过舍弃的16个数字通过上述组合排列方式,利用 表示16个数字排列,其中,这16个数字对应的位数为分别为16轮子密钥生成时循环左移的位数.由于56位密钥分组,成为两组28位,在进行循环左移时,28位小于16个数字中的子集{32,35,38,40,43,48,54,56,64}但在循环左移中实质左移位数位{4,7,10,12,15,26,0,8},即16轮分别循环左移位数为{8,9,16,18,22,24,25,4,7,10,12,15,26,0,8}.那么,排列

后 S-BOX 由原来一种模式,增加到 8! 种模式,子密钥生成循环左移的模式由原来一种情况随机增加到 16! 种模式,对线性逼近的攻击有较好的抵御效果.

3　改进方案的安全性分析

本文方案是基于 DES 的,保留了原 DES 密码体制的各种置换,压缩变化,保留和继承了原密码体制的优点,而改进的方案仅仅针对 S-BOX 序列及子密钥生成做了相应变换,改善原有密码体制的缺点.

(1) 密钥长度的增加,原有密码体制中密钥生成实质为 56 位二进制码,舍弃了 8 位奇偶校验位,本文充分利用其舍弃 8 位,参与整个加密流程中,所以增加密钥长度到 64 位.

(2) 消除半弱密钥,分析已知的 6 对 DES 半弱密钥,由于子密钥移位位数不定及 S-BOX 组合排列,没有哪一对半弱密钥的奇偶校验位是完全一致的,所以消除半弱密钥.

(3) 消除 S-BOX 陷门,采用本文改进方案,即使 DES 算法中 S-BOX 设计中存在陷门,但不知道密钥也就无法得知 S-BOX 排列顺序,更无法利用陷门加以破解.

4　结　　论

本文基于 DES 算法原理,对 DES 算法内部结构进行详细分析,针对其原有算法的缺点,进行算法优化,对唯一的非线性函数 S-BOX 进行改进,同时,利用密钥舍弃的位数与 F 函数运算及生成子密钥,增加密钥长度、消除陷门、消除半弱密钥,有效提高 DES 算法的安全性.

参考文献:

[1] 温凤桐. 分组密码工作模式的研究[D]. 北京:北京邮电大学,2006:1-2.

[2] SchneierB. 应用密码学:协议、算法与 C 源程序[M]. 吴世忠,祝世雄,张文政,等译. 北京:机械工业出版社,2000.

[3] Patterson, C. High performance DES encryption in virtex FPGAs using Jbits [C]. FCCM' 00, Napa Valley, CA, USA: IEEE Comput Press, April 2000: 113-121.

[4] 周旋. 分组密码的设计与分析[D]. 长沙:国防科技大学,2003:8-11.

[5] S. Trimberger, R. Pang, and A. Singh, A 12 Gbps DES Encryptor/Decryptor Core in an FPGA [C], Proc. Cryptographic Hardware and Embedded Systems, 2000:156-163.

[6] 胡予濮,张玉清,肖国镇. 对称密码学[M]. 北京:机械工业出版社,2002:152-179.

[7] 肖堃,罗蕾. 一种 DES 的改进方案[J]. 福建电脑,2008,5.

[8] 付莉. 一种基于改进 DES 算法的高效率 FPGA 硬件实现[J]. 桂林电子科技大学学报,2009,(6).

Design of System Optimization based on DES Algorithm

FU Xiu-wei

(School of Information and Control Engineering, Jilin University of Chemical Technology, Jilin 132022, China)

Abstract: With the technical progress of password analysis method, the safety of DES algorithm be sustained serious threats, improving DES algorithm is an effective way to improve the safety. This paper analyzes the related formula of safety DES, and it puts forward a simple and practical improvement plan. This system expands key length and enhances the code analysis against difficulty.

Key words: DES algorithm; safety; improvement plan; key length