实验二 分组密码算法 DES

一、 实验目的

通过用DES算法对实际的数据进行加密和解密来深刻了解DES的运行原理。

二、 实验原理

分组密码是一种对称密码体制，其特点是在明文加密和密文解密的过程中，信息都是按照固定长度分组后进行处理的。在分组密码的发展历史中，曾出现了许多优秀的算法，包括 DES，IDEA，AES，Safer＋＋等等。下面以 DES 算法为例介绍分组密码算法的实现机制。

DES 算法将明文分成 64 位大小的众多数据块，即分组长度为 64 位。同时用 56 位密钥对 64 位明文信息加密，最终形成 64 位的密文。如果明文长度不足 64 位，即将其扩展为 64 位（如补零等方法）。具体加密过程首先是将输入的数据进行初始置换（IP），即将明文 M 中数据的排列顺序按一定的规则重新排列，生成新的数据序列，以打乱原来的次序。然后将变换后的数据平分成左右两部分，左边记为 L_0，右边记为 R_0，然后对 R_0 实行在子密钥（由加密密钥产生）控制下的变换 f，结果记为 f（R_0，K_1），再与 L_0 做逐位异或运算，其结果记为 R_1，R_0 则作为下一轮的 L_1。如此循环 16 轮，最后得到 L_{16}、R_{16}，再对 L_{16}、R_{16} 实行逆初始置换 IP^{-1}，即可得到加密数据。解密过程与此类似，不同之处仅在于子密钥的使用顺序正好相反。DES 全部 16 轮的加密过程如图 1－1 所示。

DES 的加密算法包括 3 个基本函数：

1．初始置换 IP

它的作用是把输入的 64 位数据块的排列顺序打乱，每位数据按照下面的置换规则重新排列，即将第 58 位换到第一位，第 50 位换打第 2 位，…，依次类推。置换后的 64 位输出分为 L_0 、R_0（左、右）两部分，每部分分别为 32 位。

58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4

62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8

57 49 41 33 25 17 9　1 59 51 43 35 27 19 11 3

61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7

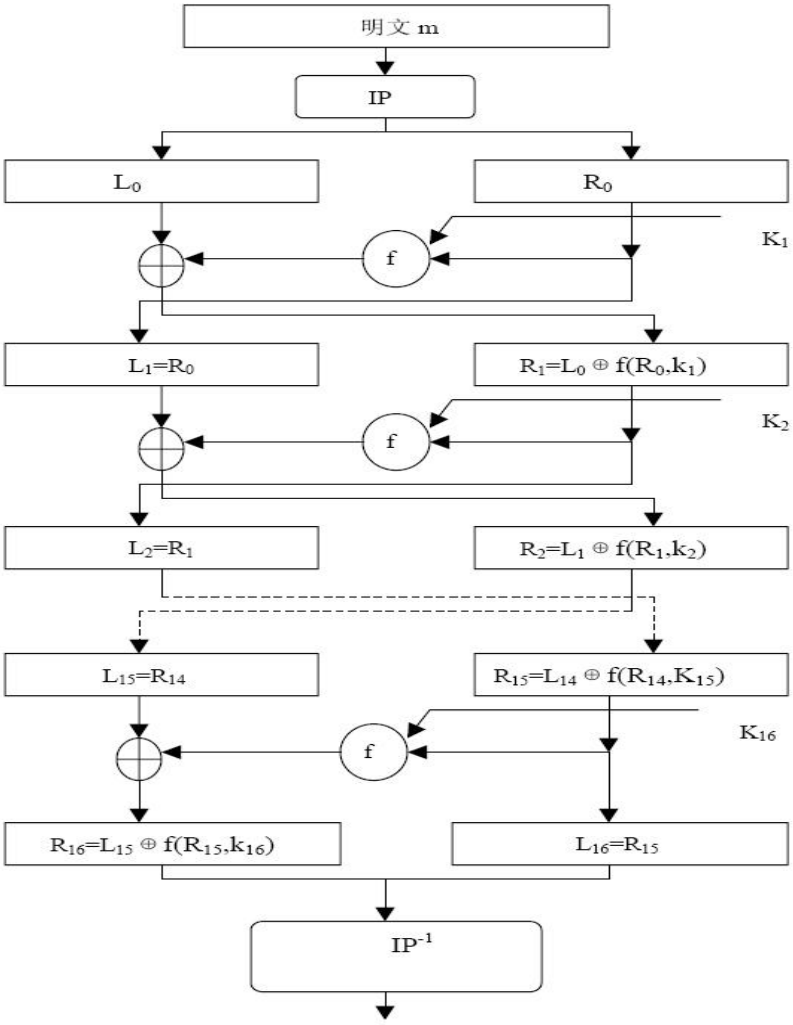

图 1－1 DES 加密/解密流程

R_0 和 K_1 经过 f（R_0，K_1）变换后的输出结果，再和 L_0 进行异或运算，输出结果位 R_1，R_0 则赋给 L_1。L_1 和 R_1 同样再做类似运算生成 L_2 和 R_2，…，经过 16 次运算后生成 L_{16} 和 R_{16}。

2．f 函数

f 函数是多个置换函数和替代函数的组合函数，它将 32 位比特的输入变换为 32 位的输出，如图 1－2 所示。R_i 经过扩展运算 E 变换后扩展为 48 位的 $E(R_i)$，与 K_{i+1} 进行异或运算后输出的结果分成 8 组，每组 6 比特。每一组再经过一个 S 盒（共 8 个 S 盒）运算转换为 4 位，8 个 4 位合并为 32 位后再经过 P 变换输出为 32 位的 $f(R_i,K_{i+1})$。其中，扩展运算 E 与置换 P 主要作用是增加算法的扩散效果。

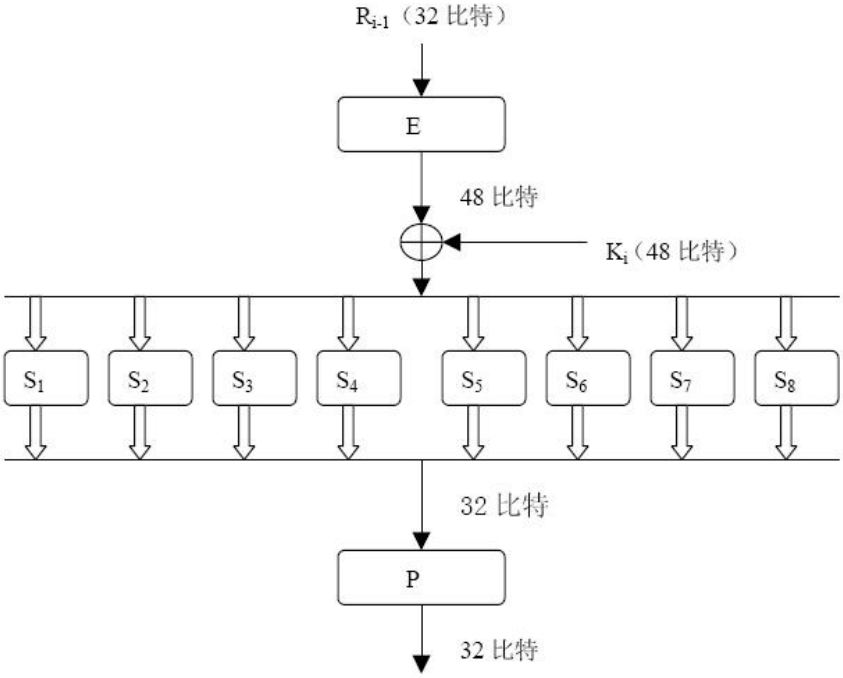

图 1－2 f 函数原理图

3．逆初始置换 IP^{-1}

它将 L_{16}和 R_{16}作为输入，进行逆初始置换得到密文输出。逆初始置换是初始置换的逆运算，置换规则如下所列：

40，8，48，16，56，24，64，32，39，7，47，15，55，23，63，31

38，6，46，14，54，22，62，30，37，5，45，13，53，21，61，29

36，4，44，12，52，20，60，28，35，3，43，11，51，19，59，27

34，2，42，10，50，18，58，26，33，1，41，9， 49，17，57，25

DES 的加密算法中除了上面介绍的 3 个基本函数，还有一个非常重要的功能模块，即子密钥的生成模块，具体子密钥的产生流程图如图 1－3 所示。输入的初始密钥值为 64 位，但 DES 算法规定，其中第 8、16、…、64 位为奇偶校验位，不参予 DES 的运算。所以，实际可用位数只有 56 位，经过缩小选择位表 1（表 1－2）即密钥置换 PC-1 的变换后，初始密钥的位数由 64 位变成了 56 位，将其平分位两部分 C_0，D_0。然后分别进行第一次循环左移，得到 C_1和 D_1，将 C_1（28 位）、D_1（28 位）合并后得到 56 位的输出结果，再经过压缩置换 PC-2(表 1－3)，从而得到了密钥 K_1（48 位）。依次类推，便可得到 K_2、…、K_{16}。需要注意的是，16 次循环左移对应的左移位数要依据表 1－1 的规则进行。

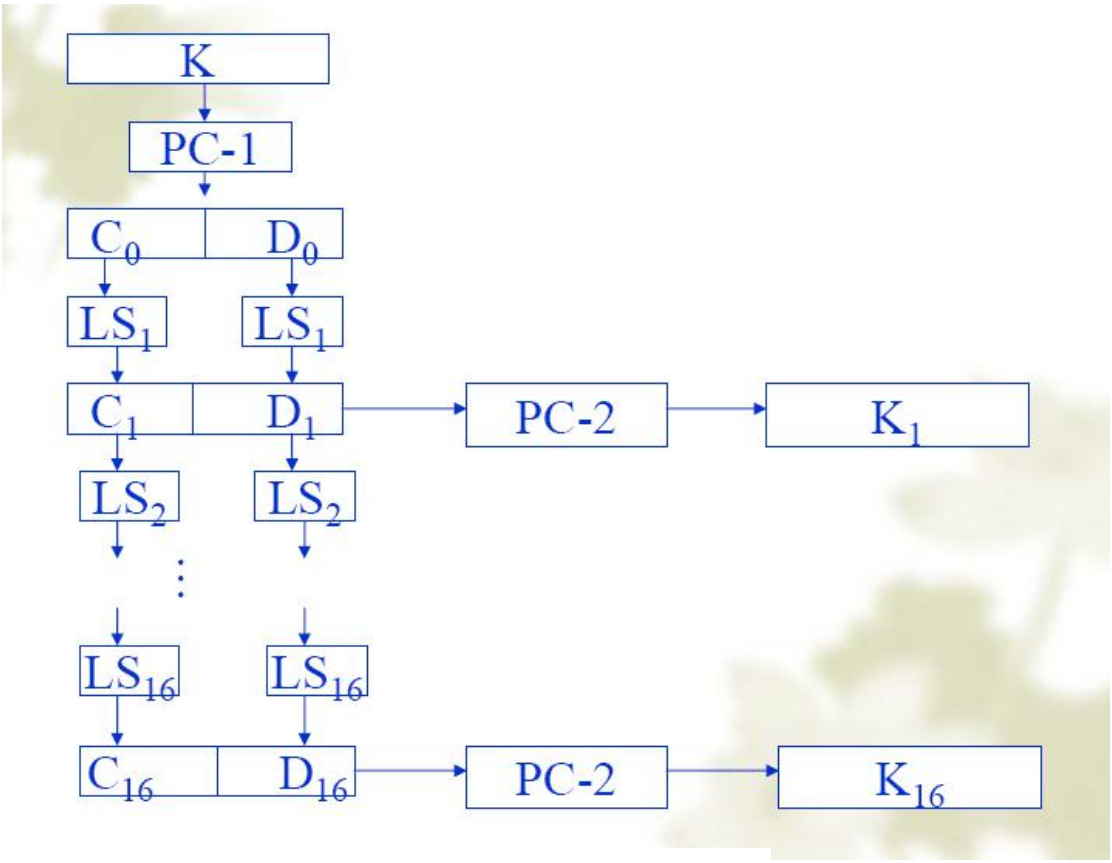

图 1－3 子密钥的生成流程

表 1－1 左移位数规则

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LS_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 1－2 压缩置换 PC－1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

表 1－3 压缩置换 PC－2

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	3	48
44	49	39	56	34	53
46	42	50	36	29	32

三、 实验环境

运行 Windows 操作系统的 PC 机，具有 VC 等语言编译环境

四、 实验内容和步骤，

1．算法分析：

对课本中 DES 算法进行深入分析，对初始置换、E 扩展置换，S 盒代换、轮函数、密钥生成等环节要有清晰的了解，并考虑其每一个环节的实现过程。

2．DES 实现程序的总体设计：在第一步的基础上，对整个 DES 加密函数的实现进行总体设计，考虑数据的存储格式，参数的传递格式，程序实现的总体层次等，画出程序实现的流程图。

3．在总体设计完成后，开始具体的编码，在编码过程中，注意要尽量使用高效的编码方式。

4．利用 3 中实现的程序，对 DES 的密文进行雪崩效应检验。即固定密钥，仅改变明文中的一位，统计密文改变的位数；固定明文，仅改变密钥中的一位，统计密文改变的位数。

五、 实验报告和要求

（1） 分别实现 DES 的加密和解密，提交程序代码和执行结果。

（2） 在检验雪崩效应中，要求至少改变明文和密文中各八位，给出统计结果并计算出平均值。