DES 算法的 C++实现

16340305 郑先淇

算法原理概述

DES 主要包含三部分：

1. IP 置换
2. 轮巡函数与 16 个字密钥加密的过程；
3. IP 逆置换；

算法详解

1. IP 置换

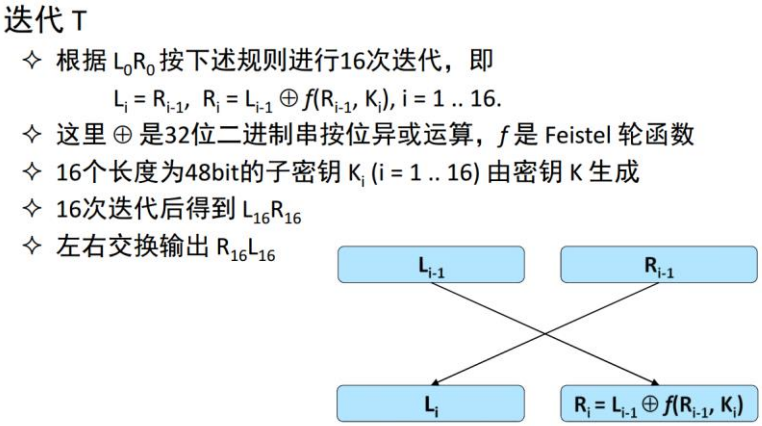
   IP 置换矩阵如下：

IP 置换表							
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

   64 位明文根据 IP 置换表进行置换，规则为：置换表中每个小方格的位置代表原先 64 位明文的对应的位，方格中的数字为产生的 64 位字符中该位所放置的原先的 64 位明文的位；举例：图中 58 表示新的字符串的第一位是原先字符串的第 58 位；

2. 轮巡函数与 16 个字密钥加密；

   首先是轮巡的过程



轮巡函数的具体内容：

(1) 将长度为32位的串 R_{i-1} 作 E-扩展，成为48位的串 $E(R_{i-1})$

(2) 将 $E(R_{i-1})$ 和长度为48位的子密钥 K_i 作48位二进制串按位异或运算，K_i 由密钥 K 生成

(3) 将 (2) 得到的结果平均分成8个分组 (每个分组长度6位)，分别经过8个不同的 S-盒进行 6-4 转换，得到8个长度分别为4位的分组

(4) 将 (3) 得到的分组结果合并得到长度为32位的串

(5) 将 (4) 的结果经过 P-置换，得到轮函数 $f(R_{i-1}, K_i)$ 的最终结果

E-扩展的规则：

E-扩展规则 (比特-选择表)					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

S-box 盒：

S_1-BOX															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	15	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2-BOX															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3-BOX															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4-BOX															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
12	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

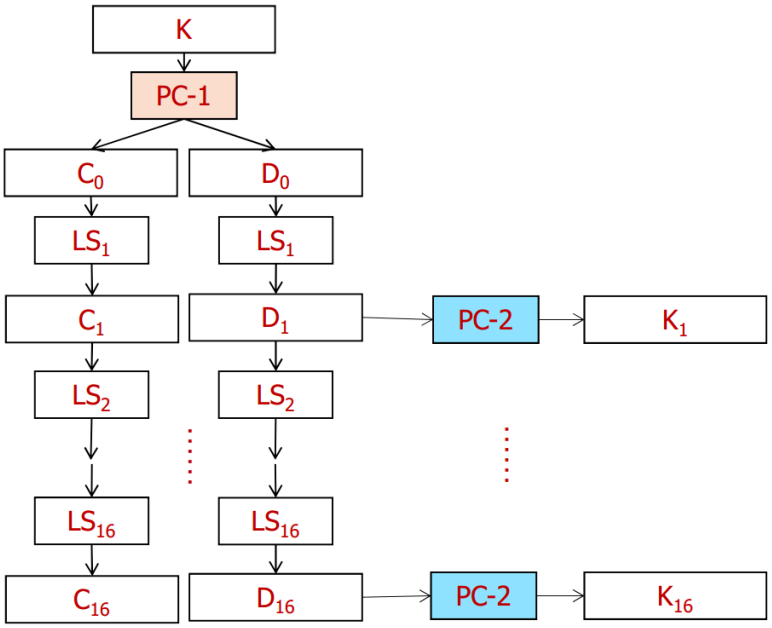
S_5-BOX															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6-BOX															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7-BOX															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8-BOX															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

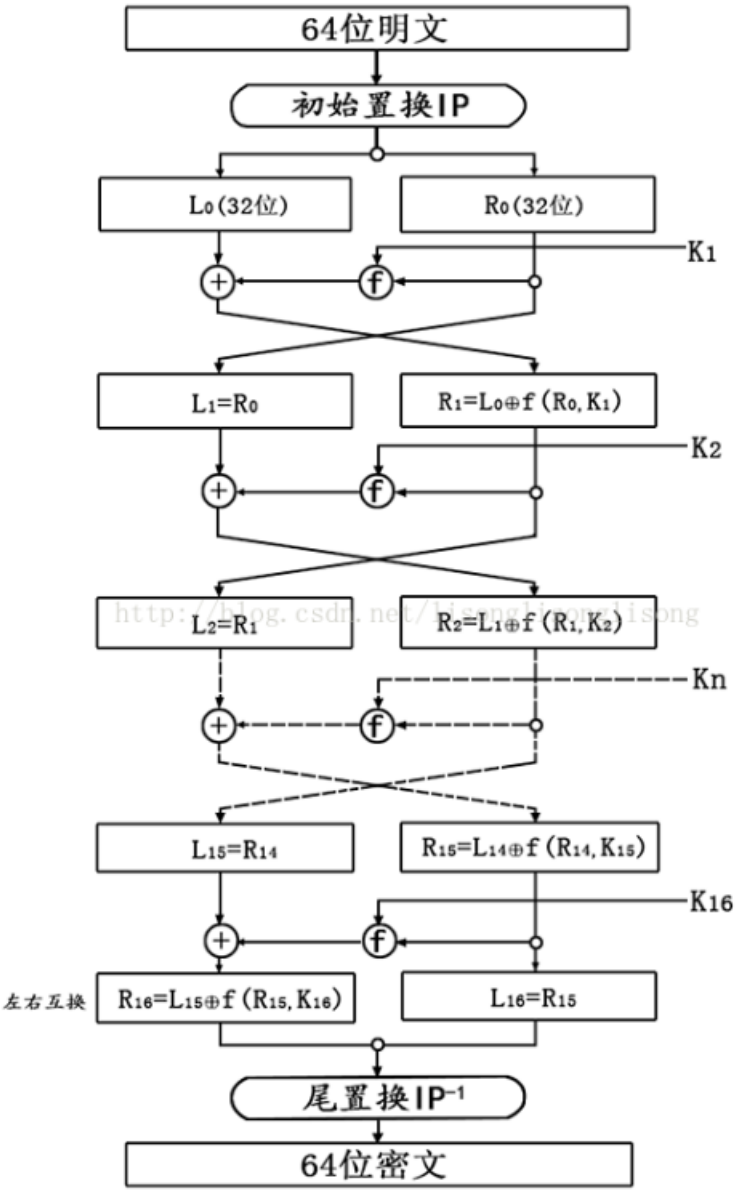
字密钥生成：



P-置换表

P-置换表			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

总体结构



数据结构

IP 置换矩阵、IP 逆置换矩阵、8 个 S_box 盒、P 置换矩阵

编译运行的结果