加密和解密可以使用相同的算法。加密和解密唯一不同的是秘钥的次序是相反的。就是说如果每一轮的加密秘钥分别是K1、K2、K3...K16，那么解密秘钥就是K16、K15、K14...K1。为每一轮产生秘钥的算法也是循环的。加密是秘钥循环左移，解密是秘钥循环右移。解密秘钥每次移动的位数是：0、1、2、2、2、2、2、2、1、2、2、2、2、2、2、1。

ri\_48

li\_48

ro\_48

lo\_48

**des\_subkeys\_unit.v**

**des\_subkeys\_gen.v**

低28bits

高28bits

48bits

**E**

**S**

48bits

**P**

**F**

RI

LI

RO

LO

**des\_f\_structure.v**

KI 48bits

48bits

**PC2**

28bits

28bits

28bits

28bits

**×15**

**<<**

**<<**

输入64bits明文 0x0123 4567 89AB CDEF

(最左边的位为1，最右边的位为64)

**IP**

高32bit(L0)

是4

低32bit(R0)

64bits

64bits

**PC1**

**IP-1**

输出64bits密文

0x85E8 1354 0F0A B405

是4

输入64bits密钥

0x1334 5779 9BBC DFF1

32bits

32bits

**×15**

32bits

32bits

32bits

32bits