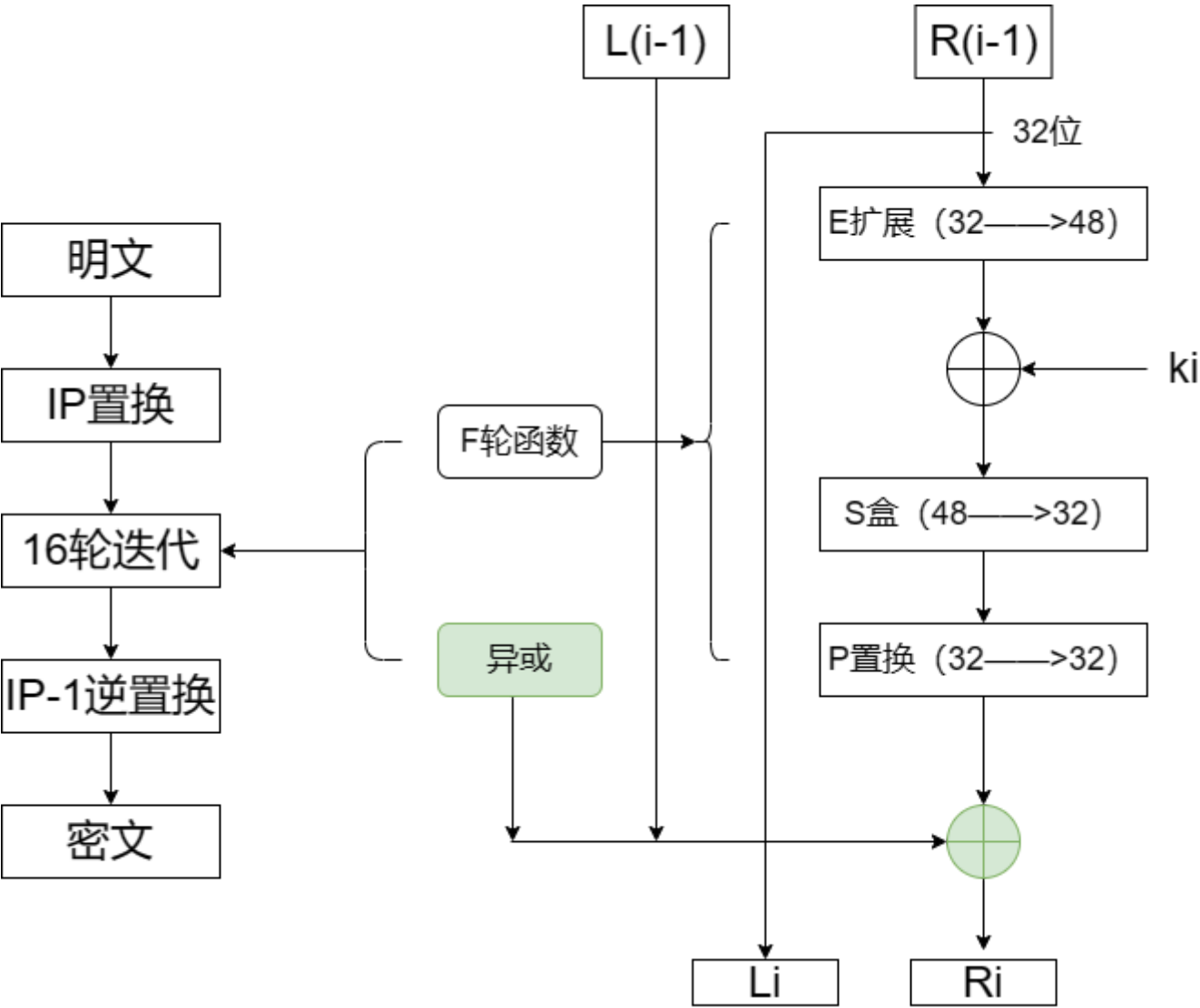


DES算法实现。

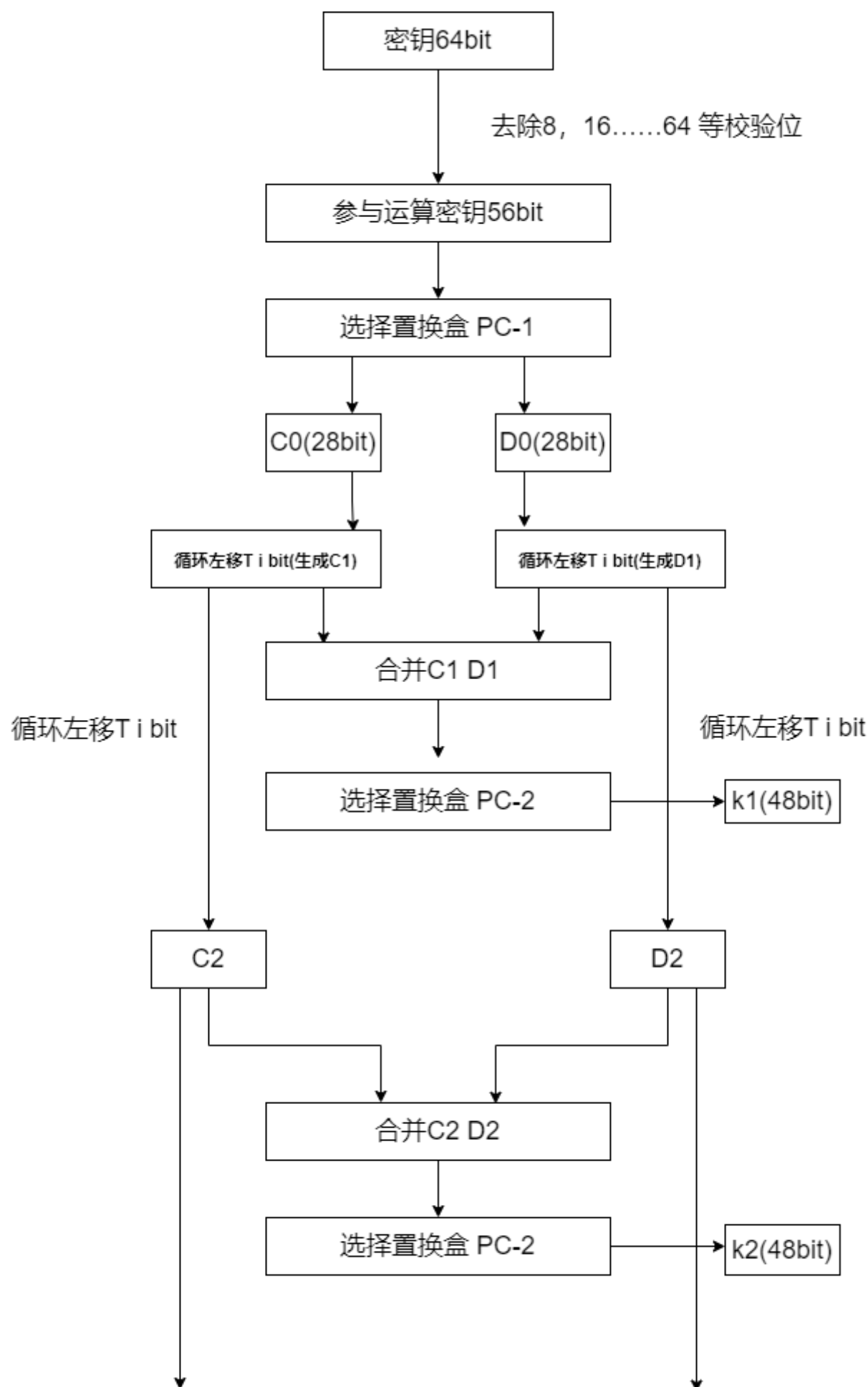
三大步：

- 1. 置换 (INITIAL PERMUTATIONS)：将明文的数据位置有规律的打乱
- 2. 16轮迭代
- 3. 置换：将迭代完成后得到的数据 根据 置换后得到密文

算法流程图：



子密钥的生成算法：



					每	轮	左	移	位	数	表					
轮(i)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数 (ti)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1