DES加密算法标准

2.1 分组长度：8-bit

2.2 密钥长度：10-bit

2.3 算法描述：

2.3.1 加密算法：[C=IP^{-1}(f\_{k\_{2}}(SW(f\_{k\_{1}}(IP(P)))))](" \l ")

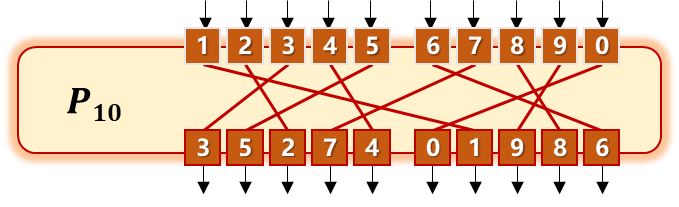
2.3.2 解密算法：[P=IP^{-1}(f\_{k\_{1}}(SW(f\_{k\_{2}}(IP(C)))))](" \l ")

2.3.3 密钥扩展：[k\_{i}=P\_{8}(Shift^{i}(P\_{10}(K))), (i=1,2)](" \l ")

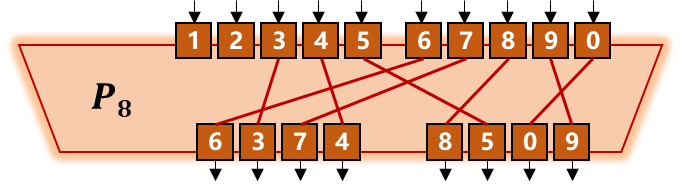
2.4 转换装置设定：

2.3.1 密钥扩展置

* [P\_{10}=(3,5,2,7,4,10,1,9,8,6)](" \l ")



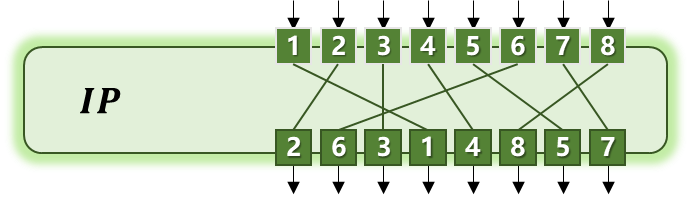
* [P\_{8}=(6,3,7,4,8,5,10,9)](" \l ")



* [Left\_Shift^1=(2,3,4,5,1)](" \l ")
* [Left\_Shift^2=(3,4,5,1,2)](" \l ")

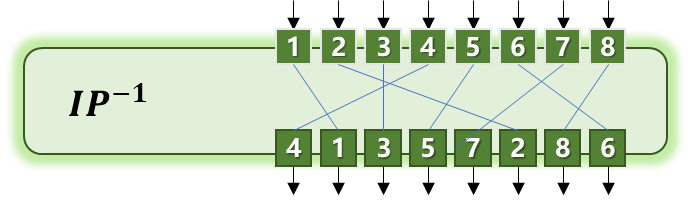
2.3.2 初始置换盒

* [IP=(2,6,3,1,4,8,5,7)](" \l ")



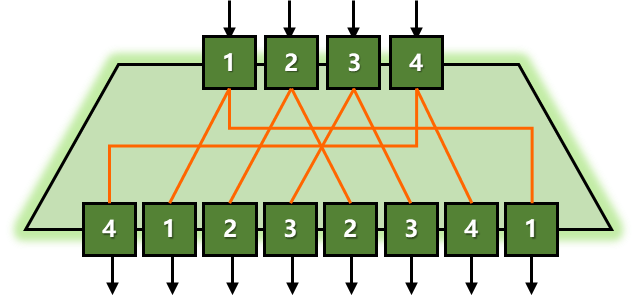
2.3.3 最终置换盒

* [IP^{-1}=(4,1,3,5,7,2,8,6)](" \l ")

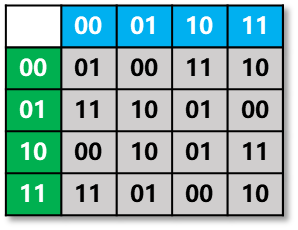


2.3.4 轮函数[F](" \l ")

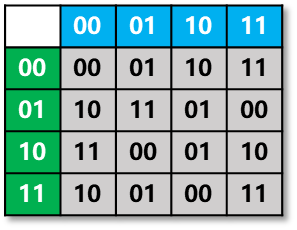
* [EPBox=(4,1,2,3,2,3,4,1)](" \l ")



* [SBox\_{1}=[(1,0,3,2);(3,2,1,0);(0,2,1,3);(3,1,0,2)]](" \l ")



* [SBox\_{2}=[(0,1,2,3);(2,3,1,0);(3,0,1,2);(2,1,0,3)]](" \l ")



* [SPBox=(2,4,3,1)](" \l ")

