DES实现文档

DES算法分析：

明文分组长为64比特，密钥长为56比特。如果加密的分组不足64比特，应当采取某种方式进行填充和补齐。需要根据初始密钥生成16个子密钥，分别对应于16次轮函数。

1. 初始置换

用于重排明文分组的64比特数据。

1. E拓展代换
2. S盒代换
3. 轮函数实现
4. 密钥生成

在本步骤中提供一个64位的初始密钥，通过密钥转化变成了56位。再将改56位密钥拆分成左右各28位，在每一轮中左移位相应的位数，再合并置换成为48位的轮密钥。

