lab2实验报告

DES算法基本流程

`开始` -> `初始置换` ->16次`轮函数变换` -> `逆初始变换` -> `结束`

初始置换(IP)

使用初始置换数组重排64bit的数据

轮函数(以第i+1轮为例)

对第i+1轮的`轮函数变换`,即`Li`和`Ri`转换成`Li+1`和`Ri+1`

首先,得到`Li+1` = `Ri`.

然后 ,得到密钥`Ki+1`.原64bit密钥经过`PC-1变换`生成56bit密钥,再依次经过`i+1`轮`左移位`和1轮`PC-2变换`得到`Ki+1`.

最后得到`Ri+1`. `Ri`经过`E拓展变换`生成48bit数据,与48bit密钥`Ki+1`异或运算,将其结果`S盒变换`成32bit数据,再经过`P变换`输出32位数据,再与`Li`做异或运算得到`Ri+1`.

自此,由`Li`和`Ri`经`轮函数变换`得到`Li+1`和`Ri+1`

逆初始置换

将经过16轮轮函数变换得到的密文,使用逆初始置换数组,重排64bit的数据.