

lab2实验报告

1811464 郑佶

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 L_i 和 R_i 转换成 L_{i+1} 和 R_{i+1}

首先,得到 $L_{i+1} = R_i$.

然后,得到密钥 K_{i+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 K_{i+1} .

最后得到 R_{i+1} . R_i 经过 E拓展变换 生成48bit数据,与48bit密钥 K_{i+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 L_i 做异或运算得到 R_{i+1} .

自此,由 L_i 和 R_i 经 轮函数变换 得到 L_{i+1} 和 R_{i+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.

代码实现简述

初始置换数组, 逆初始置换数组, E拓展变换数组, 轮函数变换中的 左移位数组, PC-1变换数组, PC-2变换数组, P盒, S盒,均存储于头文件 array.h .

初始置换, 逆初始置换, E拓展变换, 轮函数变换中的 左移位, PC-1变换, PC-2变换, P置换, S置换, 16进制字符与二进制字符的转换,均是通过类 DES 的成员函数实现,均存储于头文件 des.h ,且其引用头文件 array.h .

主程序的1,2,3分支分别实现 DES加密, DES解密, 雪崩效应测试 ,且其引用头文件 des.h .