# 《程序设计专题》实验报告 4

## 位运算与文件操作

## 1. 实验目的

通过实验：
1）掌握位运算
2）掌握二进制文件操作

## 2. 实验内容

1) 实现一个简单的数据解密程序。
2) 打包源代码和解密的结果为.zip 格式，上传至学在浙大，不需要写实验报告。上传的压缩文件命名为学号_姓名_HW4.zip。

## 3. 实验题目

实际中如果需要加密通信，一种方式是通信双方确认一个相同的密钥。消息发送方用密钥对消息的明文进行加密，生成密文发送给接收方；接收方采用相同的密钥解密后查看明文。

假设我们通信的密钥是整数 21，我加密了一张 jpg 格式的图片发送给你。请根据下面的简单加密算法实现相应的解密算法。

**加密算法：**

1. 对原始文件进行分块，每块大小为 8 字节 64 位；如果文件末尾不足 8 字节，则补 0。例如，文件大小对 8 取余为 1，则最后一块有效数据只有 1 字节，后面的 7 字节都设置为 0。
2. 对每一块数据，采用以下的方式置换其每一个二进制位，置换矩阵如下图所示：

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

假设一块数据的 64 位从 1~64 编号，以行优先方式对置换矩阵中的元素也编号为 1~64。则置换矩阵中的元素 x（编号为 i）意为，原数据块中的第 x 位应当被置换到新数据块中的第 i 位上。例如，对于第 2 行第 3 列的 44 来说，表示原数据块中的第 44 位应当被置换到新数据块的第 11 位上。上述置换操作可以得到一个新的数据块。

3. 对上述新数据块逐字节与密钥进行异或操作。
4. 每一个加密的数据块依次写入一个加密文件中。

**加密数据：**

原文件大小为 10155 字节，加密文件大小为 10160 字节（因为进行了补 0，解密时最后一个数据块需要截断 5 个字节）。

原文件类型为.jpg，因此解密后如果保存的扩展名不是.jpg，则修改为.jpg 后缀之后用图像编辑器查看是否成功解密。