实现功能：基于霍夫曼编码的无损压缩 简单加密算法

程序设计：

输入文件

是压缩文件？

有密码？

输入密码

用密码对加密部分进行异或解密

是

是

读取霍夫曼编码信息

对文件进行解码

否

统计文件中各字符出现的次数

否

生成霍夫曼树

生成霍夫曼编码

对文件进行编码

设置密码？

用密码对文件内容进行异或加密

输出结果文件

程序结束

是

否

文件格式设计：

|  |  |  |  |
| --- | --- | --- | --- |
| 非加密压缩文件 | | | |
|  | 属性 | 长度 | 说明 |
| 头部 | 标识 | 4字节 | 总是FF00FF00 |
| 补零个数 | 1字节 | 进行霍夫曼编码后不能保证是整数字节数，所以要进行补零。 |
| 编码字典大小 | 1字节 | 由于关键字最多256个，所以一个字节可以存储字典大小。由于字典大小不能为0，所以0代表256 |
| 编码字典字典 | 不定 | 字典格式：关键字1字节，长度1字节，霍夫曼编码不定长，不足整数字节部分补零 |
| 正文 | 编码正文 | 不定 | 霍夫曼编码后的内容。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 加密压缩文件 | | | |
|  | 属性 | 长度 | 说明 |
| 头部 | 标识 | 4字节 | 总是FF00FF01 |
| 密码校验 | 16字节 | 存储密码的MD5哈希值，用来验证密码输入是否正确。 |
| 补零个数 | 1字节 | 【异或加密】 |
| 编码字典大小 | 1字节 | 【异或加密】 |
| 编码字典字典 | 不定 | 【异或加密】 |
| 正文 | 编码正文 | 不定 | 【异或加密】 |