Project1 DES 算法实现

林士翰　15307130120

一、概述

用 C/C++实现了 16 轮迭代的 DES 加密解密算法，能够在 Linux 下编译后执行。

二、文件描述

DES.cpp, DES.h, Util.h：算法源码

DES：在 macOS 下编译得到的可执行文件

三、使用说明

1. 编译

在 Linux 或者 macOS 下使用 g++编译。

```
LSHs-MacBook-Pro:Project_DES lsh$ g++ DES.cpp -o DES
LSHs-MacBook-Pro:Project_DES lsh$
```

2. 运行

直接运行可执行文件会显示使用方法。

```
LSHs-MacBook-Pro:Project_DES lsh$ ./DES
Usage:
./DES -i input [-dko]

      -i input    Input path.
      -o output   Output path.
      -d          Decode mode.
      -k key      Key.

LSHs-MacBook-Pro:Project_DES lsh$
```

各个选项解释如下：

选项	解释	默认
-i	必选项，参数 input 为需要加/解密文件的路径	
-o	非必选，参数 output 为加/解密后的文件的路径	输出路径为当前文件夹 加密模式输出文件名为输入文件名加上.des 后缀 解密模式输出文件名为加密前的文件名
-d	非必选，使用解密模式	加密模式
-k	加密模式非必选，解密模式必选	加密模式下自动随机生成密钥并输出到终端

示例：

```
>>./DES -i a.in -k 1a2b3d4e
>>./DES -i a.in.des -d -k 1a2b3d4e
>>./DES -i b.in -o ~/Desktop/bbb.des -k abcdefgh
>>./DES -i ~/Desktop/bbb.des -d -k abcdefgh -o ./TEST/
```

四、加解密实验

1. 实验一

./TEST 下有一个“test.txt”文件，内容如下：

```
LSHs-MacBook-Pro:Project_DES lsh$ cat ./TEST/test.txt
Hello world!
This is DES algorithm!
LSHs-MacBook-Pro:Project_DES lsh$
```

对其加密，指定密钥为 12345678，输出到当前文件夹下。

```
LSHs-MacBook-Pro:Project_DES lsh$ ./DES -i TEST/test.txt -k 12345678
test.txt.des
Size: 36B

####################
#  Key: 12345678  #
####################
LSHs-MacBook-Pro:Project_DES lsh$
```

对得到的 test.txt.des 进行解密，在当前文件夹下得到原始文件。

```
LSHs-MacBook-Pro:Project_DES lsh$ ./DES -i test.txt.des -d -k 12345678
test.txt
Size: 36B

####################
#  Key: 12345678  #
####################
LSHs-MacBook-Pro:Project_DES lsh$ ls
DES             DES.h           Util.h          test.txt.des
DES.cpp         TEST            test.txt
LSHs-MacBook-Pro:Project_DES lsh$ cat test.txt
Hello world!
This is DES algorithm!
LSHs-MacBook-Pro:Project_DES lsh$
```

2. 实验二

~/Desktop/下有一个“测试.pdf”文件，如下：

对其加密，不指定密钥，输出到~/Desktop/abc.des(文件较大时需要较长时间)。

```
LSHs-MacBook-Pro:Project_DES lsh$ ./DES -i ~/Desktop/测试.pdf -o ~/Desktop/abc.des
/Users/lsh/Desktop/abc.des
Size: 1988959B

####################
#  Key: dKJBY96l  #
####################
LSHs-MacBook-Pro:Project_DES lsh$
```

得到密钥 dKJBY96l，使用它解密 abc.des，输出到./TEST 下。由于加密时记录了原始文件的文件名，解密未指定文件名时得到了原始文件名。

```
LSHs-MacBook-Pro:Project_DES lsh$ ./DES -i ~/Desktop/abc.des -o ./TEST/ -d -k dKJBY96l
./TEST/测试.pdf
Size: 1988959B

####################
#  Key: dKJBY96l  #
####################
LSHs-MacBook-Pro:Project_DES lsh$ ls ./TEST/
test.txt        测试.pdf
LSHs-MacBook-Pro:Project_DES lsh$
```

测试.pdf