Project2 RSA 算法实现

林士翰　15307130120

一、概述

用 C/C++实现了 128bits 的 RSA 算法，包括素数和密钥对生成。使用 RSA 算法加密 DES 密钥，用 DES 算法对传输内容进行加解密。能够在 Linux 下编译后执行。

二、文件描述

keygen.cpp：素数和密钥对生成源码
encrypt.cpp：使用 RSA 算法和公钥加密 DES 密钥，用 DES 算法对传输内容加密
decrypt.cpp：使用 RSA 算法和私钥解密 DES 密钥，用 DES 算法对传输内容解密
DES.cpp, DES.h：DES 算法源码
Integer.h, Prime.h, RSA.h, stdcpp.h, Util.h：算法其他细节的源码
public.key：公钥文件
private.key：私钥文件
DESKey.rsa：用 RSA 算法和公钥加密后的 DES 密钥
make.sh：用于编译的 shell 脚本

三、使用说明和实验

1. 编译

在 Linux 或者 macOS 下运行 make.sh 即可编译，生成 keygen, encrypt, decrypt 三个可执行文件。

```
LSHs-MacBook-Pro:RSA lsh$ ./make.sh
LSHs-MacBook-Pro:RSA lsh$
```

2. 密钥对生成

直接运行 keygen 可以在当前文件夹下生成密钥对文件，public.key 和 private.key。

```
LSHs-MacBook-Pro:RSA lsh$ ./keygen
LSHs-MacBook-Pro:RSA lsh$ ls *.key
private.key     public.key
LSHs-MacBook-Pro:RSA lsh$
```

3. 加密文件

运行 encrypt，并用-i 和-o 分别指明输入输出文件路径(-o 非必选，默认为当前文件夹)。运行后生成被加密后的文件，以及用公钥加密后的 DES 密钥文件 DESKey.rsa。

如下图所示，在~/Desktop/下有一个 test.pdf 文件，现在对其加密，并将加密后的文件放置在当前文件夹下。

```
LSHs-MacBook-Pro:RSA lsh$ ./encrypt -i ~/Desktop/test.pdf -o ./
./test.pdf.des
Size: 944918B
LSHs-MacBook-Pro:RSA lsh$ ls *.rsa *.des
DESKey.rsa      test.pdf.des
LSHs-MacBook-Pro:RSA lsh$
```

当前文件夹下出现了加密后的文件 test.pdf.des 和被加密后的 DES 密钥文件 DESKey.rsa。

4. 解密文件

运行 decrypt，并用-i 和-o 分别指明输入输出文件路径(-o 非必选，默认为当前文件夹)。运行后在终端显示 DES 密钥，并生成解密后的文件。

如下图所示，将之前加密的文件 test.pdf.des 解密，并将解密后的文件放置在当前文件夹下。

```
LSHs-MacBook-Pro:RSA lsh$ ./decrypt -i ./test.pdf.des
####################
#  Key: zt7jlY72  #
####################
test.pdf
Size: 944918B
LSHs-MacBook-Pro:RSA lsh$ ls *.pdf
test.pdf
LSHs-MacBook-Pro:RSA lsh$
```

终端显示了用私钥解密后得到的 DES 密钥，当前文件夹下出现了原文件 test.pdf。