Chapter 4

公钥密码

Exercise 5

用 GNU MP 库，实现 512 位 RSA 加解密算法。**此练习不需要写报告**。

例如:

密钥生成：rsacipher -keygen pkey skey

加密执行的命令: rsacipher -e 1.txt pkey c1

解密执行的命令: rsacipher -d c1 skey 2.txt

其中：pkey 是保存公钥的文件，skey 是保存私钥的文件，c1 是密文二进制文件，1.txt 是原文的 txt 文件，2.txt 是解密后原文文本文件。

项目参考初始仓库`https://gitee.com/buuer/rsacipher`

提交的仓库中，要将文件 plain_buu_intr.docx 进行加密，密文以二进制方式存储在 cipher.docx 中，同时将 cipher.docx[1]进行解密，解密后存为文件 decode.docx[2]。

说明

- 既然 pkey 和 skey 是命令参数，这就意味这存储公私要的文件名，你是可以自己定义的。
- 在公私钥文件中，存的不是一个数，而应该是两个数，所以存储格式你自己要明确，否则，读就是个问题。
- n 怎么确定?你可以参考`https://blog.csdn.net/chengqiuming/article/details/82725708`。
- 更完整、安全的方法，可以查阅 NIST 的 SP 800-56,FIPS 186-4 等系列标准。密钥产生是个很重要的问题，所以 NIST 对其有一系列的标准涉及到。
- 在所有密码算法实现中，随机数是一个非常重要的基础部件，GNU MP 库提供了大伪随机数产生的算法。

[1]此时文件已经不能被 Word 应用程序正常打卡。

[2]此时文件可以被 Word 应用程序正常打卡。

- 在实现此算法中，可以直接利用 GNU MP 库中已有的算法，比如用 GCD 进行互素判定、mpz_probab_prime_p 进行素性判断等。