# **课外实践三** RSA实验要求

1. **实验目标：** 要求实现RSA的密钥生成、数据加密和解密。
2. **实验要求**

1. 用C或C++语言完成程序。

2. 密钥生成包括随机生成两个大素数p,q，计算n=p×q和Φ(n)=(p-1)(q-1)，然后选择与Φ(n)互素且小于Φ(n)的整数e，计算d=e-1mod Φ(n)，最后得到公钥{e, n}和私钥{d, n}。要求p,q至少均大于1010, 将生成的整数p、q、n、e、d分别写入文件p.txt、q.txt、n.txt、e.txt、d.txt中。**注意**，所有整数都必须用16进制表示。必须将整数转化成字符串后再写入文件，例如素数p=6B1BCF(用16进制表示)，则写入文件的应是字符串"6B1BCF"而非整数6B1BCF。

3. 数据加密是指用私钥{*e, n*}对指定的明文进行加密。数据解密是指用公钥{d, n}对指定的明文进行解密。数据加密和解密有一组对应的**测试数据**，以便检查程序的正确性。要求以命令行的形式，指定明文文件、密钥文件的位置和名称以及加密完成后密文文件的位置和名称。加密时先分别从指定的明文文件、密钥文件中读取有关信息，然后进行加密，最后将密文写入指定的密文文件。注意，密文(一个整数)必须用16进制表示。必须将密文(一个整数)转化成字符串后再写入文件，例如密文c=154A6B(用16进制表示)，则写入文件的应是字符串"154A6B"而非整数154A6B。

4. 命令行的具体格式如下：

e3rsa -p plainfile -n nfile [-e efile] [-d dfile] -c cipherfile

参数：

-p plainfile 指定明文文件的位置和名称  
 -n nfile 指定存放整数n的文件的位置和名称  
 -e efile 在数据加密时，指定存放整数e的文件的位置和名称  
 -d dfile 在数据解密时，指定存放整数d的文件的位置和名称  
 -c cipherfile 指定密文文件的位置和名称

5. 不超过3人为一组，每组的明文内容由成员的学号与姓名组成rsa\_plain.txt，例如：

学号1-姓名1；学号2-姓名2； ……

如果一个分组不足64bit，低位补0。

6. 最终上交的文件，包括：

（1）电子版的实践报告：标题、学号、姓名、实验内容描述、实验环境描述、实验过程简述、实验结果(实验的正确性)、实验的收获和体会。

（2）程序源代码以及生成密钥时所产生的文件p.txt、q.txt、n.txt、e.txt、d.txt。要求由源代码能重新正确生成可执行代码。

**测试数据 （进行设计的正确性测试）：**

**明文：**(用16进制表示) 63727970746F677261706879 (明文文件如：rsa\_plain.txt)  
**公钥：**(用16进制表示，公钥文件如：rsa\_pubkey.txt)

*n* = 73299B42DBD959CDB3FB176BD1

*e* = 10001

**私钥：**(用16进制表示，私钥文件如：rsa\_prikey.txt)

*n* = 73299B42DBD959CDB3FB176BD1

*d* = 63C3264A0BF3A4FC0FF0940935

**密文：**(用16进制表示)

6326DC198AAE1DB64FDC32D440（密文文件如rsa\_ cipher.txt）

实验完成时间为两个星期，实验完成之后将所有文件压缩成一个ZIP包，发送至课程中心