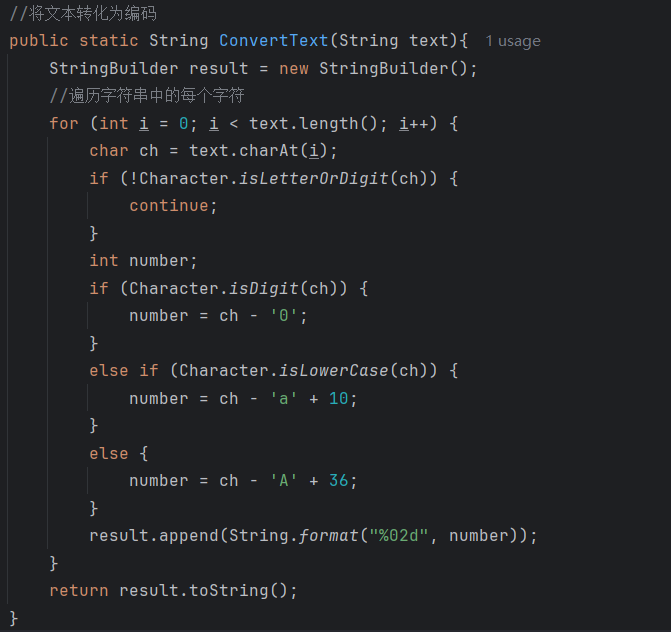
|  |
| --- |
| 哈尔滨工业大学（深圳） |
| **《密码学基础》实验报告** |
|  |
| RSA密码算法实验  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 黄宇浩 | | 学 号: | 220110415 | | 专 业: | 计算机科学与技术 | | 日 期: | 2023-10-xx | |

# 实验步骤

**请说明你的字符分组方式，以及关键的算法例如扩展欧几里德，素数检测，快速幂等函数的实现。**

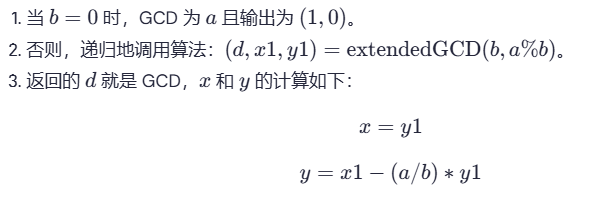
字符分组方式：每个字符对应一个编码数字，编码规则为：数字0-9对应00-09，小写字母𝑎-z对应10-35，大写字母𝐴-Z对应36-61），故一个字符对应两个十进制数。明文的一个分组块由4 个十进制数字组成，即两个字母。去掉空格和其他标点符号。

****代码截图：

扩展欧几里得算法：

输入a、b，输出x、y与GCD（a，b）

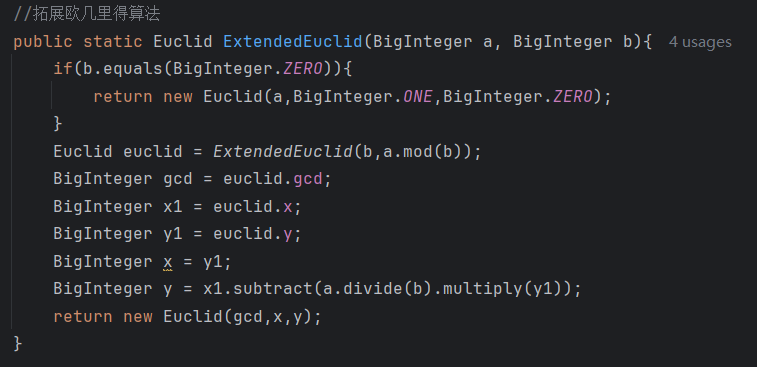
算法步骤：



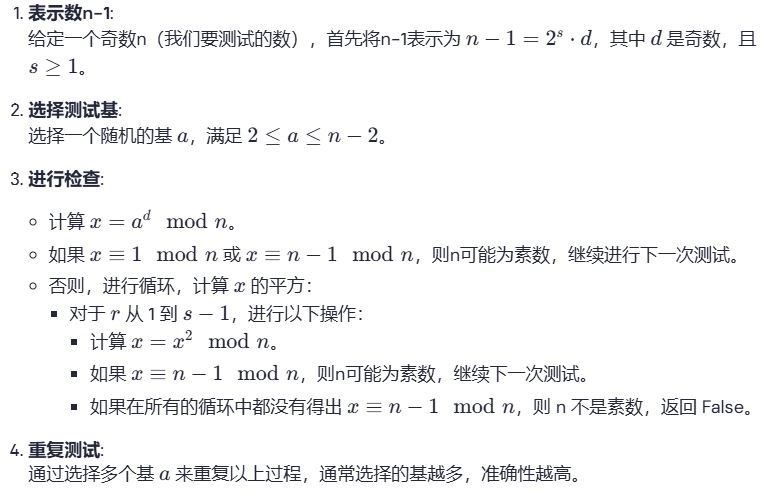
代码截图：

首先定义了一个欧几里得类：

然后是拓展欧几里得算法：

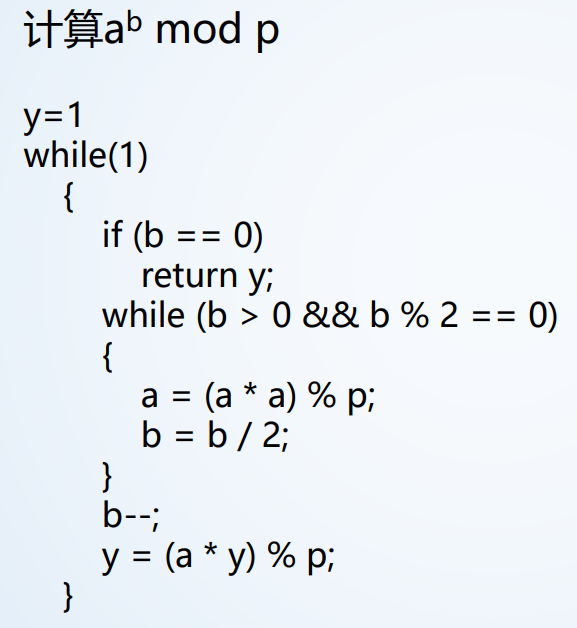
素数检测算法：Miller-Rabin算法

输入一个奇数n，判断其是否为素数

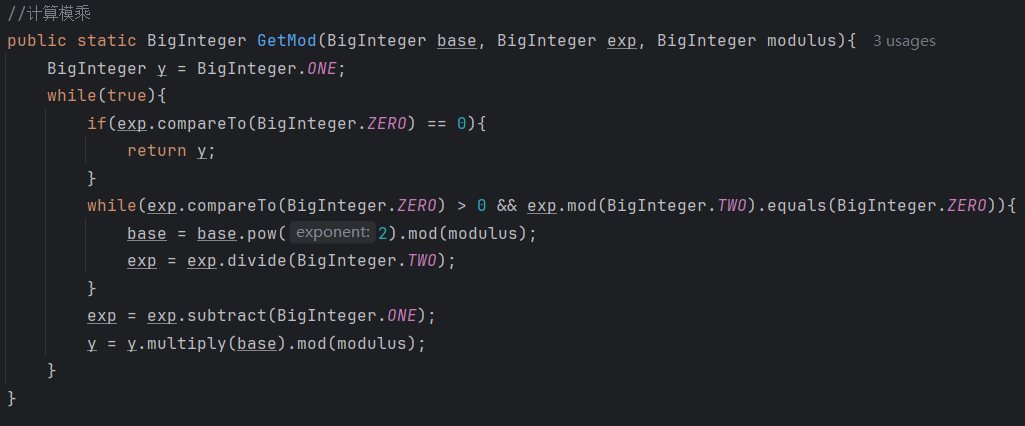
算法步骤：

在这次试验中，循环次数被设置为10次

代码截图：

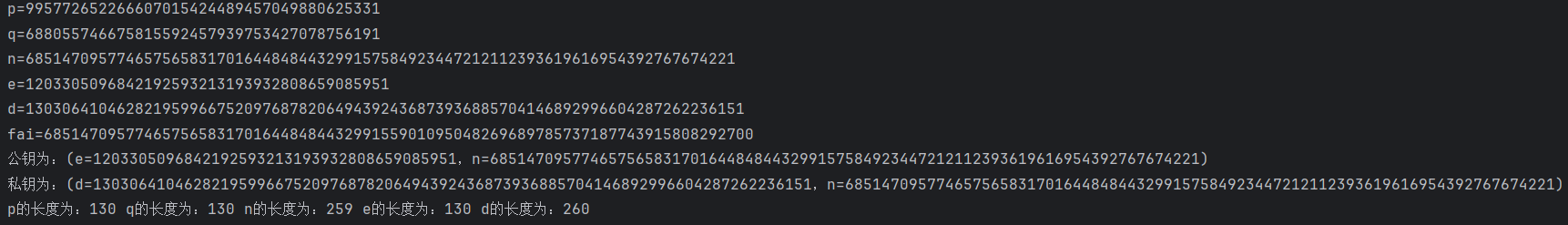
****快速幂函数算法：

代码截图：

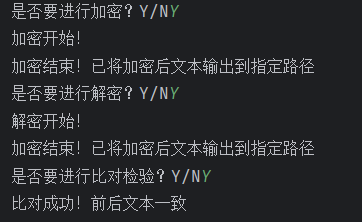


# 二、实验结果与分析

程序正确运行的结果截图，包括𝑝, 𝑞, 𝑛,𝑒, 𝑑,𝜙(𝑛)这些参数的值，可输出加密解密时间作为时长参考。

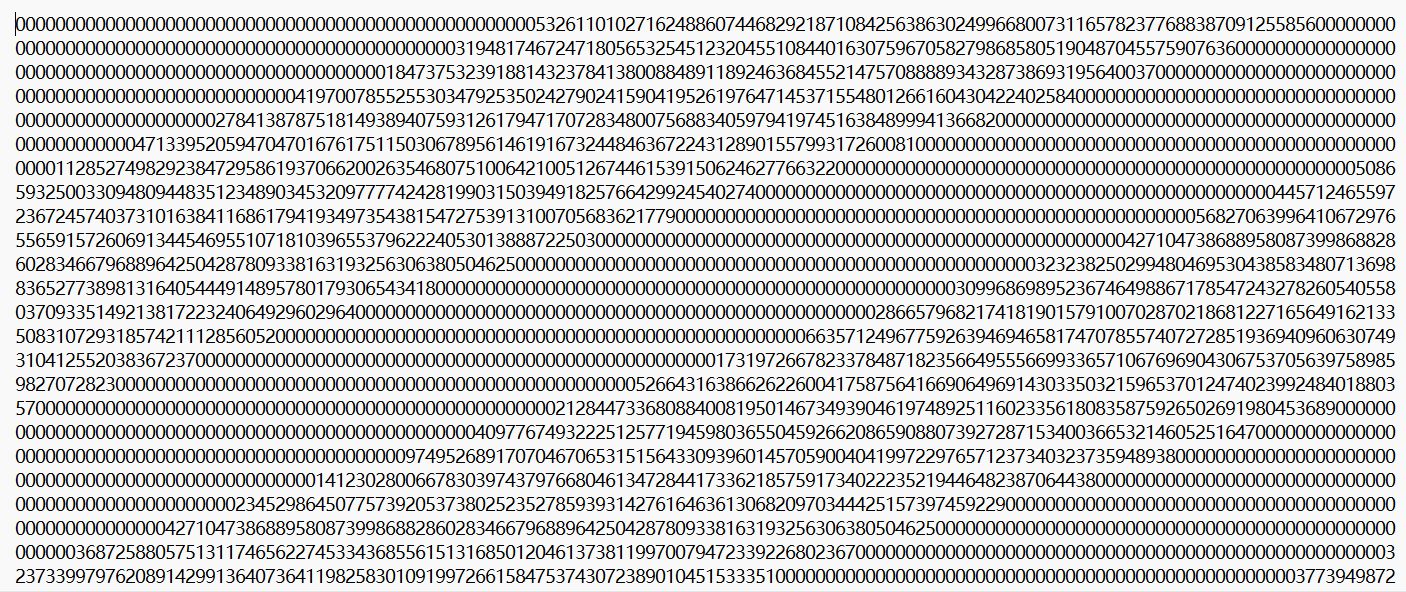


如图可以看到𝑝, 𝑞, 𝑛,𝑒, 𝑑,𝜙(𝑛)参数的值（其中fai为𝜙(𝑛)），并且进行长度检测，可以看到，它们都大于128位，这是因为设定了大素数的位数为130.

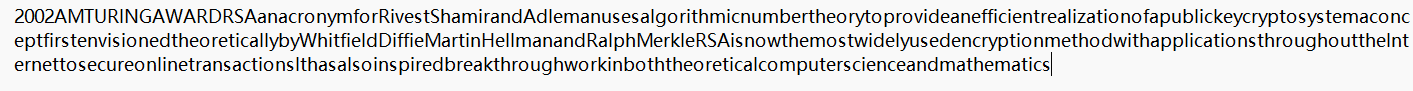


加密、解密均成功，且将密文解密后，其与最初的明文相同（比对成功）

密文截图(部分)：



解密后的明文截图：



可以看到，进行了正确的加密和解密

# 三、总结

1、实验过程中遇到的问题有哪些？你是怎么解决的？

遇到的问题：代码量太大，写了五六个小时。用到了新的数据结构BigInteger，有一些方法要自己查，包括算法的一些实现细节和理解。还遇到了一个栈溢出的错误，结果发现是递归调用出了问题。不过把算法理解清楚后，写起代码其实不算难。

2、关于本实验的意见或建议。

扩展欧几里得算法和Miller-Rabin算法可以给出伪代码，帮助更好地理解。也可以给一个代码框架，减少一些写代码的时间。