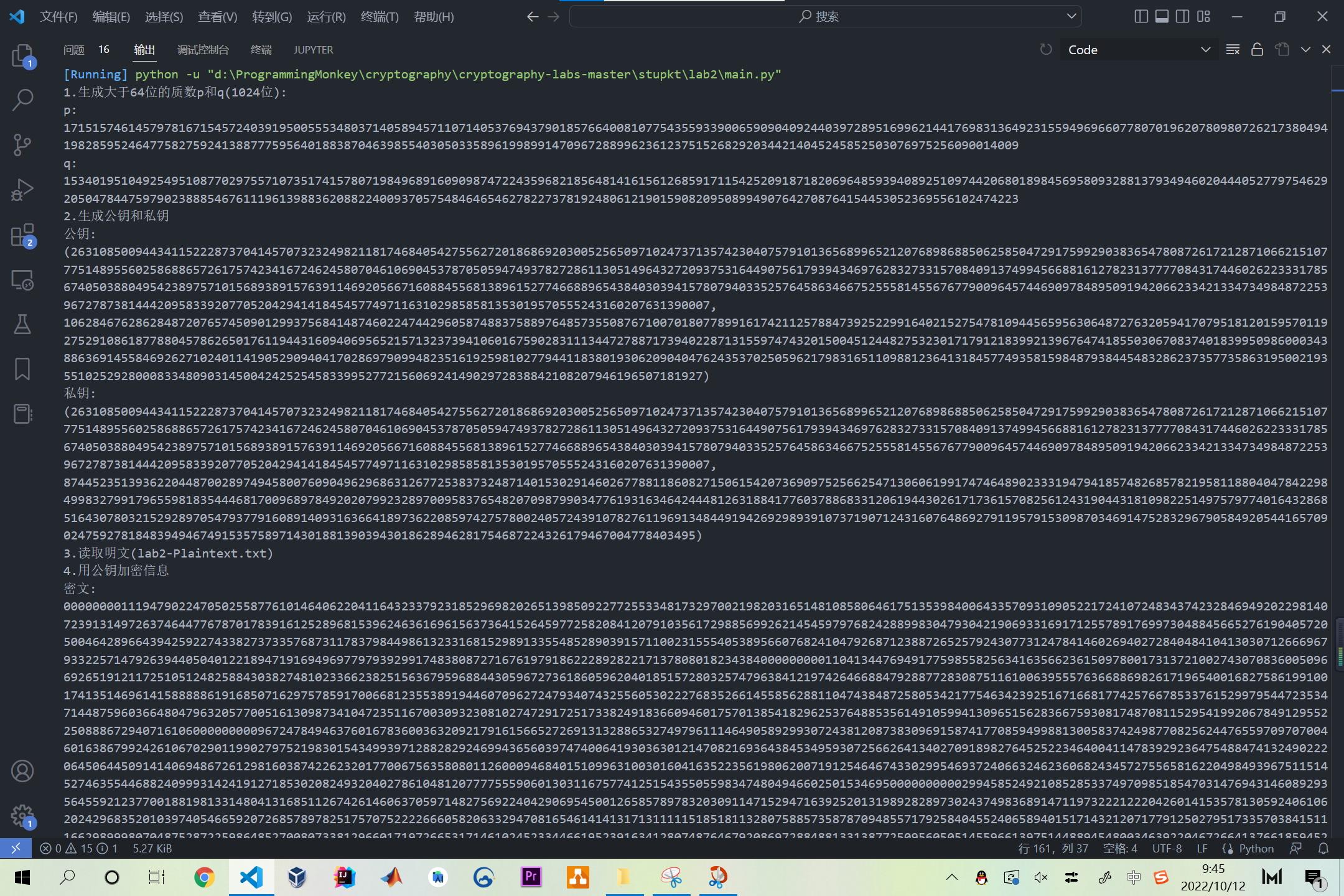
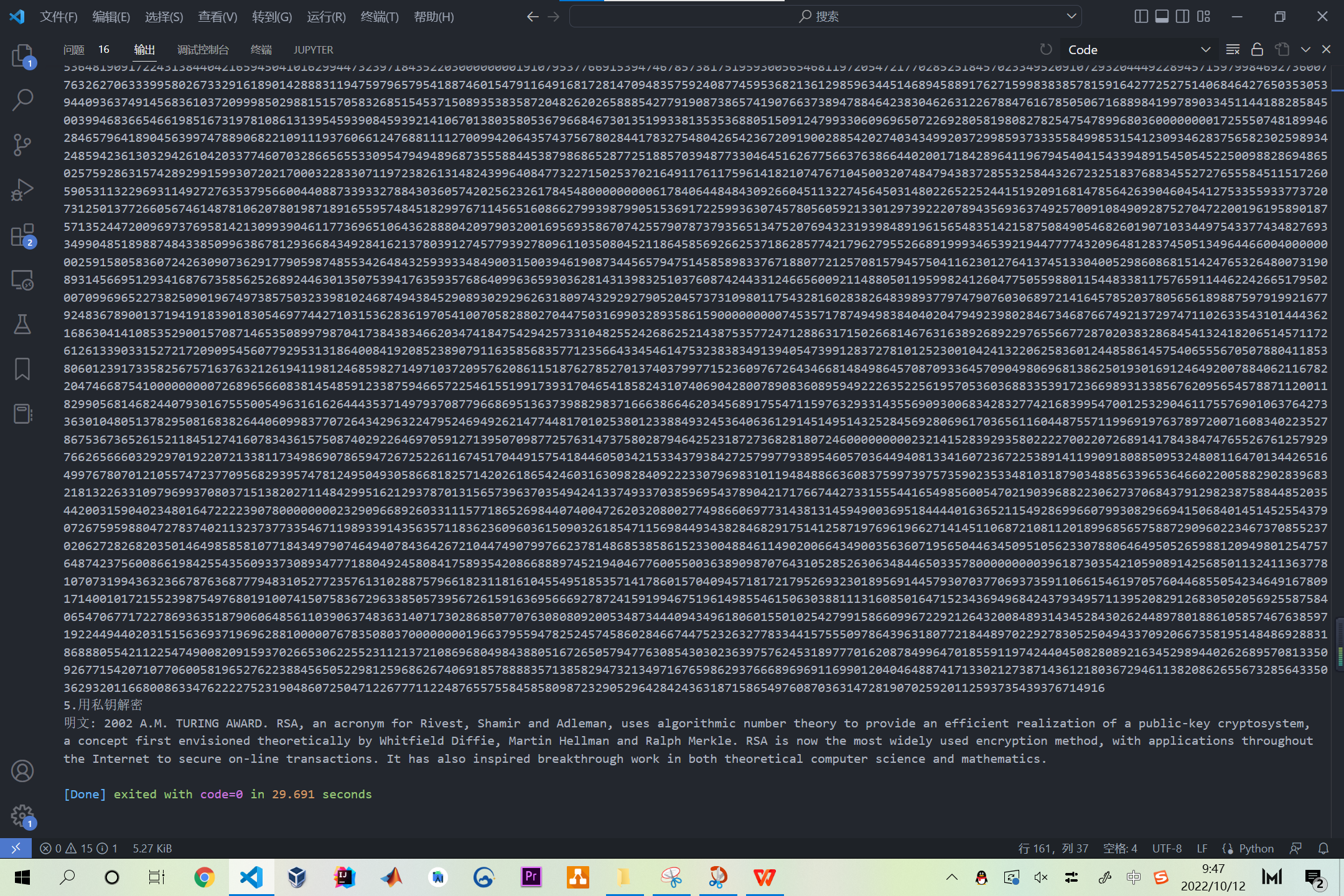
**实验2 RSA密码算法**

**姓名：\_\_\_\_\_张景昊\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_学号：\_\_\_200110631\_\_\_\_\_\_\_\_**

1. **运行截图**

**（秘文较长，此处未全部截图）**





1. **实验过程中遇到的问题有哪些？你是怎么解决的。**

*处理十进制数时由于不细致而出错；对密文分组的长度处理出现错误：*

*仔细思考阅读得到正确的处理方式*

*产生大素数的算法的实现细节出现问题：查阅相关资料后得到解决*

1. **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。**

*字符分组方式：加密时每4个十进制字符位为1组，若存在位数不足则补足4位，这个过程中进行相关标记，解密时需删除补位数*

*扩展欧几里得算法：形参为（a,b）；若b在mod a下有乘法逆，则返回b的逆元；否则递归调用，形参改为（a,a%b）。*

*素数检测算法（Miller-Rabin算法的Test算法）：形参为两个数k,q，其中k>0且q为奇数，满足（n-1 = 2^k \* q）。随机选取0到n-1范围内的整数a，如果a^q mod n = 1 或 n-1，返回肯定结果，即为素数；对于变量i在1到k-1循环，如果*

*a^(2^j\*q)mod n = n-1， 返回肯定结果，即为素数；若以上两个条件均不满足，返回错误结果，即不是素数。*