

**密码学及应用**

实 验 报 告

**学生姓名**

**学 号**

**专业班级**

**指导教师**

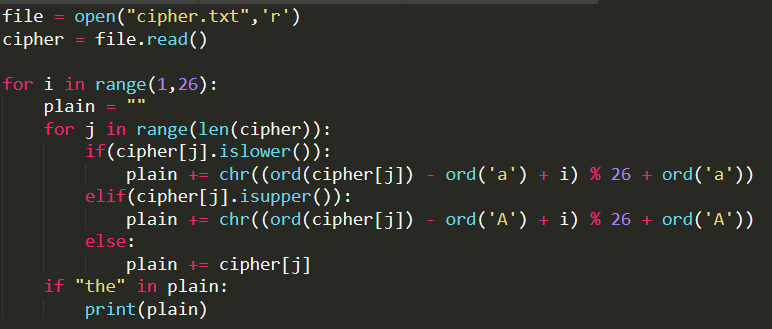
**学 院** 计算机学院

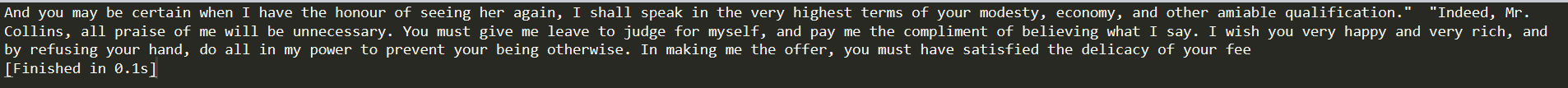
**完成时间** 2020年10月~2021年1月

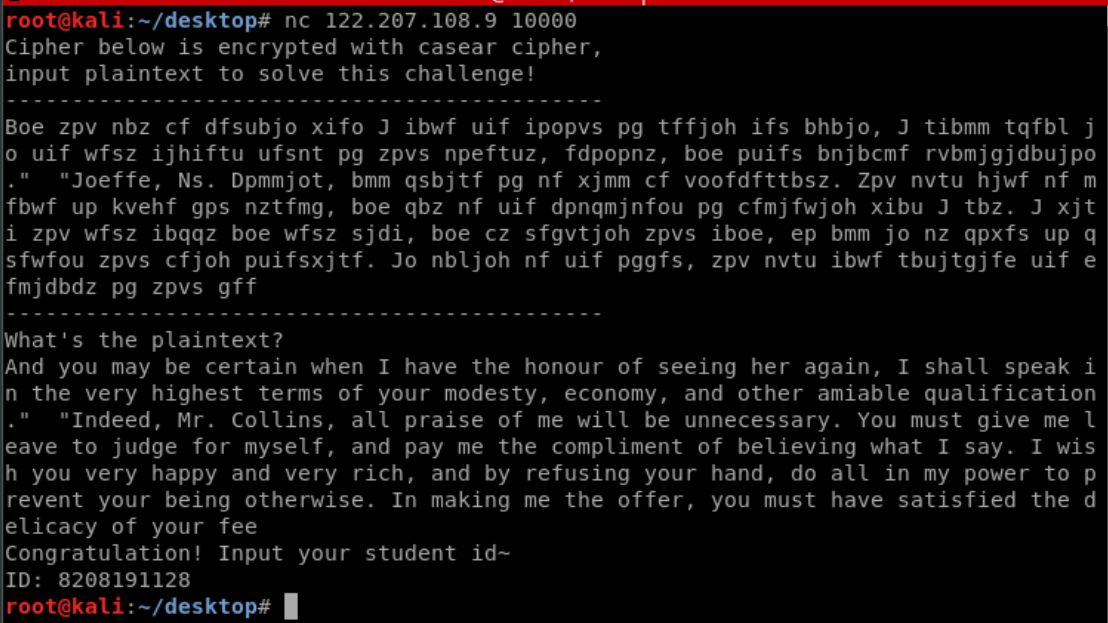
## 古典密码

1. **移位密码**

攻击方法：对26位字母进行爆破即可。

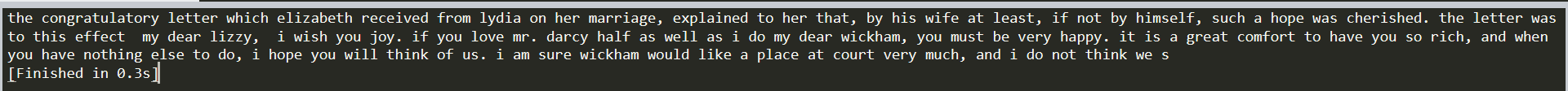


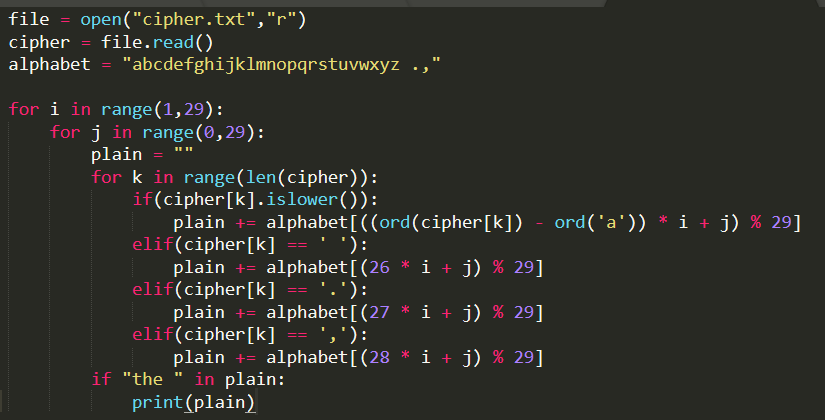


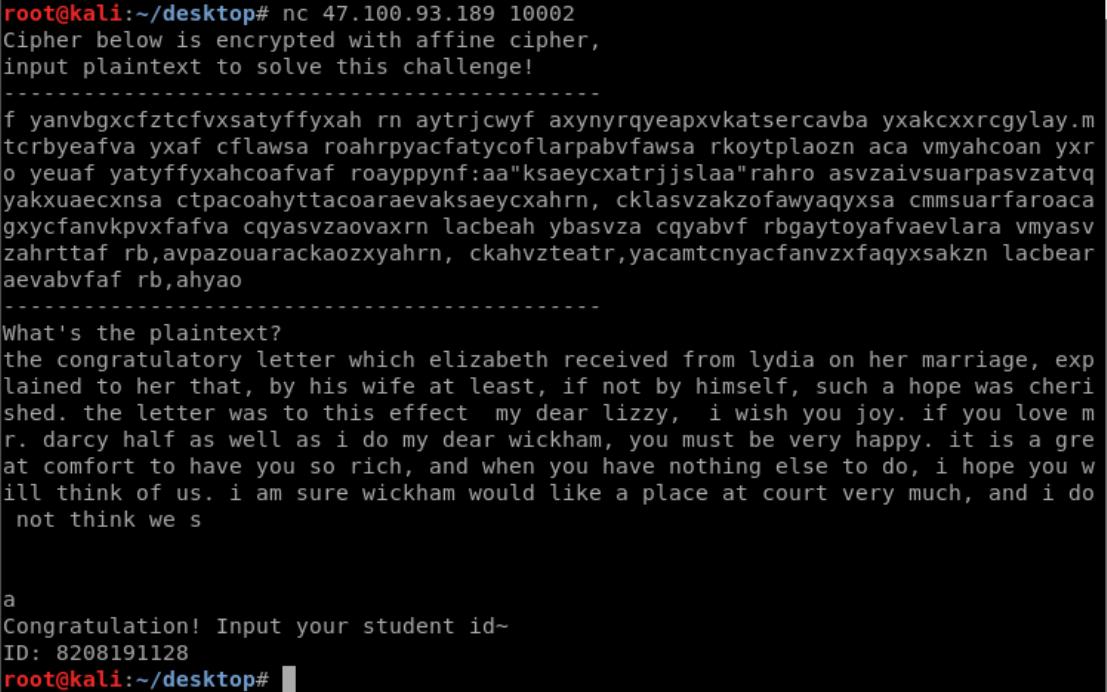


1. **仿射密码**

攻击方法：同casear密码，爆破乘数a和位移数b。

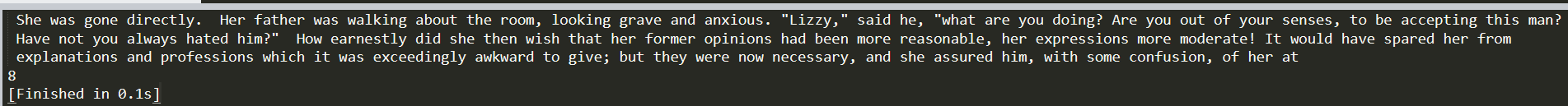


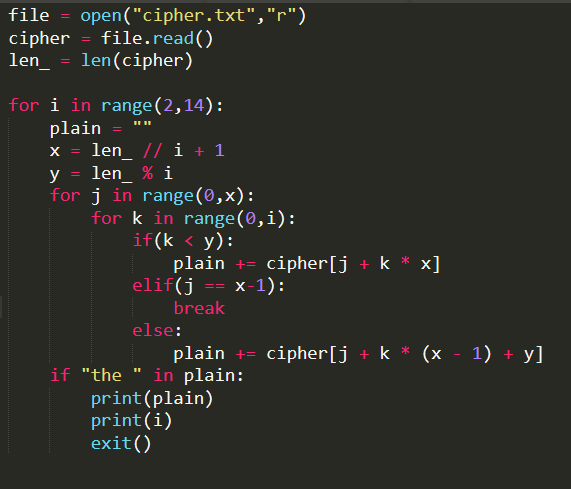


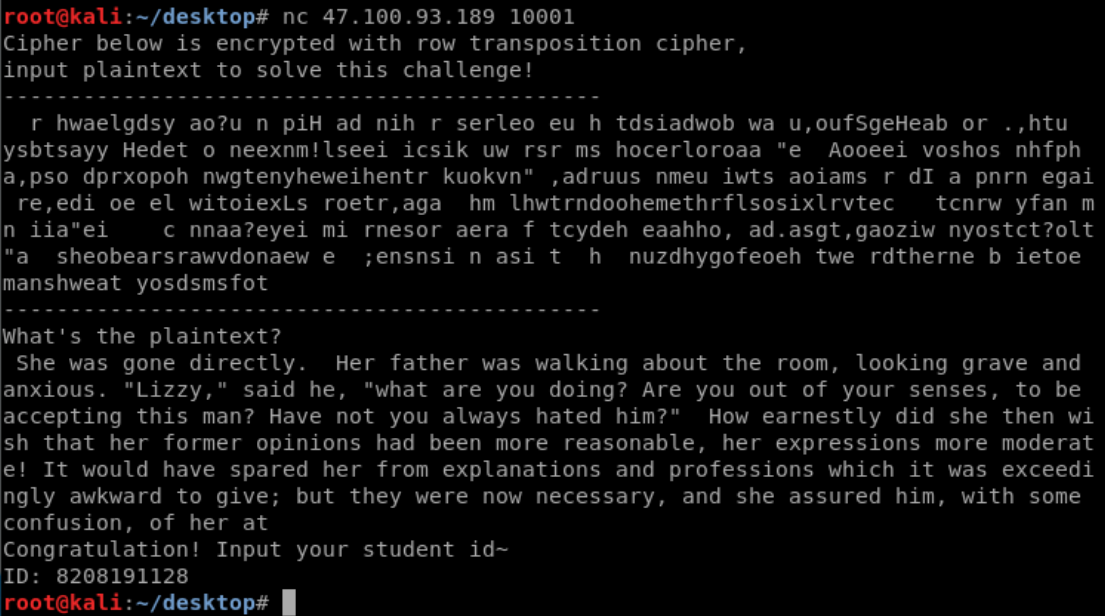


1. **列换位密码**

攻击方法：枚举列数r，对密文进行重新排列。



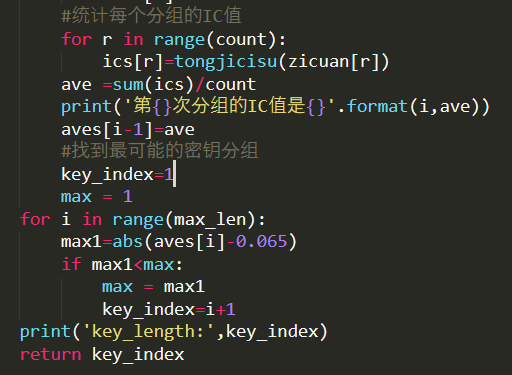


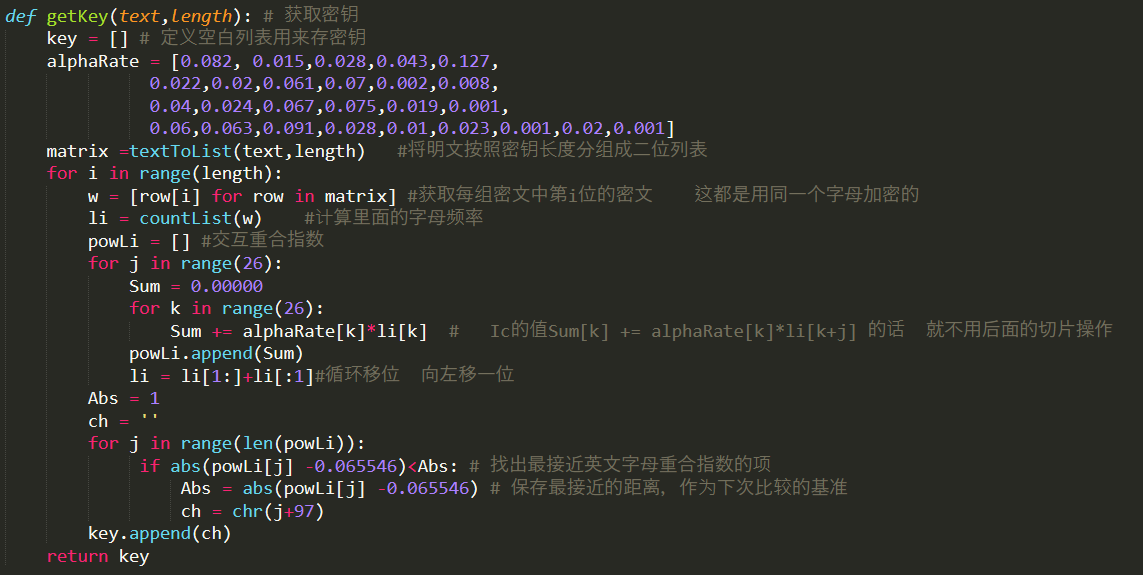


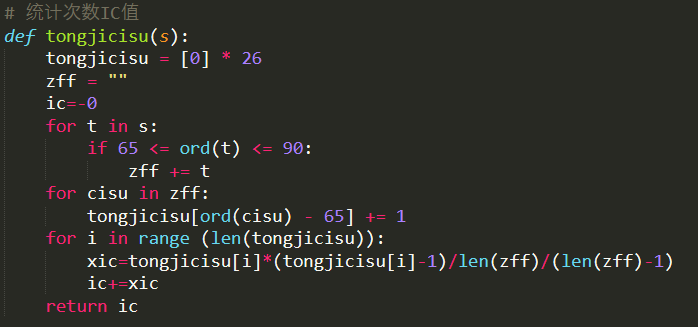
1. **（二选一）维吉尼亚密码**

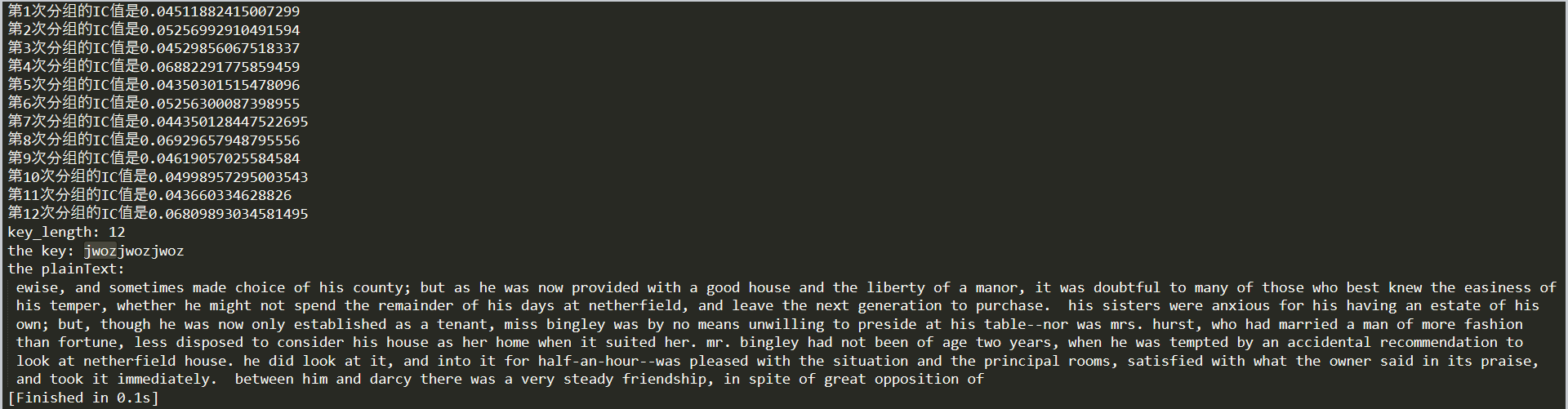
**攻击原理：**

* **密钥长度：**枚举密钥长度，根据密钥长度，统计各密钥长度下的字母频率，比较平均值最靠近0.065的即为正确密钥长度。
* **密钥：**首先获得未加密文本的字母频率表，对每一组子串进行移位，得到最靠近原始字母频率表的即为正确的位移长度。
* **明文：**利用所得密钥对密文进行位移操作。







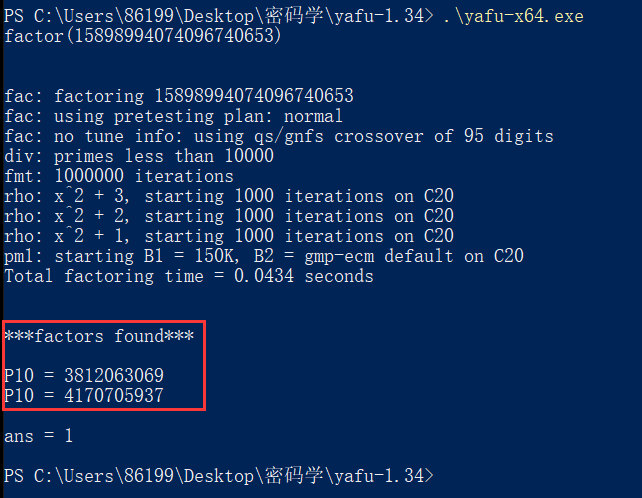


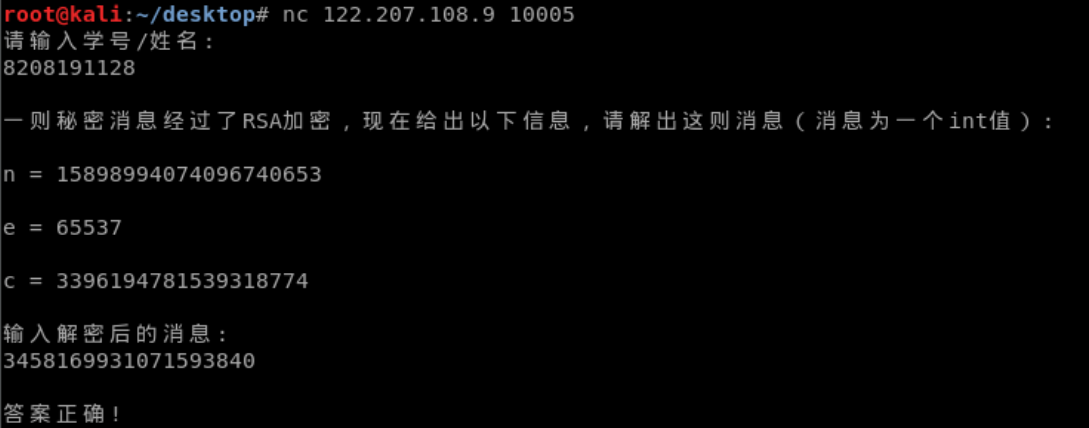


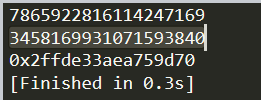
## 现代密码学

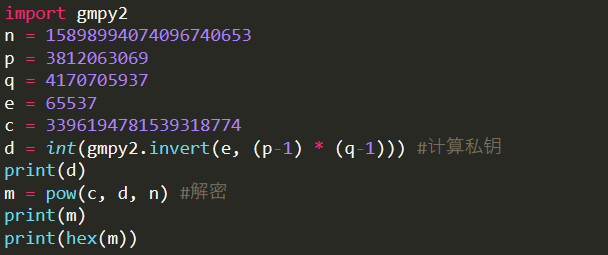
1. **因数分解攻击**

攻击方法：当n比较小时，可以使用工具（yafu）进行因数分解得到p,q。





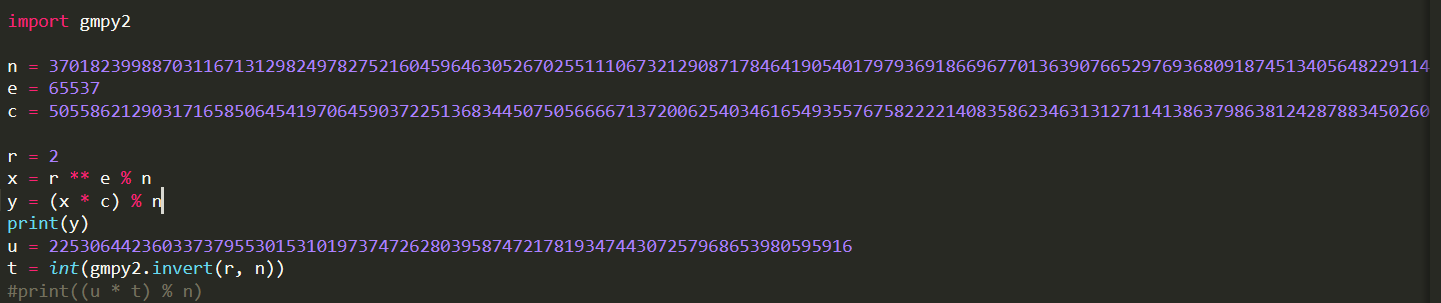


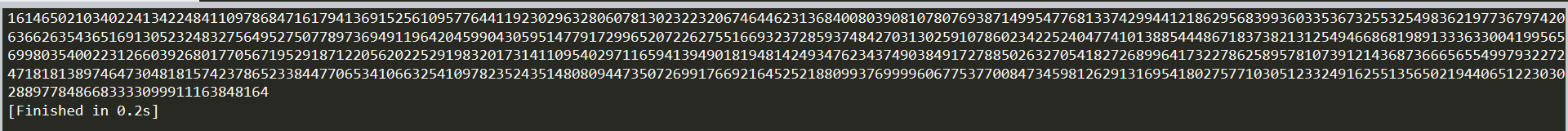


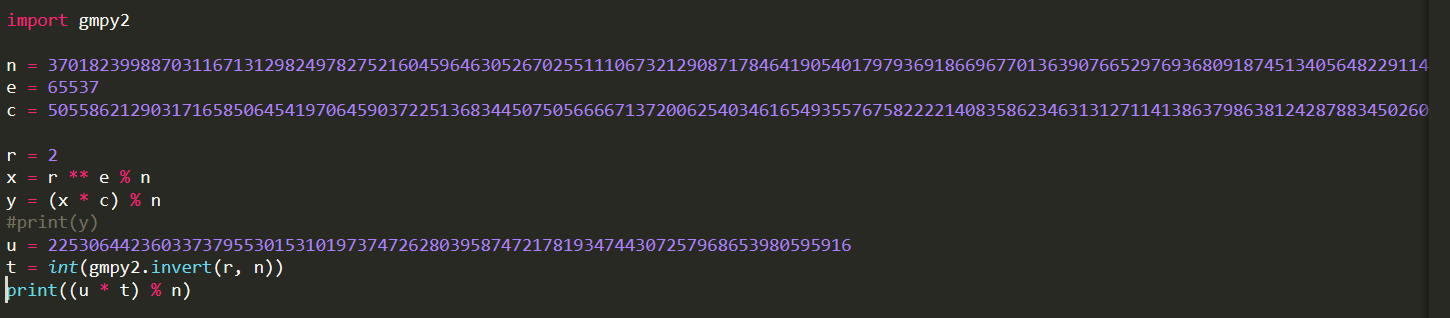
1. **选择密文攻击**

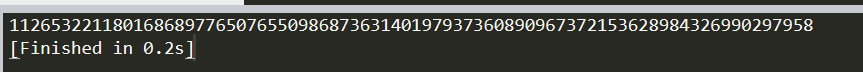
**攻击方法：**构造y = ( 2 \*\* e \* c ) % n ,签名后得u = 2 \*\* ( e \* d ) \* c \*\* d % n ,

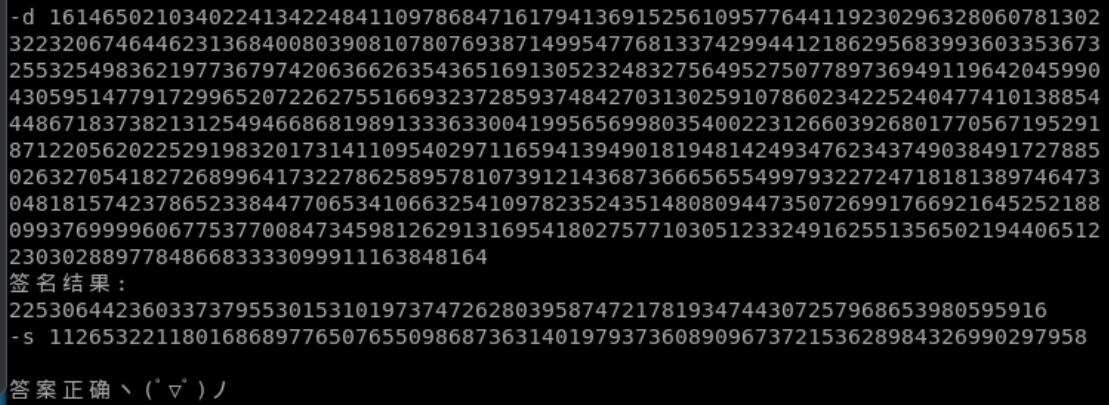
即 u = 2 \* m % n ,即可得到m。





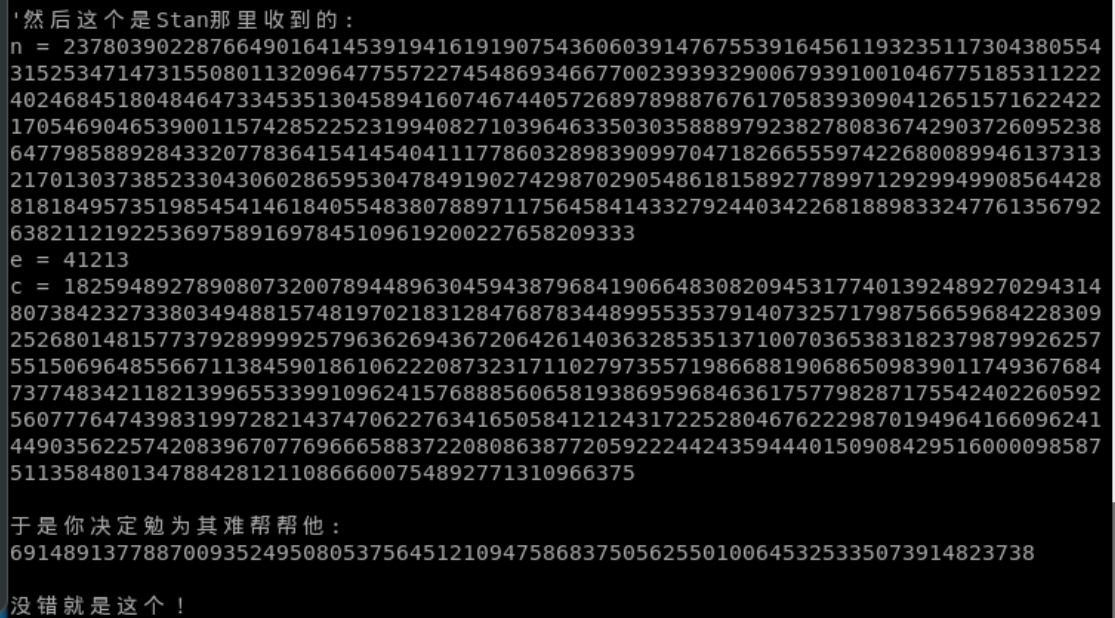


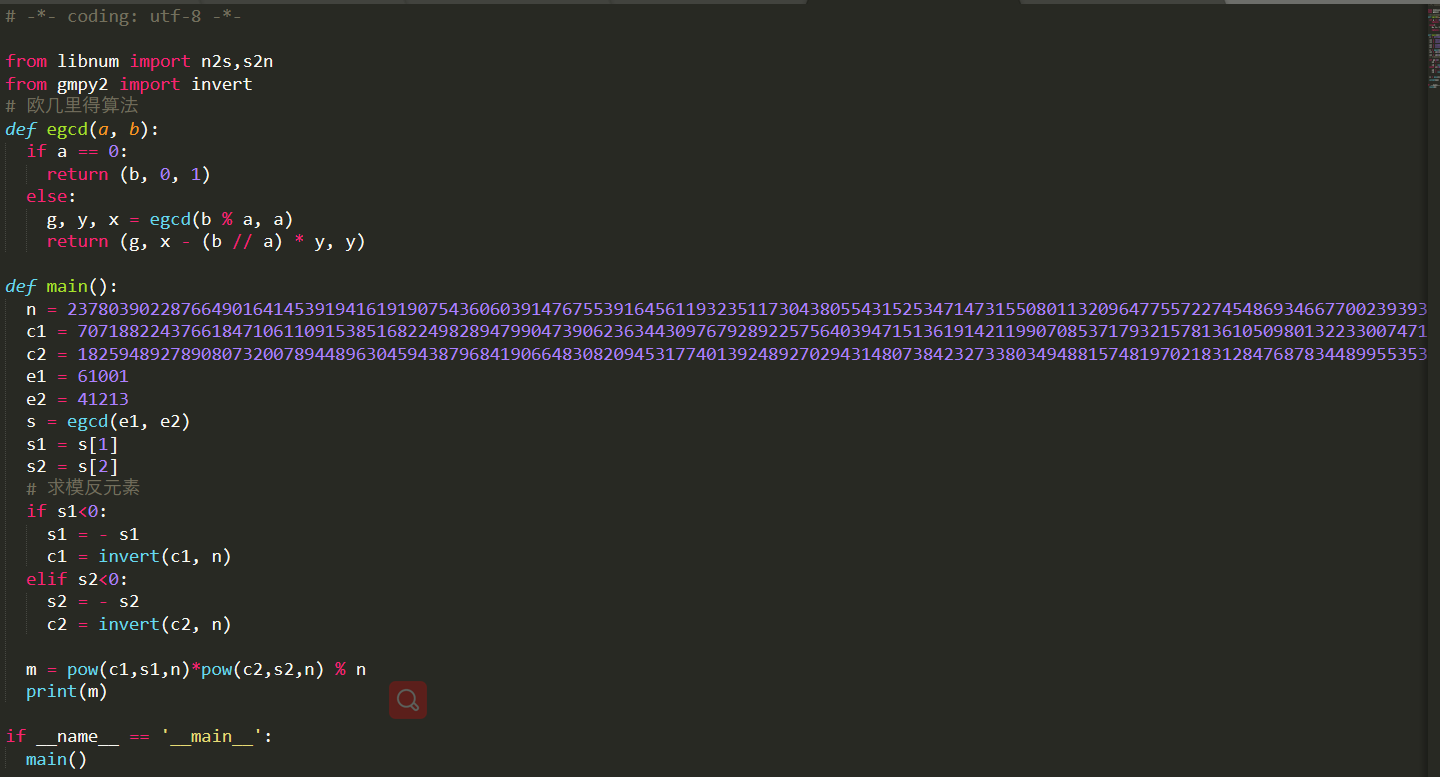


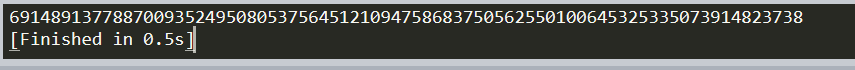


1. **共用模数攻击**

**攻击原理：**c1 = m \*\* e1 % n , c2 = m \*\* e2 % n , 存在s1 , s2使e1 \*s1 + e2 \*s2 = 1 % n , 即c1 \*\* s1 \* c2 \*\* s2 = m \*\* ( e1 \*s1 + e2 \*s2 ) = m % n。







1. **（二选一）低加密指数广播攻击**

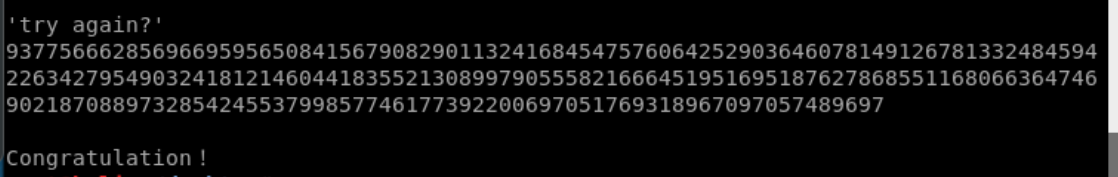
**攻击原理：由于e（=3）相同而且很小，则**

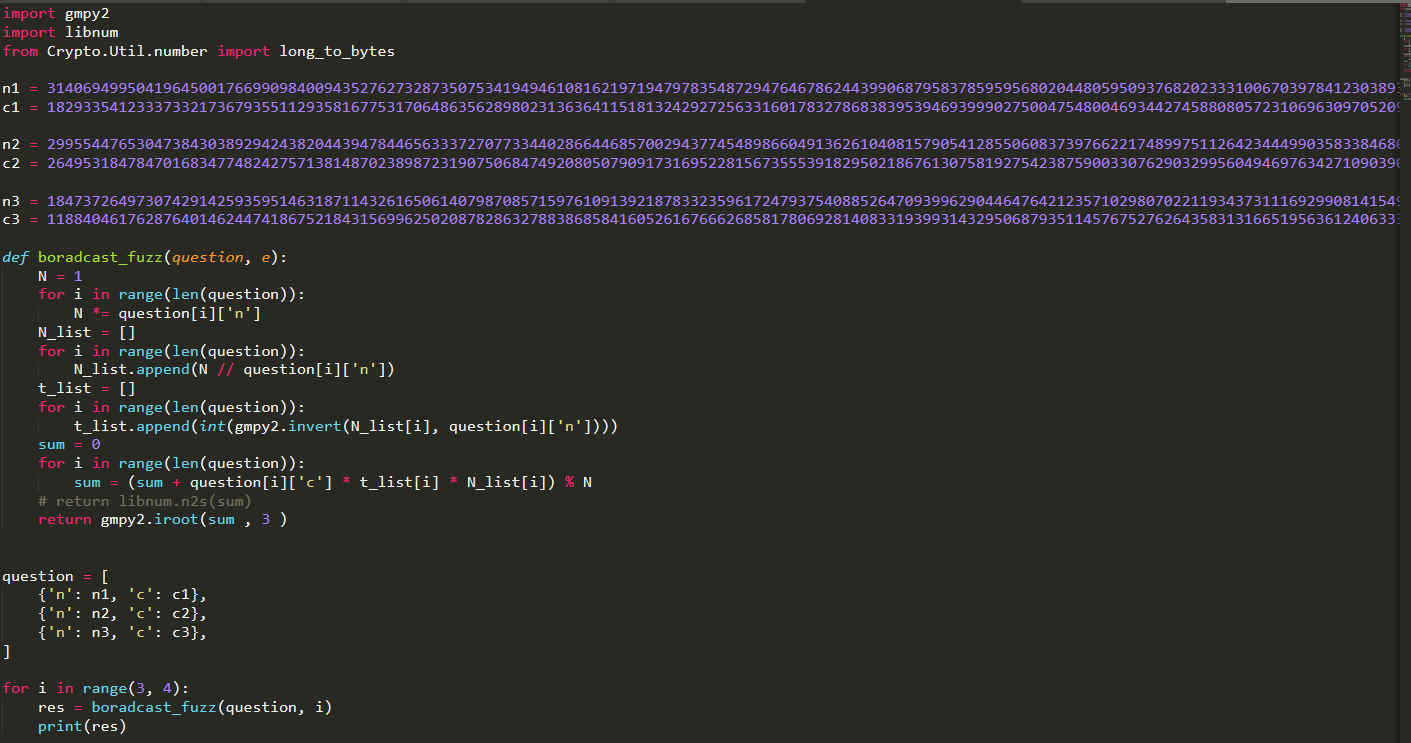
**c1 = m \*\* 3 % n1**

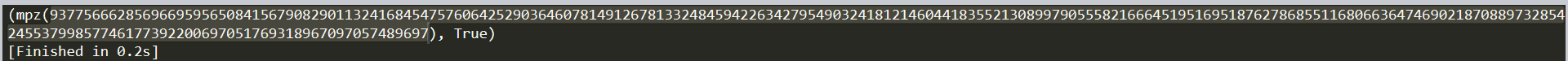
**c2 = m \*\* 3 % n2**

**c3 = m \*\* 3 % n3**

**使用中国剩余定理，可得 m \*\* 3 = c % N ,对c开方即可得到m。**







## 安全协议

1. **门限方案**

操作方法同低加密指数广播攻击，利用中国剩余定理即可得到m，由于本题为（5，3）门限方案，对三组消息进行处理即可。

