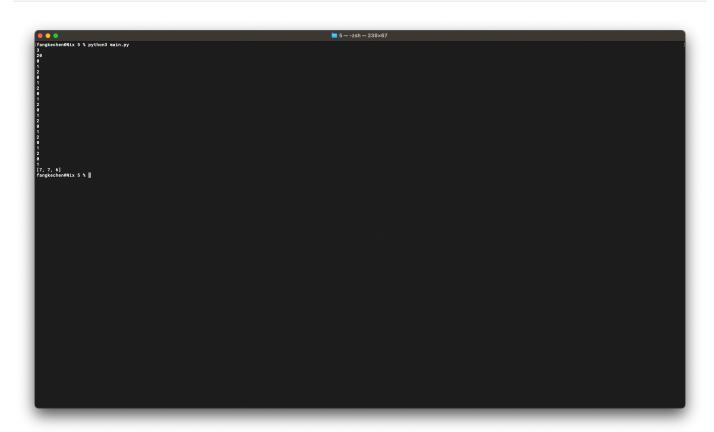
Exp5 同态加密匿名投票

实验步骤

- 1. 在主程序代码 main.py 中,首先实现了Paillier算法。其中 generate 函数用于生成公钥和私钥。 encode 用来对明文进行加密, decode 用于对密文进行解密。
- 2. 参考书中匿名电子投票的过程,代码中实现了三个类: Voter, Tally, Show 分别表示投票方、计票方和公布方。其中,私钥只有在公布方处拥有。在电子投票过程中,投票方首先使用公钥将其对每个候选者的投票数进行加密,并返回加密后的结果。计票方得到所有投票方的结果,然后对于每一位候选者,将所有投票方对其加密后的投票进行相乘,全部运算结束后返回每个候选者的加密投票结果。公布方获得计票方的结果后,使用私钥将其解密。
- 3. 在实现中,需要依次每行输入候选者人数、投票方人数。然后对于每位投票方每行输入投给的候选者编号(从 0 开始计),最终代码会输出计票结果。
- 4. 代码运行方式: 直接在命令行运行 python main.py 即可。

实验现象



在该次测试中,共有 3 位候选者, 20 位投票方且依次投给 $0,1,2,\cdots$ 号候选者,可以发现三位候选者的票数应当分别为 7,7,6 票。程序最终的输出结果符合预期。