《数据安全》实验报告

姓名：管昀玫 学号：2013750 班级：计科一班

**实验名称：**

秘密共享实践

**实验要求：**

实验 3.2 假设有三个同学需要对班里的优秀干部 Alice、Bob、Charles、Douglas 进行投票，最后统计各个班干部获得的票数。这个时候就可以利用 Shamir 秘密共享将各个投票方的投票分享出去并进行隐私求和计算。

借鉴实验3.2，实现三个人对于他们拥有的数据的平均值的计算。

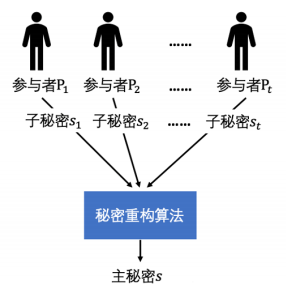
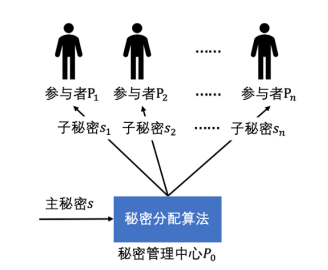
**实验过程：**

1. 门限秘密共享

门限秘密共享（Threshold Secret Sharing）是一种密码学技术，可以将秘密分割成多个部分，并将这些部分分配给不同的参与者，从而保护秘密免受单点故障和恶意攻击。

在门限秘密共享中，将秘密分成 n 个部分，其中只要 k 个部分被收集，就可以重构出原始秘密。这个 k 值称为“门限”，通常满足 k ≤ n，以确保秘密不被泄露。只有在收集到至少 k 个部分时，才能重构出秘密，因此，即使一些部分被泄露或丢失，也可以保持秘密的安全性。

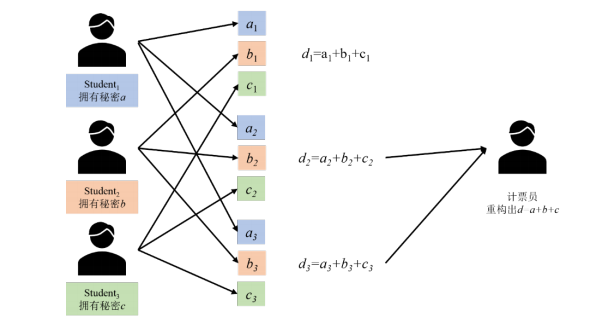
门限秘密共享可以用于许多场景，例如：多方拥有的敏感信息（例如金融账户密码）、公共密钥基础设施、加密密钥管理等等。



1. 投票统计

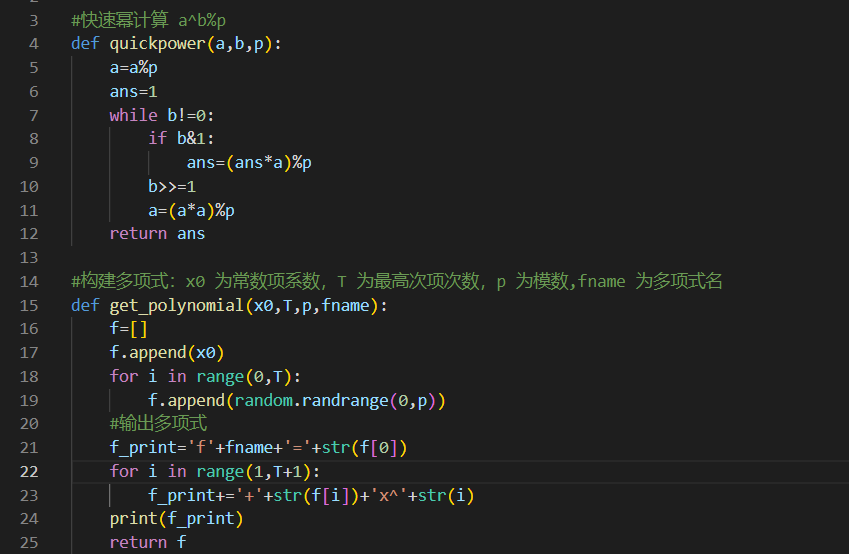
首先，要基于 Shamir 门限秘密共享进行协议设计。

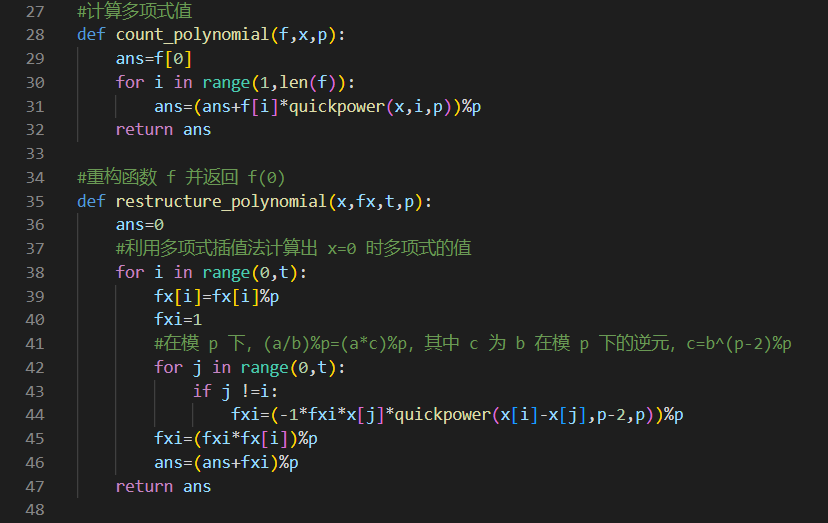
以计算 Alice 的票数为例，三个同学的隐私输入为 0 或 1，0 表示不投票给 Alice，1 表示投票给 Alice。假设三个同学 Student1、Student2 和 Student3 分别拥有隐私输入 a、b 和 c，他们将各自的隐私输入通过(2,3)门限的 Shamir 秘密共享分享给另外两个同学：Student1 获得a、b 和 c 的秘密份额 a1、b1 和 c1；Student2 获得秘密份额 a2、b2 和 c2；Student3 获得秘密份额 a3、b3和 c3。之后，三位同学各自将获得的秘密份额相加，分别得到 d1=a1+b1+c1，d2=a2+b2+c2和 d3=a3+b3+c3。一个计票员从三个同学中任选两个，例如 Student2和 Student3，获得他们拥有的 d2 和 d3，就可以重构出 d=a+b+c，也就是 Alice 获得的票数总和。具体过程如下图所示。



**① ss\_function.py**

这个文件包含了常用函数，如快速幂计算 a^b%p、构建多项式、计算多项式值、重构函数f并返回f(0)。

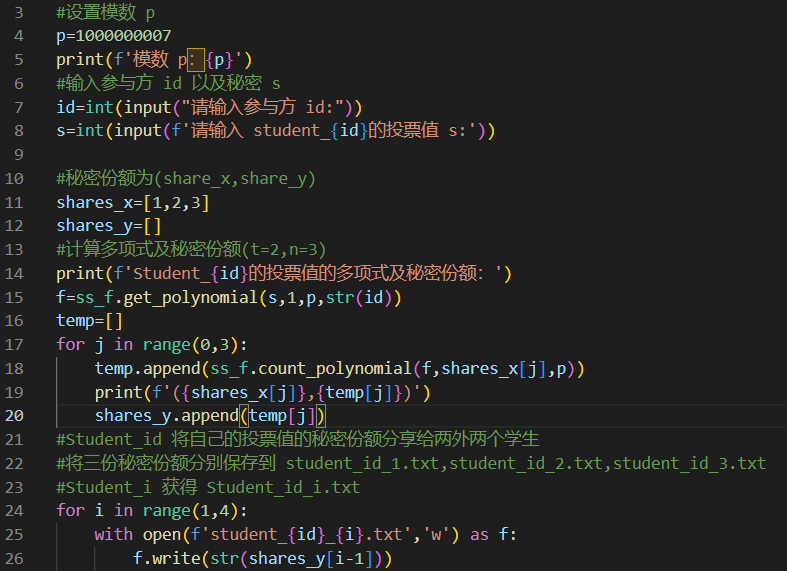




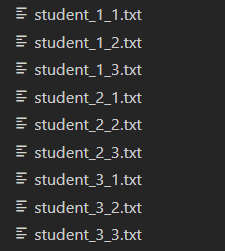
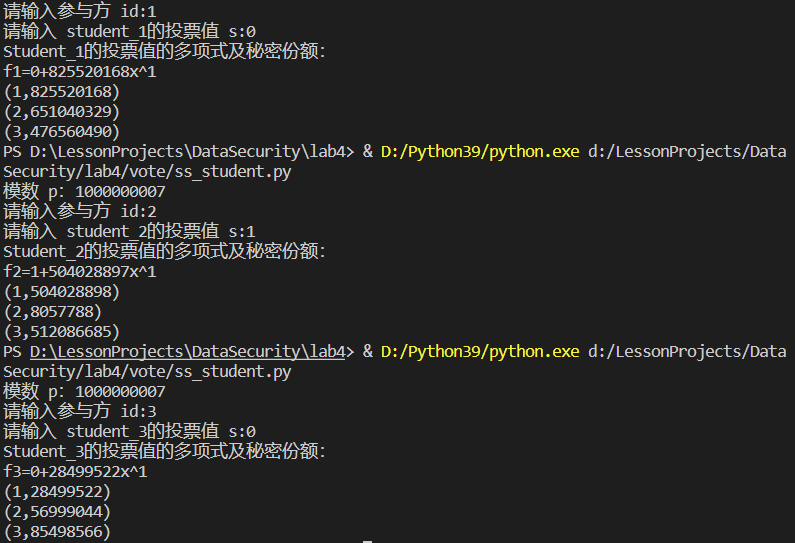
**② ss\_student.py**

这个文件输入了输入参与方 id 以及秘密 s，构造秘密份额，计算多项式及秘密份额(t=2,n=3)，之后每个学生将自己的投票值的秘密份额分享给两外两个学生，将三份秘密份额分别保存到 student\_id\_1.txt,student\_id\_2.txt,student\_id\_3.txt。

Student\_i 获得 Student\_id\_i.txt

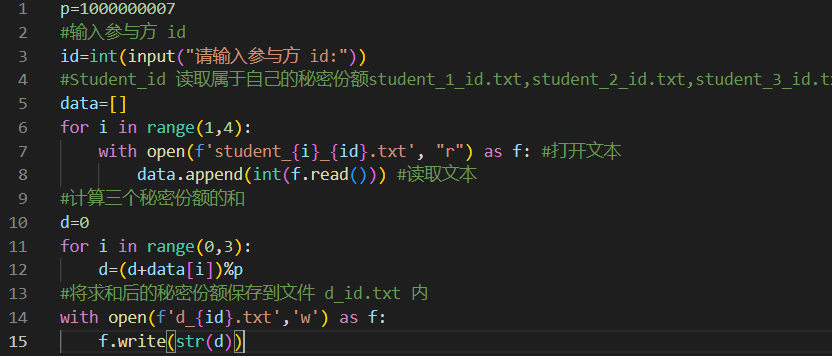


三个学生分别执行ss\_student.py，将自己的秘密投票值共享给另外两个学生。每次输入id和投票制，会产生9个txt，分别保存三个秘密值的秘密份额。

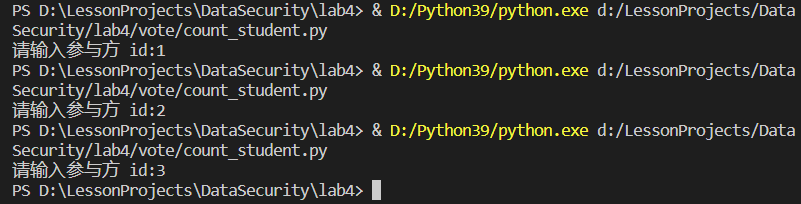


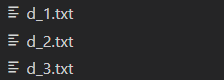
**③ count\_student.py**

在这个文件中，每个学生读取自己的秘密份额（txt文件），计算三个秘密份额的和，并将求和后的秘密份额保存到文件d\_id.txt中。



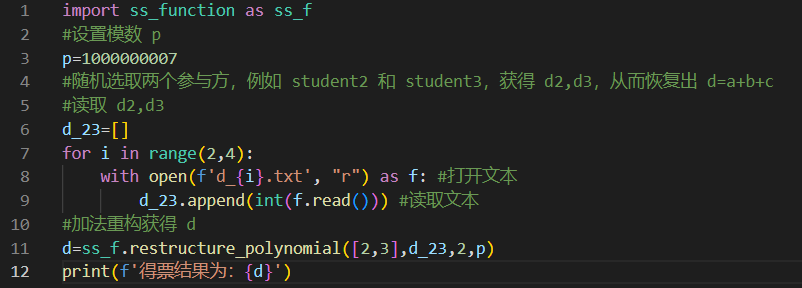
三个学生分别执行count\_student.py，获取另外两个学生的投票值的秘密份额，并将三个投票值的秘密份额相加。执行之后能够得到以下结果：



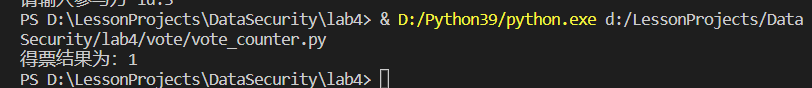


**④ vote\_counter.py**

在这个文件中，随机选取两个参与方，例如 student2 和 student3，获得 d2,d3，从而恢复出 d=a+b+c。之后读取d2和d3，使用加法重构获得d，即得到三位同学投票值之和。



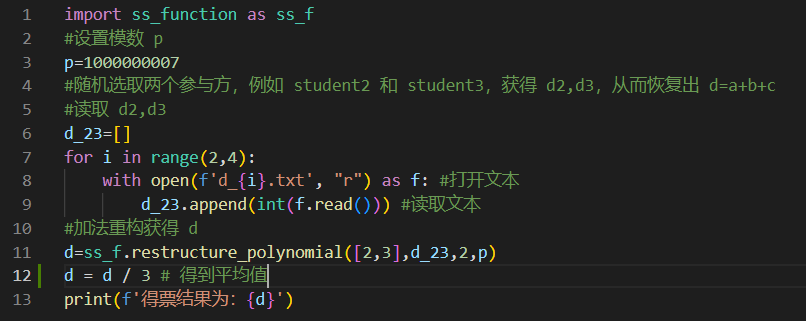
执行后得到以下结果：



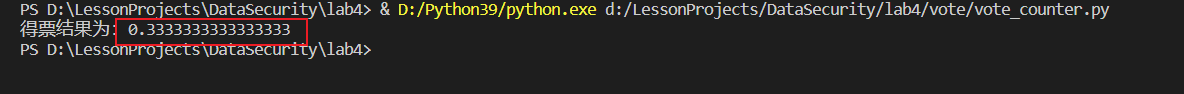
则三个人的总票数为1。

3. 实现三个人对于他们拥有的数据的平均值计算

为了得到三个人拥有数据的平均值，只需要将三个人的总票数除以人数即可。



运行vote\_counter.py，得到平均值：



**心得体会：**

通过这次实验，我对shamir门限秘密共享有了更深的体会。通过网上查询，我了解到了秘密共享实践的优缺点：

相对于其他隐私计算技术，秘密共享的优点是：

1. 安全性较高：秘密共享方案能够保证秘密数据的安全，只有多个参与方一起才能够获取原始秘密数据，保证了隐私的安全性。
2. 灵活性较高：秘密共享方案可以适用于多种计算场景，不需要像差分隐私技术那样需要针对不同的查询场景进行设计和调整。

秘密共享的缺点是:

1. 计算代价较高：秘密共享需要在多个参与方之间进行数据通信和计算，因此需要消耗更多的计算资源和带宽资源。

2. 实现复杂性较高：秘密共享方案需要对多项式运算、加密算法等进行深入的理解和掌握，实现难度较高。

而具体对于Shamir秘密共享方案，其优缺点为：

优点：

    1. 在加密和解密过程中，计算开销小，效率高。

    2. 可以适用于不同的分布式系统场景。

缺点：

    1. 需要事先知道参与者的个数和重建秘密所需的最小阈值。

    2. 不支持动态增减参与者。

除了Shamir秘密共享之外，还有Brickell和Blakley秘密共享方案，希望在以后的学习中能够有更深的了解。