题目

Alice和Bob刚刚得知一门考试的成绩，他们都想知道两个人的成绩是否相同。但是，谁也不愿意暴露自己的成绩。假设成绩采用优、良、中、差四个等级。设计一种安全的游戏方案，使Alice和Bob在游戏中执行相应的算法，在不暴露自己成绩的前提下判定二人成绩是否相同。

为了得到正确的判定结果，假设Alice和Bob不会篡改自己的成绩，但为了保证游戏的公平性，应保证Alice和Bob均能验证结果的正确性。

给定如下三个场景，分别对应三个游戏。

1. 除了Alice和Bob之外，存在一个第三方且知道二人的成绩。假设第三方是可信的，不会泄漏与成绩相关的任何信息。
2. 除了Alice和Bob之外，存在一个第三方但只知道其中一个人的成绩。假设第三方是可信的，不会泄漏与成绩相关的任何信息。
3. 不存在任何知道Alice或Bob成绩的第三方。

只设计了1个场景的游戏可得60～70分，设计了2个场景的游戏可得71～90分，设计了3个场景的游戏可得91～100分。

参考资料

- ElGamal公钥密码体制
  - https://www.cryptopp.com/docs/ref/struct_el_gamal.html
  - https://math.asu.edu/sites/default/files/elgamal.pdf
- Pedersen承诺方案，https://asecuritysite.com/public/ped.pdf
- Diffie-Hellman密钥交换方案
  - https://cryptobook.nakov.com/key-exchange/diffie-hellman-key-exchange
  - https://www.cryptopp.com/docs/ref/struct_d_h.html

程序设计要求

1. 在给定公开参数上编写程序。
2. 多个程序之间可以通过文件传递信息。
3. 编程语言不限。推荐使用C++ GMP library，包括但不限于如下函数：
   - 随机数函数(mpz_urandomm) https://gmplib.org/manual/Integer-Random-Numbers
   - 模幂函数(mpz_powm) https://gmplib.org/manual/Integer-Exponentiation
   - 乘法函数(mpz_mul) https://gmplib.org/manual/Integer-Arithmetic
   - 乘法逆元函数(mpz_invert) https://gmplib.org/manual/Number-Theoretic-Functions

- mpz_set_str函数：GMP参数均为mpz_t类型，该函数是将const char* 类型转化为mpz_t类型，https://gmplib.org/manual/Assigning-Integers

验收要求

1. 分别演示Alice和Bob执行程序的过程，给出成绩相同和不同时的运行结果。
2. 给出当Alice和Bob最终得到结果时，游戏所花费的时间（单位：ms）。
3. 给出游戏所花费的存储空间（例如，全部文件大小的总和，单位：bit）。

报告撰写要求

1. 报告采用《计算机学报》模板http://cjc.ict.ac.cn/wltg/new/submit/index.asp，分为word模板和Latex模板，使用Latex模板可酌情加分。科技排版系统CTEX的下载地址为http://mirrors.ustc.edu.cn/ctex/legacy/2.9/，选择CTeX_2.9.2.164_Full.exe。
2. 报告的内容至少包括如下几方面：
   ① 问题的形式化定义：给出输入、输出的数学表示，并加以文字说明。
   ② 参数/变量表：将所有参数和变量的命名、位数和含义用表格方式列出。

③ 程序交互过程图：将Alice和Bob执行程序的交互过程以图的形式给出，并加以文字说明。

④ 伪代码：分别给出每个算法的伪代码，并加以文字说明。

⑤ 安全性证明：给出游戏方案安全性的证明过程，包含如下四个性质，其中，无论选择哪个场景，性质1的证明为必备项；性质2～4的证明为可选的加分项。

- 性质1：假设Alice和Bob不会篡改自己的成绩，那么他们在游戏中一定能够得到正确的判定结果，并且无法确定对方的成绩。（必备项）
- 性质2：在场景1中，除了Alice和Bob之外，存在一个第三方且知道二人的成绩。那么，在满足性质1的同时，除了Alice、Bob和这个第三方之外的其他人不会在游戏中得到与成绩相关的任何信息。（可选，加分项）
- 性质3：在场景2中，除了Alice和Bob之外，存在一个第三方但只知道其中一个人的成绩。那么，在满足性质1的同时，这个第三方不会在游戏中得到任何额外的信息，并且除了Alice、Bob和这个第三方之外的其他人不会在游戏中得到与成绩相关的任何信息。（可选，加分项）
- 性质4：在场景3中，不存在任何知道Alice或Bob成绩的第三方。那么，在满足性质1的同时，除了Alice和Bob之外的其他人不会在游戏中确定任意一个人的成绩。（可选，加分项）

⑥ 性能分析：

- 时间复杂性：给出每个算法的时间复杂性分析过程
- 空间复杂性：从参数/变量位数的角度，给出每个算法的空间复杂性分析过程

日程安排

- 6月27日（周日）14:00：（腾讯课堂）线上宣讲任务书。
- 6月28日（周一）：学生提交分组和分工（在线填写excel模板）。
- 第一周最后一次课：指导教师评价学生的“算法汇报”，5分钟/组，PPT形式。成绩占比20%（评价指标见excel模板）。
- 第二周最后一次课：指导教师评价学生的“程序汇报”，以演示和测试程序为主。成绩占比20%（评价指标见excel模板）。
- 第三周最后一次课：指导教师评价学生的“验收汇报”，5分钟/组，PPT形式。成绩占比30%（评价指标见excel模板）。
- 7月23日（周五）：学生提交报告。成绩占比30%（评价指标见excel模板）。