Project-6 Google Password Checkup

实验目的

本实验模拟 Google Password Checkup 协议，实现用户密码集合与泄露密码库的安全交集计算，并统计交集密码对应的风险值总和。实验目的是验证基于盲化与同态加密的隐私保护交集协议可行性。

实验原理

本实验参考论文 "Privacy-Preserving Password Checking" Section 3.1 (Figure 2) 中提出的协议：

1. **盲化（Blinding）**
    - P1 对自己的密码集合使用随机数 k1 盲化：

$$v_{k1} = H(v)^{k_1} \mod p$$

    - P2 对接收到的盲化值再用随机数 k2 盲化：

$$Z = (v_{k1})^{k_2} \mod p$$

2. **Paillier 同态加密**
    - P2 对泄露库中每个密码的风险值 t 加密：

$$encrypted\_t = Enc(t)$$

- P1 对盲化匹配的密码收集对应加密风险值，并利用 Paillier 的加法同态性计算加密总和：

$$encrypted\_sum = \sum encrypted\_t$$

3. **安全交集计算**
   - P1 将加密总和发送给 P2，由 P2 解密得到交集密码的风险值总和。
   - 整个过程中，P1 和 P2 无需泄露各自密码明文，保证隐私。

实验思路

1. **P2**：
   - 生成 Paillier 公私钥对
   - 对接收到的盲化值进行二次盲化
   - 对自身密码库的风险值进行加密
   - 将盲化集合和加密风险值发送给 P1
2. **P1**：
   - 对自身集合进行第一次盲化
   - 接收 P2 数据后再次盲化匹配交集
   - 使用 Paillier 同态加法累加交集风险值
   - 发送加密总和给 P2

3. **P2**:
    - 对加密总和解密，得到交集密码的风险值总和

实验结果

```
--------- RESTART: D:/实验文件/shujia/project-6/Google-Pas
====
交集的总风险值：5
```

- 成功计算出 P1 和 P2 密码集合的交集
- 交集密码对应的风险值总和正确
- 实验验证了基于盲化与 Paillier 同态加密的隐私保护交集协议可行性