Project 6：

Google Password Checkup验证

来自刘巍然老师的报告 google password checkup，参考论文 https://eprint.iacr.org/2019/723.pdf 的 section 3.1 ，也即 Figure 2 中展示的协议，尝试实现该协议，（编程语言不限）。

说明：

一、系统简介

本系统是一个基于高级密码学技术实现的隐私保护密码安全检查服务，能够在完全不暴露用户真实密码的前提下，帮助用户检测自己的密码是否存在于已知泄露密码数据库中。系统采用了业界领先的同态加密技术和安全多方计算协议，确保整个检查过程满足最高级别的隐私保护要求。

二、核心组件说明

1. Paillier加密模块

Paillier加密是本系统的基础加密方案，具有以下关键特性：

加法同态特性：允许在加密数据上直接进行加法运算

非对称加密：使用公钥加密、私钥解密的模式

概率加密：相同明文每次加密会产生不同的密文

大数安全：基于大整数分解难题，使用1024位以上的密钥

该模块主要负责：

系统密钥对的生成和管理

敏感数据的加密和解密操作

支持加密状态下的安全计算

2. DDH安全协议模块

DDH(Decisional Diffie-Hellman)协议是系统的隐私保护核心，提供：

安全的密码哈希转换机制

隐私保护的集合成员关系验证

基于离散对数问题的安全基础

主要功能包括：

将密码转换为不可逆的加密指纹

实现不暴露原始数据的比对功能

提供协议所需的安全参数生成

三、工作流程详解

1. 系统初始化阶段

服务端会执行以下准备工作：

生成Paillier加密所需的密钥对

创建DDH协议的安全参数

预处理已知泄露密码数据库

建立必要的安全通信基础架构

2. 密码检查处理流程

完整的密码检查过程分为以下几个步骤：

服务端预处理：

对泄露数据库中的每个密码进行加密处理

生成对应的安全标记

随机打乱存储顺序以增强隐私

客户端准备：

用户输入待检查的密码列表

对每个密码进行相同的加密转换

生成查询请求

安全比对：

系统在加密状态下比对密码指纹

只判断是否存在匹配

不泄露任何额外信息

结果返回：

服务端解密比对结果

仅返回是否存在泄露的布尔值

确保结果与原始密码正确对应

四、安全特性说明

1. 隐私保护机制

数据保密性：全程加密处理，原始密码永不暴露

最小披露原则：仅返回必要的检查结果

抗关联分析：通过随机化处理防止信息推断

2. 安全防护措施

抵抗暴力破解：使用密码学强度的随机数和大素数

防止重放攻击：每次处理都包含新鲜随机因子

抗中间人攻击：完整的安全协议设计

3. 密码学保证

基于经过验证的数学难题

采用标准化的密码学原语

实现完整的协议安全性

实验结果测试：

