题目

前六题：第九章内容

1. 素性检测
2. 大整数分解问题
3. RSA 问题
4. 二次剩余
5. 离散对数问题
6. 双线性对问题

7. AES 加密
8. 椭圆曲线在密码学中的应用
9. 同态加密算法
10. 基于属性的加密（Attribute-based encryption，ABE；包括 CP-ABE，KP-ABE）
11. 零知识证明
12. 安全多方计算

探究内容包括但不限于：

前六题是数学问题：介绍数学问题，算法思想、特点，在密码学中的应用；

后六题是密码原语：介绍密码原语，其应用的具体场景，其中包含的数学问题。

一共12题，分为12组。（**分组截至时间是5月3日晚上23:59，如果超过这个时间没有提交名单，则视为放弃这次作业，直接记零分**）

会给12组随机分配题目进行探究，选一个进行PPT展示，15-20分钟。

（其中有一些问题比较简单，所以对展示的要求会比困难题目更高）

另外，每个人需要交一共报告，从第九章的6个题中选两个题，后6道题目中选一道。每个人一共选3道题，写一个探究报告。

展示是一组展示一个题目，报告每个人都需要提交。每个人都写3个题目的探究报告。

报告提交要求：以小组为单位，将小组的展示 PPT 以及小组所有成员的个人报告（pdf 格式），打包命名位“第xx组信息安全数学基础探究报告.zip/rar”，发送到助教邮箱（2113414@email.nankai.edu.cn）

小组展示时间和探究报告提交时间另行通知。