前 6 道题：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 6 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 6 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；每组不超过 10 个人。

每组选一个题目进行探究，选一个人进行 PPT 展示，15-20 分钟。

另外，每个人需要交一个报告，从第九章的 6 个题中选两个题，后 6 道题中选一个。每个人选 3 道题，写一个探究报告。

展示是一组选一个题展示，报告每个人都需要交。每个人都写 3 个题目的探究报告。

小组展示时间：

2023.5.25 和 2023.6.1 周四晚上两次课。

报告提交要求：

以小组为单位，将小组的展示(.pptx)以及小组所有成员的个人报告（.docx/.pdf），打包命名为“第 xx 组信息安全数学基础探究报告.zip/rar”，2023.6.11 晚 23:59 前发送至助教邮箱（2013920@mail.nankai.edu.cn）。