2023-2024学年《信息安全数学基础》期末

一、计算题(8+5+6)

1.将1写成11和247的线性组合，并且计算说明$11x^2 \equiv 1(mod\ 247)$是否有解?

2.在七进制体系下，计算十进制数2024^{2023}的最后一位。

3.计算同余方程的解：$63x \equiv 42(mod\ 546)$（具体的数字忘了，反正就是一个简单的同余方程）

二、简答题（8+4+6）

1.证明题

第一问：证明$(a+b)^p \equiv (a^p + b^p)(mod\ p)$

第二问：一个简单的关于欧拉函数的证明，用算术基本定理分解就能做

2.证明：$(Z_6, +)$是群

3.选择一个有关探究报告的题目，论述其数学原理和应用前景

三、综合题(12+12+11+21+7)

1.自定义置换群

- 第一问，就是置换群，注意掌握逆元和点乘的算法
- 第二问，根据协议内容写出加密后的数据流
- 第三问，说明该算法的缺点

2.Rabin加密

就是一个简单的CRT

- 第一问，根据明文算密文，简单
- 第二问，根据密文算明文，一共是四个，很简单

3.D-H密钥交换

给了DH密钥交换的协议背景

- 第一问，证明交换体系是域
- 第二问，计算113的原根
- 第三问，证明该加密传输体系得到的两个值是相等的

4.椭圆曲线

给了一整个椭圆曲线加密的体制，告诉你了一些背景知识

- 第一问，求点的阶，纯计算
- 第二问，求3G，纯计算
- 第三问，求两个密钥，也是纯计算
- 第四问，根据明文求密文，反正也是点加和倍加的计算

5.同态同构

忘了，考试随便写了点上去，不知道对不对，反正很难就是了