2020年南开大学网络空间安全学院信息安全专业

**《信息安全数学基础》试卷**（B卷）

学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 姓名\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 总分 |
| 得分 |  |  |  |  |  |

**一、解答题（共计25分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 判断方程是否有解，给出判断过程(无需求解). **（5分）**

2. 判断3是否为17的原根，请说明理由. **（5分）**

3. 设，将分解成不相交的轮换**（5分）**

4. 构造16个元素的有限域. **（5分）**

5. 为素数，阶群是否为循环群，为什么？如果是循环群，生成元有多少个？**（5分）**

**二、计算题（共计25分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 求解方程：. **（8分）**

2. 设上的椭圆曲线为，是其上一点

(1) 计算；**（5分）**

(2) 计算；**（7分）**

(3) 求点的阶.**（5分）**

**三、应用题（共15分）**

|  |  |
| --- | --- |
| 得分 |  |

RSA是现今应用最广泛的公钥密码系统，其数学原理为数论中的欧拉定理. 在RSA密码系统中，记两个不同的素数分别为和，，公钥为，私钥为，欧拉函数为；明文为，密文为.

加密过程为：；

解密过程为：

请根据所学的相关数学知识回答下面两个问题：

(1) 已知公钥为，明文20，试求密文.**（5分）**

(2) 证明RSA解密的正确性.**（10分）**

**四、证明题（共计35分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 设是偶数，是奇数，证明. **（8分）**

2. 设是环，为到的满同态映射，证明

(1) 是的子环；**（6分）**

(2) 与同构；**（7分）**

(3) 若，理想是的素理想而非极大理想；**（6分）**

(4) 若，商环不是欧几里得环（提示：找到此时的）**（8分）**