信息安全数学基础课程
课外读书报告撰写要求

（二零二一年九月）

一、方向

1. RSA 算法的数论基础分析；

2. 椭圆曲线公钥密码算法的数学原理分析；

3. AES 算法的数学理论基础分析；

4. 大数素性检测的数学理论基础分析。

二、要求

（一） 针对上述四个方向，请同学根据自己的学号选择，学号末尾为奇数选择 1 和 3 方向，为偶数选择 2 和 4 方向。要求同学写两篇读书报告，题目自拟；

（二） 要求将主题描述出来，能让读者看懂；

（三） 要求将自己的学习过程，体会，以及知识的关联关系融合进去；

（四） 要求内容有条有理，真实体现自己的学习过程；

（五） 要求文字讲究，格式优美；

（六） 要求大家主动看书、主动思考，并且主动整理；

（七） 要求诚实，有信；自己独立撰写；鼓励讨论，但独立完成；

(八) 要求大家不断的为自己定义目标，不断的分解，最终汇成报告；

三、提交

(一) 只能电子版提交，可以使用 LaTex 或者 MSWord，注意使用 MSWord，公式请务必使用 MSWord 自带的，而且要求 2007 版本以上；LaTex 推荐使用 overleaf，使用 LaTex 可提交 Zip 包或者 pdf。

(二) 要求第一篇不得晚于期中考试完毕的那一周，第二篇不得晚于期末考试时间，鼓励大家提前提交，要求大家务必按照约定时间来提交，延迟视为未提交，这是规则，契约，希望大家要有这个精神。

(三) 提交到 guoshengxu@aliyun.com；

(四) 要求读书报告文件名：01-2020211804-2020212329-张三-20210925-题号-题目.docx/zip/pdf，即需要包含你的序号（每个同学有两个题目，先提交 01，第二次提交位 02），班级，学号，姓名，提交时间，报告题目题号（1，2，3，4，共 4 道题），报告题目。

四、考查

根据大家提交的内容进行批改，并给予每个同学一个评分，最终汇总成平时成绩的一部分。