**《信息安全基础综合实验》课程实验报告**

|  |
| --- |
| **实验题目：Fermat素性检验** |
| **班级：1918039** **学号1：**19180300017 **姓名1：王申奥**  **班级：1918011**  **学号2：**19180100060 **姓名2：贺紫怡**  **班级：1918031** **学号3：**19180300025 **姓名3：王乾旭** |
| **一、实验目的**  **（包括实验环境、实现目标等等）**  实验环境：python3.8  实现目标：大数的费马素性检测 |
| **二、方案设计**  **（包括背景、原理、必要的公式、图表、算法步骤等等）**  原理：Fermat小定理  给定素数p，a∈Z，则有  算法步骤：  给定奇整数m≥3和安全参数k   1. 随机选取整数a，2≤a≤m-2 2. 计算g=（a,m），如果g=1，转（3）；否则，跳出，m为合数 3. 计算(mod m),如果r=1，m可能是素数，转（1）；否则，跳出，m是合数 4. 重复上述过程k次，如果每次得到m可能为素数，则m为素数的概率为 |

|  |
| --- |
| **三、方案实现**  **（包括算法流程图、主要函数的介绍、算法实现的主要代码等等）**  算法流程图：    算法实现代码： |
| **四、数据分析**  **(包括算法测试数据的分析等等)**    输入一个500多位的大素数，安全参数k=5时，检验结果如图。  5次素性检测通过，在96.875%的概率下可以认为是素数 |
| **五、总结**  **（完成的心得和其他，主要是自己碰到的问题，以及解决问题的方法等）**  当大数通过K次费马素性检测时，要根据安全参数K来计算是素数的概率；  当发现输入的数是合数时（不互素，或不满足费马小定理），应直接返回False。 |