**电子科技大学信息与软件工程学院**

**标 准 实 验 报 告**

**（实验）课程名称 信息安全数学基础实验**

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陆圣珩 学 号：2017221302009 指导教师： 陈大江**

**实验地点：信软学院楼西304 实验时间：12.11**

**一、实验室名称： 网络安全实验室**

**二、实验项目名称：模指数运算的实现**

**三、实验学时：2学时**

**四、实验原理：**

重复平方乘算法。

**五、实验目的：**

* 1. 熟悉一种模指数运算算法；
  2. 运用高级程序设计语言完成一种模指数运算算法的程序，加深对模指数运算的理解；
  3. 提供该算法的使用说明手册，可执行代码、源代码及测试用例（包括测试用例手册、可执行代码和源代码）。

**六、实验内容：**

* 1. 本实验要求学生掌握常用的模指数算法的实现方法，即**：**求ae mod m 的值。算法采用重复平方乘的方法实现。

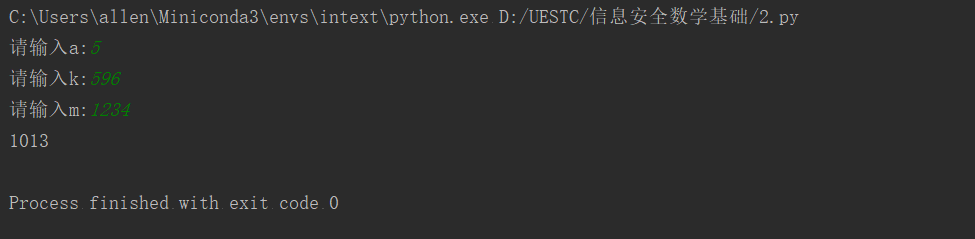
**七、实验步骤：**

1. 熟悉模指数运算的数学原理；
2. 进行算法需求分析；
3. 制定算法流程图；
4. 根据算法需求分析和算法流程图编写实现代码；
5. 编译并运行。

**八、程序代码**

|  |
| --- |
| **a = int(input("请输入a:"))**  **k1 = int(input("请输入k:"))**  **m = int(input("请输入m:"))**  **k = list(str(bin(k1)))**  **k.reverse()**  **t = len(k)**  **b = 1**  **A = a**  **if k[0] == "1":**  **b = a**  **for i in range(1, t):**  **A = (A \* A) % m**  **if k[i] == "1":**  **b = (A \* b) % m**  **print(b)** |

**九、实验数据及结果分析：**



**十、实验结论：**

使用python进行编写重复平方乘算法，并完成测试用例，确认算法正确。

**十一、总结及心得体会：**

在掌握基本算法的情况下可以较容易的进行编写，只需要在指数二进制转换时稍作思考。

**十二、对本实验过程及方法、手段的改进建议：**

无

**报告评分：**

**指导教师签字：**