**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：12.13**

**一、实验室名称： 网络安全实验室**

**二、实验项目名称：模乘法逆元的实现**

**三、实验学时：2学时**

**四、实验原理：**

乘法逆元算法。

**五、实验目的：**

* 1. 熟悉一种求乘法逆元算法；
  2. 依据所选择的算法，编程实现该算法；
  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：**

本实验要求学生掌握常用的求乘法逆元算法的实现方法，并运用高级程序设计语言完成一种求乘法逆元运算算法的程序，加深对求乘法逆元运算的理解。

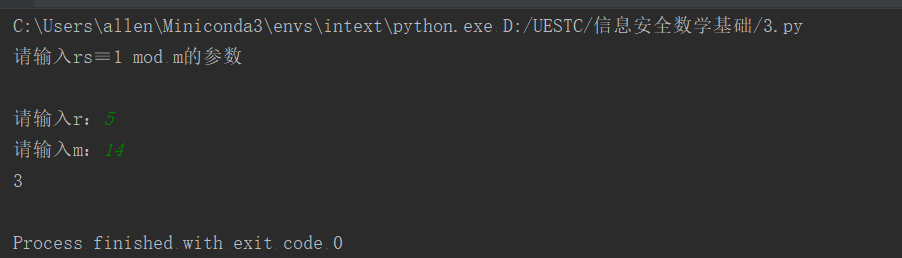
**七、实验步骤：**

1. 熟悉求乘法逆元的核心算法扩展的欧几里德算法的数学原理；
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**

|  |
| --- |
| **def gcd(m, n):**  **if not n:**  **return m**  **else:**  **return gcd(n, m % n)**  **def get(a, b):**  **if b == 0:**  **return 1, 0**  **else:**  **k = a // b**  **remainder = a % b**  **x1, y1 = get(b, remainder)**  **x, y = y1, x1 - k \* y1**  **return x, y**  **print("请输入rs≡1 mod m的参数\n")**  **a = int(input("请输入r："))**  **b = int(input("请输入m："))**  **flag = gcd(a, b)**  **if flag == 1:**  **x, y = get(a, b)**  **result = x % abs(b)**  **print(result)** |

**九、实验数据及结果分析：**



**十、实验结论：**

使用python进行编写模乘法逆元算法，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，在完成最基本的乘法逆元算法之外还需要判断是否存在乘法逆元。

**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：**