电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221302006

姓 名 周玉川

（实验） 课程名称 信息安全数学基础

理论教师 陈大江

实验教师 陈大江

**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：周玉川 学号：2017221302006 指导教师：陈大江**

**实验地点：信软楼西304 实验时间：2018.11.08**

**一、实验名称：模指数运算的实现**

**二、实验学时：2**

**三、实验目的：**

1.掌握一个数字较大的模指数运算。

2.利用掌握的编程语言，编写代码实现模指数运算。

**四、实验原理：**

数字的指数运算，尤其是当指数较大的时候，先把指数运算后的结果算出来，再进行就模运算，一般不现实，一是因为算出来的结果太大位数过长，二是因为用数组储存大数后也不易进行求模运算，这时急需一个算法解决这个问题。

模的指数运算可以运用重复平方乘算法有效实现，这一运算在很多密码学协议中都有重要用处。这一算法是基于以下结果，设k的二进制表示为，其中，则易证明

重复平方乘算法

算法2.5.2 中重复平方乘算法

输入：，整数，其二进制表示为

输出：

1、令，如果，则返回(b)；

2、令；

3、如果，则令；

4、对i从1到t，作

4.1令；

4.2如果，则令；

5、返回(b)

**五、实验内容：**

本实验要求学生掌握常用的重复平方乘算法求模指数运算的实现方法，并运用高级程序设计语言完成一种重复平方乘算法的程序，加深对模指数运算的理解。

**六、实验器材（设备、元器件）：**

Pc一台。

**七、实验步骤：**

1. 编写代码。

2. 输入数字，指数，以及要模的数字。

3.输出正确结果

**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

程序代码（利用java编写）

|  |
| --- |
| package test;  import java.util.Scanner;  //测试类  public class 重复平方乘算法 {  //定义类函数，返回结果  static int f(int a, int k, int m) {  int b = 1;  if (k == 0) {  } else {  int A = a;  if (k % 2 == 1) {  b = a;  }  k = k / 2;  while (k != 0) {  A = (A \* A) % m;  if (k % 2 == 1) {  b = (A \* b) % m;  }  k = k / 2;  }  }  return b;  }  //主函数  public static void main(String[] args) {  Scanner x = new Scanner(System.in);  int a, k, m;  //提示信息  System.out.println("Input a,k,m,usage:a^k(mod m)");  //读入用户输入的数据  a = x.nextInt();  k = x.nextInt();  m = x.nextInt();  x.close();  //提示信息  System.out.println("Your input: a=" + a + "\tk=" + k + "\tm=" + m);  //输出结果  System.out.println("After claculate: result-->" + a + "^" + k + "(mod " + m + ") = " + f(a, k, m));  }  } |

运行结果分析

|  |
| --- |
| Input a,k,m,usage:a^k(mod m)  5 569 1234  Your input: a=5 k=569 m=1234  5^569(mod 1234) = 991 |
| Input a,k,m,usage:a^k(mod m)  5 596 1234  Your input: a=5 k=596 m=1234  After claculate: result-->5^596(mod 1234) = 1013 |

**九、总结及心得体会：**

1.深入理解模的指数运算，可以很容易弄懂书中伪代码。

2.编程能力也占一定重要性。

3.重复平常算法利用的原理就是A = a (mod m)其中0<=a<m，A大于m，A\*A = a\*a = a’ (mod m)其中0<=a’<m。

**十、对本实验过程及方法、手段的改进建议：**

1.实验内容较少，书本上除了这个重复平常算法，还有Garner算法（中国剩余定理），以及同余方程，勒让德符号等均可以用代码实现，可以适当增加内容。

2.鼓励学生用C语言之外的编程语言完成要求。

3.数学知识尤其是和算术相关的定理，用计算机语言很容易实现，若有兴趣，可以全部实现，很有趣，也有成就感，对信安基础的学习也大有帮助。

4.希望老师能一次少布置一点作业，但是分多次布置一章的作业，而且一星期交一次作业，这样不容易遗忘知识。

**报告评分：**

**指导教师签字：**