武汉大学计算机学院

2011-2012 学年度第一学期 2010 级

《信息安全数学基础》期末考试试卷(B 卷)

班级_____学号_____ 姓名_____

一． 名词解释（每小题 4 分，共 20 分）。

1. 对称群； 2. 最小正完全剩余系；3.平方非剩余； 4.勒让德符号；5.指数。

二． 计算题（每小题 10 分，共 60 分）。

1.求解高次同余式 $x^{12} \equiv 37 (\mathrm{mod}\, 41)$ 。

2.有一个人每工作八天后休息两天。有一次他在星期三、星期四休息，问最少要几周后他可以在星期四休息？

3.求解同余式 $x^2+x+7 \equiv 0$（mod 27）。

4.判断同余式 $x^2 \equiv 102 (\mathrm{mod}\ 259)$是否有解？有解时求出其所有解。

5.求模 47 的所有原根，并且建立它的关于最小正原根的指标表，由此求解如下高次剩余

$$x^5 \equiv 29 (\mathrm{mod}\ 47)$$

6. 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$，

$g(x) = x^8 + x^4 + x^3 + x + 1 \in F_2[x]$，求 $q(x)$和$r(x)$，使得

$f(x) = g(x)q(x) + r(x), \deg r(x) < \deg g(x)$ 。

三. 论述题（共 20 分）

简述椭圆曲线加密和解密的一般过程，并举例说明。