**2012级《信息安全数学基础》考试试题(A)参考答案**

1. **简答题（共20分，每题4分）**

**1．**公钥密码学所基于的三个难解数学问题是：大因数分解问题；离散对数问题和椭圆曲线离散对数问题；

**2.** 16,2,4,22, 8, 26, 20, 14(答案不唯一)；

**3. **时有解，有****个解；

4. ****,***p*** 为奇质数；

5. {e, (123),(132)}

二．**判断题（共20分，每题2分，对的打“√”，错的打“×”）**

1. **√；**2. **×；**3. **√；**4. **×；**5. **√×；**

6. **√；**7. **√；**8. **×；**9. **√；**10. **×；**

**三．计算题（50分）**

1. **解： **

2. 解：

3.解：.

4.解：根据定义计算得

5.解：先求

得：，

即，

即

所以同余式的解为：

第1页

6.解：,

加法表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + | 0 | 1 | x | x+1 |
| 0 | 0 | 1 | x | x+1 |
| 1 | 1 | 0 | x+1 | x |
| x | x | x+1 | 0 | 1 |
| x+1 | x+1 | x | 1 | 0 |

乘法表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \* | 0 | 1 | x | x+1 |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | x+1 |
| x | 0 | x | x+1 | 1 |
| x+1 | 0 | x+1 | 1 | x |

7. 根据公式计算得：2Q=（9,5），3Q=（4,16）

**四、证明题（10分，每题5分）**

**1.证明：**设，于是。由此得到

，u,v都是正整数，推出d|2，d=1或d=2，显然d=1.证毕

**2.证明：**

利用综合除法，这些多项式都不整除，因此结论成立。