# 密码学基础-作业4

提交方式：通过HITsz Grade平台提交 提交截止时间：以系统上公布时间为准

提交格式：pdf文件 文件命名规则：学号\_姓名\_作业4.pdf

注：若包含照片或插图，请旋转至适合阅读的方向

1. 设在方法中，公用素数,本原根。

(a)证明是的本原根。

(b)若用户的公钥则的私钥为多少？

(c)若用户的公钥,则与共享的密钥为多少？

1. 节中介绍了针对密钥交换协议的中间人攻击。敌手生成了两个公钥-私钥对。如果只生成一个公钥-私钥对，那么能够完成攻击吗？
2. 下列上的椭圆曲线的点的负数是多少？；；。
3. 节的开头，当给定一个单分组消息的值时，敌手立即就知道两个分组消息值，因为该值仍然是。请证明上述结论。
4. 设计算法的一个变体作为数字签名是有意义的。下面的方法比更简单，它只需要私钥而不需要秘密随机数：

**公开素数** ，素数

，且是的本原根

**私钥**

**公钥**

要对消息签名，则先计算该消息的码。我们要求若不等于,则将该哈希码附在消息后再计算哈希码，继续该过程直至产生的哈希码与互素：然后计算满足的,并将作为对该消息的签名。验证签名即是验证。

(a)证明该方案能够正确运行。即证明若签名是有效的，则在验证过程中将有上述等式成立。

(b)给出一种简单的方法对任意消息伪造用户签名，以证明这种体制是不可接受的。

1. 预处理要进行消息填充：在消息原文后面需要填充第一位为其余为的消息，末尾位要填充上原文消息的长度。请计算待填充消息的长度。

（1）若消息长度为位，需要填充（ ）位

（2）若消息长度为位，需要填充（ ）位

（3）算法最终得到的消息摘要长度是（ ）位