# 密码学基础-作业3

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3.pdf

注：若包含照片或插图，请旋转至适合阅读的方向

1. 求：

2. 用扩展欧几里得算法求下列乘法逆元：

3. 用费马小定理计算：

4. 用费马小定理找到一个位于到之间的数，使得模与同余（不使用穷举法）。

5. 用欧拉定理找到一个位于到之间的数，使得模与同余（注意这等同于的十进制数展开的最后一位）。

6. 下面是孙子用来说明CRT的一个例子，请求解x。

； ；

7. 给定的本原根，构造离散对数表，并利用该表解下列同余方程：

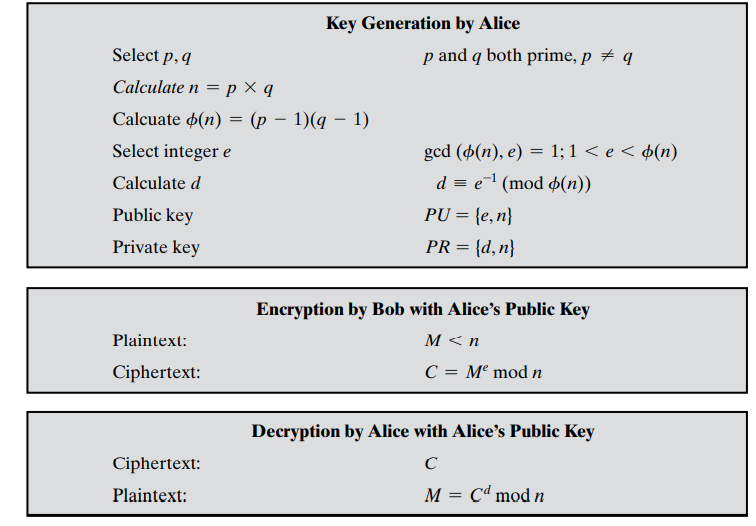
a.

b.

c.

8. 用下图所示的RSA算法对以下数据实现加密和解密：

，，，



9. 在RSA公钥密码体制中，每个用户都有一个公钥和一个私钥。假定Bob的私钥已泄密。Bob决定生成新的公钥和私钥，而不生成新的模数，请问这样做安全吗？

1. 本题说明选择密文攻击的简单应用。Bob截获了一份发给Alice的密文C，该密文是用Alice的公钥e加密的。Bob想获得原始消息$M=C^d~mod~n$。Bob选择一个小于n的随机数r，并计算，，。接着，Bob让Alice用她的私钥对进行认证（见图9.3），从而解密。Alice返回。说明Bob如何利用获得的信息求。

