第三次作业

作业3-习题1~2

- (William中文第八版)P40页习题2.20、2.21

① 用Fermat定理计算$3^{201} \bmod 11$

② 用Fermat定理找到一个位于0到72之间的数，使得a模73与9^{794}同余

作业3-习题3

- (William中文第八版)P198页习题9.2

③ 用RSA算法对下列数据实现加密和解密

a. p=3； q=11， e=7； M=5

b. p=3； q=11， e=7； M=9

c. p=7； q=11， e=17； M=8

作业3-习题4

- (William中文第八版)P41页习题2.35

④ **请通过中国剩余定理（CRT）回答下面的问题：**

六位教授分别在周一至周六开始授课，并且分别每隔2，3，4，1，6，5天授课一次，该大学禁止周日上课。什么时候所有六位教授首次发现必须同时停一次课？

作业3-习题5

⑤ 设ElGamal体制的公用素数$p = 71$，其本原根$g = 7$

a.若B的公钥$Y_b = 3$，A选择的随机整数$k = 2$，则$M = 30$的密文是什么？

b.若A选择的k值使得M=30的密文$C = (59, C_2)$，则整数C_2是多少？

作业3-习题6

⑥ 在ElGamal算法中，为什么要使用不同的随机数k来加密不同的消息？

提交要求

- 通过教学网提交，由助教王元达负责批改
- 如果包含多个文件，压缩为一个文件，提交作业的文件名采用“学号+姓名+第几次作业”
- 例 “1300048400杨帆第1次作业.rar”
- 按时提交截止时间:11月6日23：30前提交