

# 现代密码学

## 第七讲作业

## 第七讲

1. 若通信双方使用**RSA**单向陷门函数加解密信息，已知接收方公钥  $(e,n)=(5,35)$ ，截获密文为  $C=10$ ，求私钥  $d$  和明文  $M$ .
2. 若使用**ElGamal**单向陷门函数加解密信息，已知接收方 **B** 的公钥  $(p=71, g=7, y_B=3)$ .
  - 1) 设发送方 **A** 选择的随机整数  $k=3$ ，求明文  $M=10$  所对应的密文.
  - 2) 若截获到 **A** 发送的密文是  $C=(59,29)$ ，求  $M$ .
  - 3) 若截获到 **A** 发送的密文是  $C=(49,29)$ ，求  $M$ .

## 第七讲

3. (选做)调研并实践生成大素数的方法。
4. (选做)调研SM2加密标准的密钥生成、加密、解密详细步骤。
5. (选做) 调研密码库函数中模幂运算的快速实现方法.
6. (选做) 调研椭圆曲线上点乘运算 $kG$ 的快速实现方法.