现代密码学

第七讲 公钥加密

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.