## 5.5习题

1. **请简述对称密码算法与公钥密码算法的区别。**

答：对称密码体制中通信双方共享一个秘密密钥，此密钥既能用于加密，也能用于解密。公钥密码体制的最大特点是采用两个相关密钥将加密和解密能力分开，其中一个密钥是公开的，为公钥，用于加密；另一个密钥是为用户专用，因而是保密的，称为私钥，用于解密。

1. **设攻击者J截获用户A利用RSA算法加密的一条密文信息为，并获知公钥信息。问攻击者J破解出的明文信息是多少？**

解：

设e在模下的乘法逆元为d，则



则攻击者J破解出的明文信息m为



1. **在RSA算法中，若已知某用户的公钥信息为，你们该用户的私钥是多少？**

解：对n进行素因数分解得

则



**5.在ElGamal算法中，取素数，是的一个生成元，明文。**

**(1) 若公钥，随机选取，问明文加密后的密文是多少？**

**(2) 若，已知明文加密后的密文是，那么是多少？**

解:（1）



（2）



6. **设有限域上的椭圆曲线为。**

**(1) 给出上的有理点群，并说明此群的结构。**

**(2) 令，则是上的点。计算标量乘、、。**

**(3) 令，则也是上的点。解离散对数问题：**

。

a. Abel群：满足，还要包括无穷远点。

b. 标量乘：二元法

解：（1）



（2）









(3)解 得



(4)

p=(17,3)

**9、在ElGamal 数字签名方案中，素数，是模的本原根。Alice取为其私钥，求Alice的公钥。如果Bob有消息，问Alice对的签名是什么？**

解：Alice的公钥为



根据所选取的整数  会得到相应Alice对的签名，签名计算略。

**10、假设在lGamal 数字签名方案中，p=31847是模的本原根，g=5是模p的本源根，b=25703是Alice的公钥。**

**1）已知（23972，31396）与（23972，20481）分别是同一随机数k对消息m=8990与消息m=31415的签名，问随机数k=？以及Alice的私钥a=?**

**2）如果Alice的私钥k=379，而（13202，12552）与（15818，16741）分别用不同的随机数与对消息m-31415的签名，问能否确定出与？若能确定给出它们的值。**

**解：**

****

**11、在DSA 数字签名方案中，素数，是的素因子。**

1. **取。请给出你的私钥与公钥？**
2. **选择一个随机数对消息进行签名，并验证你的签名。**

解：1）根据所选取的参数会得到相应的私钥和公钥，计算略。

2）根据所选取的随机数会得到相应的签名，计算略。

**13、取， 上椭圆曲线为。**

**1） 有理点群共含有29个点，你能否给出这29个点？**

**2） 点是的一个生成元。如果取是椭圆曲线数字签名算法中你的私钥，那么你的公钥是什么？**

**3）对消息计算出你签名，并验证你的签名。**

解：

1）（0，2）（0，21）（1，11）（1，12）（4，7）（4，16）（7，20）（7，3）（8，8）（8，15）（9，11）（9，12）（10，5）（10，18） （11，9）（11，14） （13，11）（13，12）（14，5）（14，18） （15，6）（15，17） （17，9）（17，14）（18，9）（18，14） （22，5）（22，18） 无穷远点O.

1. 公钥是



1. 根据选定的参数对消息计算出相应的签名，

