网安2022真题

2022/6/13

一、简答题

（1）简述为什么输出反馈模式（OFB）传输中的比特差错不会传播，而更易受报文流篡改攻击

（2）叙述费马定理，并对费马定理做完整的证明

二、计算题

（1）用户A与用户B共同约定大素数p=23，生成元g=5，根据Diffie-Hellman密钥交换协议，用户A和用户B进行密钥交换。用户A选择私钥X_A=3，用户B选择私钥X_B=2，请图示描述密钥交换过程，并计算K_{AB}

（2）已知X≡2（mod 3）X≡3（mod 7）X≡6（mod11），通过中国剩余定理，试求解X?

（3）通过ElGamal概率密码系统对消息m进行加密，其中共享大素数p=19，生成元α=3，用户A的私钥X_A=2，用户B的私钥X_B=5，需要加密的消息m=7，m从A发送到B，A选择k=5，求：首先，阐述什么是概率密码系统，并计算密文（c_1, c_2）

三、选择题

（1）数字证书的本质目的在于（ ）

A 发布用户的公钥

B 发布用户的身份标识

C 发布用户公钥并以一种可核实的方式将该公钥与其合法持有者的身份标识联系起来

D 发布用户私钥并以一种可核实的方式将该私钥与其合法持有者的身份标识联系起来

（2）下列哪项技术不能解决重放攻击（）

A 使用时间戳

B 哈希函数

C 挑战/应答

D 使用序列号

（3）凯撒密码之所以能被穷举攻击，不是因为下列哪个原因（）

A 是对称加密技术

B 加解密算法已知

C 密钥空间小

D 所被加密的明文可识别

（4）φ（N）是N的Euler函数，φ（77）的值是（）

A 64　B 60　C 52　D 70

（5）数字签名要预先使用单项Hash函数进行处理的原因是（）

A 多一道加密工序使密文更难破译

B 提高密文的计算速度

C 缩小密文签名的长度，加快数字签名和验证前面的运算速度

D 保证密文能正确还原成明文

四、分析题

（1）如下图【就是公钥授权的示意图】，其中KUa为发起者a的公钥，KUb为应答者的公钥

1.对图中的公钥发布方案逐条按顺序（1）-（7）进行说明

2.详细阐述Request和Time1嵌入到消息2的作用，以及N1、N2的作用

3.阐述该公钥分配方案的缺点

（2）试分析为什么攻击RSA的困难是基于大合数的质因子分解问题，即分解N=pq问题