中 国 科 学 技 术 大 学

装订线 答题时不要超过此线

2019--2020学年第2学期考试试卷A卷

考试科目: 密码学导论 得分:\_\_\_\_\_\_\_\_\_\_

学生所在院系:\_\_\_\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_ 学号:\_\_\_\_\_\_\_\_\_\_\_

**一、单项选择题 （15分）**

1. 用于身份认证的哈希函数必须具备下列（）性质。

A. 单向性 B. 抗弱碰撞

C. 抗强碰撞 D. 以上全部

2. 关于RSA算法，下列说法正确的是（）。

A. RSA属于分组密码

B. RSA可以使用一对足够大的素数p和q来为所有人建立共同的公共模数n=pq

C. RSA可以设置较小的私钥，例如65537，以方便自己解密运算和签名运算

D. RSA名称的含义是分别以R、S字母开头的两个人设计的Algorithm

3. Alice和Bob拥有一对对称密钥，下列说法正确的是（）。

A. 若Bob收到该密钥加密的一段消息，则可确认该消息是Alice加密的

B. 若Bob收到该密钥加密的一段消息，则可确认发信方是Alice

C. Alice能够否认自己发送过的加密消息

D. Alice可以将时间戳与明文一同加密，来作为时间证据

4. 根据密码分析者所掌握的信息多少，可将密码分析分为：唯密文攻击、已知明文攻击、选择明文攻击和（）。

A. 已知密文攻击

B. 选择密文攻击

C. 猜测部分明文攻击

D. 猜测部分密钥攻击

5. 下面关于数字签名（私钥未丢失）的描述**不正确**的是（  ）。

A. 数字签名是不可抵赖的 B. 数字签名是不可伪造的

C. 数字签名是不可替换的 D. 被签名文件是不可更改的

**二、填空题 （15分）**

6. 分组密码的计数器工作模式英文缩写为  ，它  （支持/不支持）预处理和并行处理，  （支持/不支持）分组的随机加密或解密，  （存在/不存在）错误传播。

7. 密码学意义安全的伪随机序列生成器应能通过多项式时间统计测试和续位测试。多项式时间统计测试是指，任何算法均不能以大于1/2的概率正确区分该生成器的输出序列和一个同等长度的序列；续位测试是指不存在算法，能够根据以大于1/2的概率有效预测下一个比特。

8. RSA算法依赖的数学难题是， ElGamal算法依赖的数学难题是， ECC算法依赖的数学难题是，Diffie-Hellman协议依赖的数学难题是 。

9. 密码协议中常用的nonce有、、。

**三、问答与计算题**

10. 什么是密钥的唯一解距离？什么是消息的唯一解距离？一般而言，二者谁更大？当恰好满足消息的唯一解距离要求时，密钥被破译的概率是否大于50%？为什么？ （10分）

11. 为抵抗选择明文攻击，有人提出这样一个方案：先用算法H对明文计算摘要，然后用算法F将摘要与密钥K进行运算，得到一个新的密钥，用新密钥加密明文。当然，摘要算法H、算法F以及加密算法E都是公开的。请问：

（1）若要使该方案可行，假设明文为M，写出加密方发送给解密方的数据。

（2）该方案与二战时期德国使用Enigma的哪个操作过程有异曲同工之处？

（3）请设计一个比题中方案效率更高的方法来达到同样的效果。

本题解答时不应引入H、F、E之外的运算。（10分）

12. 加密和签名是两种重要的安全机制，在应用中可以先加密后签名，也可以先签名后加密。试举例分析这两种不同的顺序各有什么便利和局限？（10分）

13. 某RSA系统中，密钥管理中心为用户A和用户B分配了相同的模数n=77。已知用户A的公钥eA=5，用户B的公钥eB=7。攻击者从某个途径获知：有人向用户A和用户B分别加密传输了同一个消息m，给用户A的密文cA=10，给用户B的密文cB=68。试破解消息m。注意，你不能对模数分解质因数，因而也无法求解两个用户的私钥。当然，你也不可以靠猜测。（15分）

14. 在ElGamal系统中，取本原元α=7，模数p=13，Alice的私钥xa=4, Bob的私钥xb=11

（1）假定Alice加密传送m=4给Bob，随机选择k=7，密文是什么？

（2）如果Alice要签名m=8，随机选择k=5，签名是什么？随机选择k=7，签名是什么?

（3）如果消息m=5附加的签名值是(2,4)，Bob如何验证？（15分）

15. 结合以下密钥分配协议，说明已过期的旧密钥为何必须妥善销毁？如何修改此协议以避免这种威胁？（10分）

A🡪KDC: IDA || IDB || N1

KDC🡪A: E(KA, KS || IDA || IDB || N1) || E(KB, KS || IDA)

A🡪B: E(KB, KS || IDA)

B🡪A: E(KS, N2)

A🡪B: E(KS, f(N2))