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1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 （18分）**

1. 下列哪一个性质不属于密码学关注的范畴？（）

A. 保密性 B. 完整性 C. 访问控制 D. 可视性

2. AES的密钥长度不能选择下面哪一个? （）

A. 512比特 B. 256比特 C. 192比特 D. 128比特

3. 采用公开密钥加密体制，用私钥对数据进行加密运算，可以提供哪些安全服务？（）

A. 数据保密性、来源认证 B. 来源认证、隐私保护

C. 不可否认、完整性保护 D. 来源认证、访问控制

4. 关于Feistel框架，描述不正确的是？（）

A. 框架采用了S-P迭代结构

B. 从安全角度，轮函数可以采用散列函数

C. 从可解密角度，轮函数可以取消

D. 解密过程与加密过程完全一致

5. 以下哪一个不是用于序列加密的伪随机数必须具有的性质？（）

A. 不可预测性 B. 不可重复性 C. 分布一致性 D. 统计独立性

6. 采用拉格朗日插值多项式实现（t,n）秘密分享门限方案，当设定为由9个用户中的3个协作可重建秘密时，多项式的次数应当为（  ）

A. 2 B. 3 C. 8 D. 9

**二、填空题 （14分）**

7. DSA是算法，RC4是算法，RC5是算法，RIPEMD是算法，SMS4是算法（填分组密码，序列密码，散列，或数字签名）

8. SHA-1标准的分块大小为512比特，包括4轮运算，每轮20步，输出摘要长度是比特，抗强碰撞的能力是2的次方；SHA-256标准输出的摘要长度是比特，抗强碰撞的能力是2的次方。

9. 对于具有良好雪崩效应的密码算法，字符频率统计攻击（有效/无效）。这是因为  
。

10. n级最长LFSR包含个延迟存储单元，输出比特序列的周期是。在一个周期内，长为k（k≤n-2）的0游程最多有个。

**三、问答与计算题**

11. 请从密码系统的概率模型角度，简要说明“敌人了解系统”是指什么？什么是无条件安全，什么是实际安全？ （8分）

12. 分组密码的明文分组链接模式与标准CBC模式相似，区别仅在于它链接的是前一个分组的明文，而不是密文。请（1）画出明文分组链接模式的加密和解密框图；（2）若某个密文分组在传输中发生错误（即0或1发生翻转），分析错误扩散情况；（3）分析明文分组链接模式的优缺点。 （10分）

13. 线性同余生成器Xn=(aXn-1 + b) mod M （0≤a,b<M）是一种具有良好统计特性的序列发生器，常用来生成用于仿真目的的伪随机数序列，但它的安全性很差。通过观察某个发生器的输出，发现它输出的数字均小于99，且序列的前3个数字是 “15，75，93”。求：（1）系数a和b；（2）输出序列的周期。 （12分）

14. 考虑如右图的非线性组合生成器，它的输出是z序列，三个LFSR的输出分别是x1,x2,x3序列。z序列是将x1和x2相与后，再与x3异或得到。问：（1）各LFSR的输出泄露到z的概率是多大？（2）如何进行相关攻击？（3）假定各LFSR都是长度为L的最长线性反馈移位寄存器，则相关攻击的穷举工作量是多少？ （14分）

LFSR1

LFSR2

LFSR3

与

输出z

x1

x2

x3

15. Alice和Bob使用ElGamal算法实现保密和签名。已知公共大素数P=23，本原元素α=5。已知Alice的私钥XA=5，Bob的私钥XB=6。

（1）计算Alice和Bob的公钥YA和YB。

（2）若Alice欲将消息m=2加密发送给Bob，她选择的随机数k=3，求密文数据。

（3）若Alice欲将消息m=2签名发送给Bob，她选择的随机数k=3，求签名数据。

（4）若Carol对消息m=2的签名为（4,16），且她选择的随机数k=4发生泄露，求Carol的私钥。 （14分）

16. Alice有N个秘密，她想将其中一个传给Bob。Bob只能获得一个秘密，但不能选择是哪一个秘密。除Bob外，包括Alice在内的任何人都不知道Bob获得了什么秘密。请设计一个完成该任务的协议，并分析该协议的安全假设和所用到密码算法的约束。（说明：你无需默写课堂介绍的协议。可以自行设计并分析） （10分）