中 国 科 学 技 术 大 学

装订线 答题时不要超过此线

2018--2019学年第1学期考试试卷A卷

考试科目: 密码学导论 得分:\_\_\_\_\_\_\_\_\_\_

学生所在系:\_\_\_\_\_\_\_\_\_\_\_ 姓名:\_\_\_\_\_\_\_\_\_\_ 学号:\_\_\_\_\_\_\_\_\_\_\_

**一、单项选择题 （15分）**

1. 关于冗余的作用，下列表述错误的是（）

A. 冗余决定了压缩可能达到的极限

B. 自然语言中的冗余无法彻底消除

C. 冗余是描述消息性质的，与密码系统的安全性无关

D. 如果能在消息中消除冗余，那么即使采用凯撒密码加密也可以获得完美安全

2. 以下哪一种情况不是实际安全的? （）

A. 密码破译被证明等价于解数学难题，且问题规模足够大

B. 使用现有的计算资源不能破译

C. 在消息失效前不能破译

D. 破译消息的代价远超过消息本身的价值

3. 以下哪一个不是对称密钥算法？（）

A. DES B. ECC C. RC5 D. RC4

4. 在Shannon的概率模型下，攻击者截获密文后所要进行的分析不包括以下那一条？（）

A. 可能的明文的后验概率

B. 可能的密文的后验概率

C. 可能的密钥的后验概率

D. 实际的密钥

5. 用于认证的可信时间戳不能由发信人自行添加的原因，不包括（）

A. 发信人可以撒谎

B. 发信人可以抵赖

C. 发信人可以自由设定自己系统时间

D. 时间戳可以被篡改

**二、填空题 （15分）**

6. AES加密标准的分组长度是  比特，密钥长度是  比特；SMS4加密标准的分组长度是  比特，密钥长度是  比特。

7. MD5标准的摘要长度是  比特，抗强碰撞的能力是2的  次方；SHA-1标准的摘要长度是  比特，抗强碰撞的能力是2的  次方；SHA-384标准的摘要长度是  比特，抗强碰撞的能力是2的  次方。

8. 传统密码算法采用的两类基本加密方法是  和  ，交替使用这两种方法，并在其中插入一个简单变换，就可以实现  和混淆的效果，增加统计分析的难度。

9. n级最长LFSR输出的是m序列，在一个周期内，长为n-1的0游程最多有  个，长为n的1游程最多有  个。

**三、问答与计算题**

10. 仿射密码本质上是定义在模运算上的一元一次线性函数C=am+b mod 26，其中常数a和b是密钥。若已知字母“f”(5)被加密为字母“V”(21)，字母“t”（19）被加密为字母“T”（19），且密文可以唯一解密，求解所有可能的密钥。（10分）

11. 若已知一个6阶线性反馈移位寄存器自时钟为0时起的输出为001001001001…，问

a) 时钟为0时，各寄存器的状态是什么（从第5级至第0级顺序写出）？

b) 时钟为5时，各寄存器的状态是什么（从第5级至第0级顺序写出）？

c) 画出一个满足条件的线性反馈移位寄存器结构。

d) 该输出序列中，前2个比特的线性复杂度是多少？前3个比特的线性复杂度是多少？

e) 该输出序列中前12个比特的线性复杂度是6吗？为什么？（10分）

12. 五个人采用拉格朗日插值多项式方案进行（3,5）门限秘密分享。已知其中三份分享为H(x=1)=1，H(x=2)=3，H(x=3)=4，模数为11，问秘密值是多少？（10分）

13. 分组密码的明文反馈链接与标准的CFB模式相似，区别仅在于它将该分组的明文而不是密文反馈进入移位寄存器中。

a) 请画出明文反馈链接模式的加密和解密框图。

b) 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。

c) 请分析明文反馈链接与CFB相比的优缺点。（10分）

14. Alice和Bob使用RSA算法实现保密和签名。已知Alice的nA=55，Alice的公钥eA=27，Bob的nB=65，公钥eB=11。

a) 请计算Alice和Bob的私钥。

b) 若Alice欲将消息m=2加密发送给Bob，求她发送的数据。

c) 若Alice收到Bob发来的密文C=7，及对明文的签名S=2，求明文并验证签名。（10分）

15. 分组密码算法可用于构造Hash函数。假设有一个分组密码算法E(k,m)，分组长度为n比特，密文不扩展，我们可以如下构造一个Hash函数：将消息分组为M1, M2, …, Mm，采用CBC模式加密，即Hi=E(k, Hi-1⊕Mi)，H0是n比特全零分组，Hm为最终的散列函数结果，k是一个公开的常数。但这样构造的Hash函数是不抗碰撞的。

a) 给出一种基于生日悖论的复杂度为2n/2的构造强碰撞的方法

b) 给出一种基于生日悖论的复杂度为2n/2的构造弱碰撞的方法

c) 给出一种不基于生日悖论的复杂度为1的构造弱碰撞的方法 （20分）