24-25-2-现代密码学（网络空间安全学院）

判断题（10 个，10 分）

1. ECB 不能用于加密长消息
2. 序列密码的安全性与密钥长度有关，与 IV 长度无关
3. Hash 的初始变量是常数，不随输入变化而变化
4. （n, t）秘密共享方案，大于 t 个人才可以重新解密
5. 量子计算方案可用后，RSA 和 ECC 都不安全了
6. 密钥恢复和密钥撤销的前提不同，前者密钥未泄露，后者密钥已泄露

填空题（20 个，20 分）

1. AES 的分组长度（），密钥长度（）
2. 商密中 Hash 是（），分组密码是（）
3. 明文 160b，IV128b，CTR-AES 的密文长度至少为（），CBC-AES 的密文长度至少为（）
4. RSA 基于（）的困难性，DSA 基于（）的困难性
5. 在 2^{80} 的计算能力下，El Gamal 的安全的最小参数长度（），ECC 的安全的最小参数长度（）
6. 数字签名中，最强的攻击者假设（），最弱的攻击目标（）
7. 密钥的三层管理中，生存周期最长的是（），负责加密和认证通信数据的是（）
8. 无中心的密钥分配要求（）有共享密钥，有中心的密钥分配要求（）有共享密钥
9. PKI 的主要目标是（）和（）绑定

简答题（6 个，30 分）

1. 对称密码体制和非对称密码体制的区别与各自的优缺点。
2. 分组秘密、消息鉴别码、公钥密码、数字签名分别保障了何种密码学安全属性。
3. 以 AES 为例，说明 Shannon 提出的三种对称密码设计的主要技术。
4. AES 的密钥扩展规则是？它比 DES 的密钥扩展复杂的原因是？
5. 简述 RSA 的密钥生成过程以及其安全参数要求。
6. 哈希碰撞是什么？举例说明数字签名中的哈希碰撞。

计算题（4 个，40 分）

1. 计算 $3^{10} \mod 7$
2. El Gamal，公钥为 p = 47, g = 5, y_B = 3
    1. k = 3 M = 4 求对应密文 C
    2. 若截获的 C =(31,1) 求对应明文 M
    3. 若截获的 C =(25,43) 求对应明文 M
3. DH，公钥为 p = 3, g = 5，Alice 和 Bob 想要相互通信

    1. Alice 的 a = 3，求发送给 Bob 的 A

    2. Bob 的 b = 5，求发送给 Alice 的 B

    3. 求共享密钥 K

    4. 说明完整的 DH 交换过程，要求抗中间人攻击及确认密钥一致性

4. Alice 和 Bob 想通过不安全信道与 Bob 安全通信，决定使用混合加密

    1. 如何分配或协商会话密钥

    2. 通信过程具体

    3. 这样的混合加密系统相较于纯对称加密和纯非对称加密的优势