中国科学技术大学857密码学与网络安全2023年考研真题

一、填空题（共42分）

1. 伪随机序列生成器有n个元件，则生成多长的序列_____，若其中只能异或，能出现多长序列。

2. 经过一定的置乱也可能出现明文，分组密码分组长度为3，_____次置乱出现明文，分组密码分组长度为6，_____次置乱出现明文，分组密码分组长度为7，_____次置乱出现明文。

3. $2^{2022} \bmod 11$ _____。

模3系2 模7系3 模11系3 最小正整数_____。

4. 通常意义上的AAA，分别指哪几种安全服务？_____、_____和_____。

5. 每个SA由一个三元组唯一地进行标识，该三元组为_____、_____和_____。

6. SSL中会话重用回复的消息中有用户发送的消息有同样的_____。

7. SSL在传输层_____协议之上。

8. CA中心的实体名称_____，认证身份的是_____，签发证书的是_____。

9. IPSEC会话重用的指示

二、单选题（共30分，每题3分）

1. 不属于数据流的主动攻击的是

2. Feistel密码结构描述正确的是

3. Alice获取证书包括RSA的公钥和私钥，并把公钥公开，然后谁可以计算模数？

4. 会话密钥的使用正确的是（什么时候更新）

5. D-H协议的解释，下来说法正确的是

6. WEP说法正确的

7. WLAN安全接入协议

8. Email 安全协议

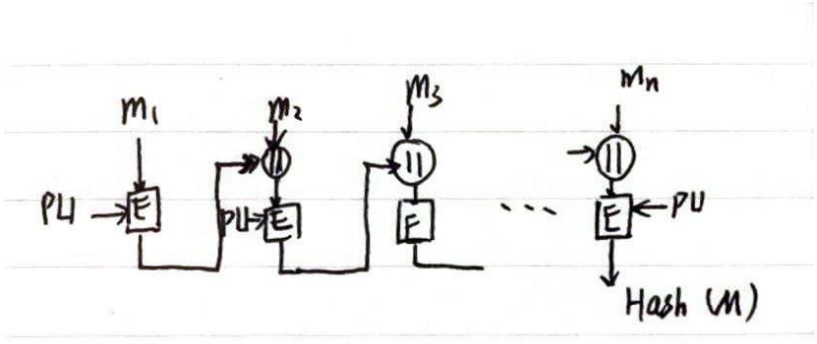
9. DNAT 的解释

10. hash 函数强碰撞性的解释

三、简答题（共 78 分）

1. DES：有一种加密方法是 DES(k1, k2, M) = (DES(k1, r), DES(k2, r⊕M))，问这种加密方法抗选择明文攻击的性能和代价。

2. Hash 函数：设计了一种用公钥加密的哈希函数，类似：



问这种哈希函数能否抗单向性攻击，抗弱碰撞和抗强碰撞。

3. RSA：把消息按字节分组，然后为了避免使明文中出现 0 或 1，给明文加上一个随机数 x=mi+r，然后加密传输。从密码学的角度评价一下这种方案。

4. DH 密钥交换：一道比较常规的计算题。

5. 数字信封如何形成，有什么作用？

6. 密钥派生在数据安全传输的作用，怎么进行秘钥派生。

7. 身份认证：一个用公钥密码和非私钥签名的认证方案，使得 A 向 B 证明自己的身份。

8. 隧道模式下 IPSEC ESP 隧道入口流程

9. PGP 在发送端的操作，如何保护本地的私钥，如何确定对方发送的消息使用的是哪个密钥对？

10. 自己设计一个方案，16 人的会议，如何协商会话秘钥，以及有人加入和退出时的操作。