1. 安全攻击分为哪两类，分别叙述并举例

主动和被动 信息内容泄露，流量分析

伪装，重放，消息内容的修改，拒绝服务

1. 安全服务分为哪五类，简要说明

认证，访问控制，数据保密性，数据完整性，抗抵赖性

1. 画出网络安全模型或网络安全访问模型，并简述其区别（一个是保证通信双方的安全，一个是保证主机不受外部系统的访问）
2. 计算安全和理论安全的含义

计算安全：价值，生命期

理论安全：不管有多少密文都无法攻破明文

1. DES算法的简单描述

初始置换；对右半部分做f,k;左右交换，对右半部分f,k2,IP逆置换

1. 一次一密为什么是最安全的，以及提供完全安全性两个基本难点、

因为即使有很多密文，解出了一个密钥，也没有办法去进行验证

密钥的生成和存储问题；密钥的分发和保护问题

1. Feistel密码的结构，以及具体实现依赖于？

是一种用来设计对称密码算法的常用结构，使用多轮；每轮都会有一个本轮密钥参与，将明文分为左右两半部分，复杂算法进行运算之后和左半部分进行异或后输出，并作为下一轮的左半部分，上一轮的左半部分作为下一轮的右半部分

依赖于：密钥长度；分组长度；轮函数；密钥生成函数；迭代轮数

1. AES产生的背景，以及AES和DES有什么不同(或提高)（AES数据结构四部分实现）

Des和3des够用，但是密钥长度比较短，分组比较短，安全性不够高

1. 为什么不使用2DES,使用3DES，

3DES是通过将3个DES算法串联，分别使用2个或3个密钥，密钥长度增长，算法的安全性大大增强了。2DES存在中间相遇攻击，不安全。

1. 3DES构造的方法，以及为什么使用两个密钥
2. 使用64位散列码，攻击者找到这样的消息为什么需要2^32次尝试，而不是2^63
3. 分组密码的各种工作模式的简要叙述；以及为什么要引入工作模式

引入工作模式是为了增强密码算法以及使具体的密码适用于具体应用

1. RC4简要叙述；以及设计流密码需要考虑的主要因素，和为什么RC4没有得到广泛应用
2. 什么是单向函数，什么是单向陷门函数
3. 端对端加密和链路加密，简要叙述其优缺点
4. 随机数的特征和一些用途
5. RSA算法的正确性和安全性证明，以及使用其构造密文，解出明文
6. RSA算法的可行性

RSA构造的关键是寻找大素数，可以先随机产生一个大的奇数，然后利用miller-Rabin算法来判断该奇数是宿舍的可能性，有素数存在性原理可以知道即使该数不是素数，在其周围存在素数的可能性也很大，所以是可行的。

1. Differ-hellman算法，简述算法+正确性+缺点
2. DSA和RSA数字签名的不同之处，以及RSA该如何改进
3. DSA的图要弄懂课本，自己可以画一下啊
4. RSA私钥的保密性，数字证书的构造机制如何实现公钥的真实性？
5. Hash函数的特性和用途
6. 比较对称加密，hash函数和mac消息鉴别码之间的区别和联系（从功能；构造方法；安全性；密钥）
7. 数字签名算法的分类
8. 服务器kerberos

产生背景，安全需求，协议的工作流程，对安全性有效性进行探讨

Diff-Hellmsn密钥交换算法

素数q

A和B希望交换密钥，那么用户A选择一个随机整数，Xa<q,并计算 YA=a（Xa）mod q

类似的 B也独立选择一个随机整数 Xb<q,并计算YB=a(^Xb)mod q

A和B保持其X是私有的，但对于另一方而言，Y是可以公开访问的，

用户A计算 K=YB(^YA)mod q 并将其作为密钥

用户B计算K=YA(^YB)mod q 并将其作为密钥，这两种计算所得到的结果是一样的，

攻击：由于Xa Xb是私有的，所以他只可以攻击 q,YA,YB,这样他必须求离散对数才能确定密钥。

密钥交换的安全性建立在下述事实之下：求关于素数的模素数幂运算相对容易，而计算离散对数却非常困难，对于大素数，求离散对数被认为是计算上不可行。