**信息安全**

判断选择 20-1  
填空 20-1  
名词解释 20-4  
简答 20-4  
问答 20-2

对称加密和非对称加密p15  
数字签名p36  
PKI   p67

PKI是基于公钥密码技术，支持公钥管理，提供真实性、保密性、完整性以及可追究性安全服务，具有普适性的安全基础设施。PKI的核心技术围绕建立在公钥密码算法之上的数字证书的申请、颁发、使用与撤销等整个生命周期进行展开，主要目的就是用来安全、便捷、高效地分发公钥，为用户建立一个安全的网络环境，保证网络上信息的安全传输。

数字证书(包含  名称，算法，等)  
ssl协议(两层协议，传输层，网络层)  
数字签名(方法)  
生物认证(个人独有特征可认证)  
防止冲撞最有效方法  
计算机病毒危害性表现在(破坏程序和数据)  
关于软件加密和硬件加密的比较(速度和兼容性等)  
计算机网络中实用的加密方式(点多点，等)  
计算机病毒特征(潜伏性等)  
目前使用的杀毒软件作用(全部杀灭病毒做不到)  
dos拒绝服务攻击  
软件缺陷服务攻击有效的防反方法(打补丁程序等)  
机器运行比较慢，可能收到什么攻击(yue)  
木马等属于什么类型  
攻击方法(ICMP泛洪，land，smurf，ping命令攻击的含义)  
VPN的定义  
  
 **填空**  
**1.网络安全属性**

机密性，完整性，真实性，可用性，可控性

**2.五大类安全服务(哪五大)**

**认证服务、访问控制服务、数据保密性服务、数据完整性服务，抗否认性服务**

**3.密码学发展三个阶段**

古典密码,近代密码，现代密码。

**4.密码学的分支**

密码编码学，密码分析学

**5.消息鉴别**

鉴别算法，鉴别协议，鉴别函数

**6.数字签名功能**

防止伪造，篡改，冒充

**7.pki认证模型**

CA（证书认证机构）、RA（证书注册机构）、KMC（密钥管理中心）。

**8.inset工作模式 ESP**

传输模式，隧道模式

**9.防火墙三种体系结构(屏蔽体系主机等)**

屏蔽主机防火墙

屏蔽子网防火墙系统

双重宿主主机

**10.vpn的类型**

[PPTP](https://baike.baidu.com/item/PPTP)、[L2TP](https://baike.baidu.com/item/L2TP)，[IPSec](https://baike.baidu.com/item/IPSec)

**安全策略**

物理安全策略，访问安全策略，防火墙控制，信息加密策略，网络安全管理策略  
  
大题  
**1.vpn定义 背**

虚拟专用网络(VPN)的功能是：在[公用网络](https://baike.baidu.com/item/%E5%85%AC%E7%94%A8%E7%BD%91%E7%BB%9C/12752077" \t "https://baike.baidu.com/item/_blank)上建立[专用网络](https://baike.baidu.com/item/%E4%B8%93%E7%94%A8%E7%BD%91%E7%BB%9C/795899)，进行[加密](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86/752748)通讯。

**2数字证书 背**

数字证书是指在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份。

**3 DES加密流程 背**

1. 初始置换IP
2. 16轮迭代
3. 初始逆置换IP^-1
4. f函数
5. 子密钥产生

**4.信息安全定义 背**

信息安全指信息系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，信息系统连续可靠正常地运行，信息服务不中断。

**5.数字签名定义 背**

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。

**6安全关联SA 背**

安全关联是单向的，在两个使用IPSec的实体间建立的逻辑连接，定义了实体间如何使用安全服务进行通信。

**7防火墙定义和功能和特点 背**

定义：防火墙是一个由软件和硬件组合而成的、起过滤和封锁作用的计算机或者网络系统。

特点：1.所有的通信，无论是从内部到外部还是从外部到内部的，都必须经过防火墙。2.只有被授权的通信才能通过防火墙，这些授权将在本地安全策略中规定。3.防火墙本身对于渗透必须是免疫的。

功能：访问控制功能。

2）内容控制功能。

3）日志功能。

4）集中管理功能。

5）自身安全和可用性。

**8 RSA流程**

1. 密钥生成
2. 加密运算
3. 解密运算

**9入侵检测过程 背**

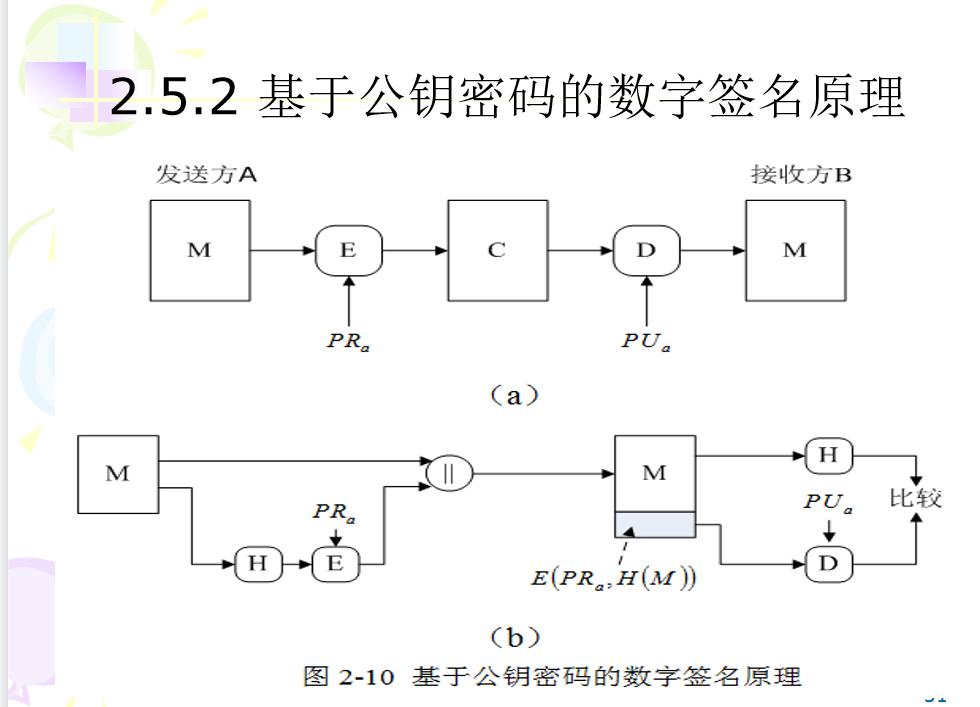
入侵检测的典型过程是：信息收集、信息预处理、数据的检测分析、根据安全策略做出响应。有的还包括检测效果的评估。

**10 pgp服务5种**

身份认证、信息保密、压缩、电子邮件的兼容性，分段  
11计算机病毒定义，特征   
**12蜜罐技术**

一种主动防御技术，是一种对攻击方进行欺骗的[技术](https://baike.baidu.com/item/%E6%8A%80%E6%9C%AF/13014499)，通过布置一些作为诱饵的主机、[网络服务](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%9C%8D%E5%8A%A1/9498645)或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

**13数字签名利用公钥实现(大题) 对称加密（古典密码，分组密码，序列密码），非对称加密（公钥密码）**



**14隧道技术概念**

隧道技术是一种通过使用[互联网络](https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91%E7%BB%9C/6908194" \t "https://baike.baidu.com/item/%E9%9A%A7%E9%81%93%E6%8A%80%E6%9C%AF/_blank)的[基础设施](https://baike.baidu.com/item/%E5%9F%BA%E7%A1%80%E8%AE%BE%E6%96%BD/3831695)在网络之间传递数据的方式。  
  
  **选择2**  
置换和代换定义

pki与权限无关

**ca功能(生成，管理，等)**

制定并发布本地CA策略。但本地策略只是对上级CA策略的补充，而不能违背。

对下属各成员进行身份认证和鉴别。

发布本CA的证书，或代替上级CA发布证书。

产生和管理下属成员的证书。

证实RA的证书申请，返回证书制作的确认信息，或返回已制作的证书。

接收和认证对所签发证书的撤销申请。

产生和发布所签发证书和CRL。

保存证书、CRL信息、审计信息和所制定的策略。

数字证书包含内容  
对安全的认证形式(卡，用户名，dna等)  
arp期协议  
攻击方式(被动攻击类型:采集流量等 )  
清理病毒最有效方法(格式化)  
木马和病毒不同点(木马无法自己复制，需要潜伏到其他的xx)  
入侵检测系统步骤IDS(收集信息，等)  
ping命令攻击ddos(拒绝服务攻击)  
数据完整性定义  
防范攻击方法(选不行的 防火墙不能)  
  
  **填空**  
  
明文，密文，加密算法，解密算法，密钥五个组成

认证(物理认证，身份认证)

IPsec体系结构(esp协议，ah协议，加密算法，认证算法，密钥管理)

计算机病毒分类（恶意代码）

计算机病毒

木马

蠕虫