# 第4章：计算机网络与信息安全

【考点梳理】

## 【计算机网络】

### 考点1、开放系统互连参考模型OSI（★★）

#### 【考法分析】

##### 本知识点的主要考查形式有：给定物理设备判定所属层次；或给定传输单位，判断其所属层次；或给定相关功能描述，判断其所属层次。

#### 【要点分析】

##### 

#### 【备考点拨】

##### 掌握OSI七层模型各个层次对应的主要功能、传输单位、主要物理设备。

### 考点2、TCP/IP协议族（★★★★）

#### 【考法分析】

##### 本知识点主要考查的形式有：给定协议，判断其基于TCP或UDP协议基础；或给定协议，判断其所属层次；或给定端口号，判断其对应协议。

#### 【要点分析】

##### 1、TCP/IP协议层次模型

##### 

##### 2、常见协议功能和端口号：

##### POP3：110端口，邮件收取

##### SMTP：25端口，邮件发送

##### FTP：20数据端口/21控制端口，文件传输协议

##### HTTP：80端口，超文本传输协议，网页传输

##### DHCP：67端口，IP地址自动分配

##### SNMP：161端口，简单网络管理协议

##### DNS：53端口，域名解析协议，记录域名与IP的映射关系

##### TCP：可靠的传输层协议

##### UDP：不可靠的传输层协议

##### ICMP：因特网控制协议，PING命令来自该协议

##### IGMP：组播协议

##### ARP：地址解析协议，IP地址转换为MAC地址

##### RARP：反向地址解析协议，MAC地址转IP地址

#### 【备考点拨】

##### 1、掌握TCP/IP协议族的分层模型；

##### 2、掌握常见协议的功能和对应端口号。

### 考点3、IP地址与子网划分（★★★★★）

#### 【考法分析】

##### 本知识点的考查形式主要有：给定网络号，求取子网划分的网络号个数和主机号个数；或给定多个子网，求取路由汇聚后的网络号、主机数量等。

#### 【要点分析】

##### 1、相关概念：

##### （1）IP地址分类：A类地址（网络号8位，0开始），B类地址（网络号16位，10开始），C类地址（网络号24位，110开始），D类地址（组播地址，1110开始），E类地址（保留地址，11110开始）。

##### 2、子网划分：将一个网络划分成多个子网（取部分主机号当子网号）。

##### 3、路由汇聚：将多个网络合并成一个大的网络（取部分网络号当主机号）。

#### 【备考点拨】

##### 1、掌握IP地址分类；

##### 2、掌握子网划分和路由汇聚的计算。

### 考点4、网络规划与设计（★）

#### 【考法分析】

##### 本知识点的考查形式有：给定一些描述，判断所属设计原则；或给定一些描述，判断所属的设计层次，或给定层次，判断其功能描述正误。

#### 【要点分析】

##### 

#### 【备考点拨】

##### 1、了解网络规划原则；

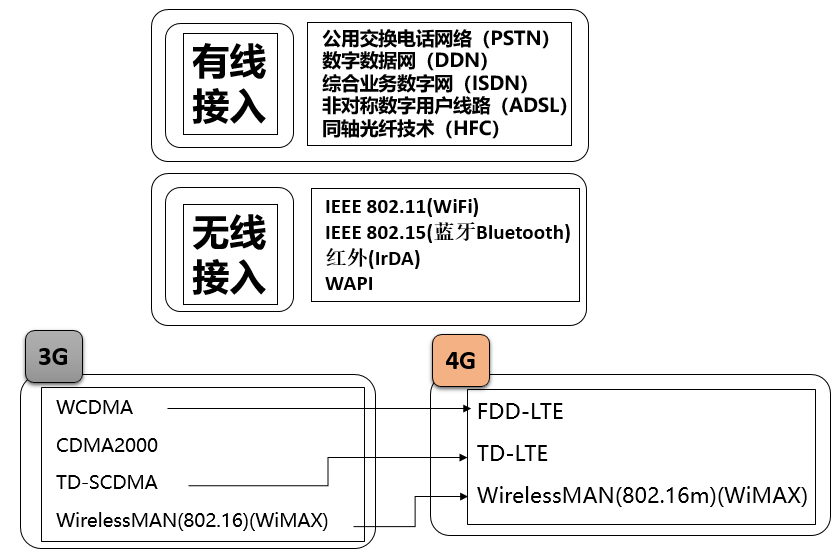
##### 2、掌握核心层、接入层、汇聚层的功能和区别。

### 考点5、3G/4G标准（★★）

#### 【考法分析】

##### 本知识点的考查形式有：对3G/4G标准的分类，给定场景描述找到所属的协议。

#### 【要点分析】



#### 【备考点拨】

##### 了解相关协议标准的应用场景。

### 考点6、HTML语言（★★）

#### 【考法分析】

##### 本知识点的考查形式主要是给定一些要求，选择使用的标签，或给定标签，选择对应的描述。

#### 【要点分析】

##### 

#### 【备考点拨】

##### 1、了解常用的HTML标签。

## 【信息安全】

### 考点7、对称加密与非对称加密（★★★）

#### 【考法分析】

##### 本知识点的考查形式有：区分对称加密和非对称加密算法；根据给出的描述判断正误；根据对称加密和非对称加密算法的特点区分选择算法；或根据情景描述，确定在某个阶段使用的秘钥。

#### 【要点分析】

##### 1、对称加密（又称为私人秘钥加密/共享秘钥加密）：加密与解密使用同一秘钥。

##### 特点： 1、加密强度不高，但效率高； 2、密钥分发困难。

##### （大量明文为了保证加密效率一般使用对称加密）

##### 常见对称密钥加密算法：DES、 3DES(三重DES)、 RC-5、IDEA、AES算法。

##### 2、非对称加密（又称为公开密钥加密）：密钥必须成对使用（公钥加密，相应的私钥解密）。

##### 特点：加密速度慢，但强度高。

##### 常见非对称密钥加密算法： RSA、ECC

#### 【备考点拨】

##### 1、掌握对称加密和非对称加密机制的加密过程。

##### 2、记住对称加密和非对称加密的加密算法。

##### 3、了解对称加密和非对称加密的特点和适用情景。

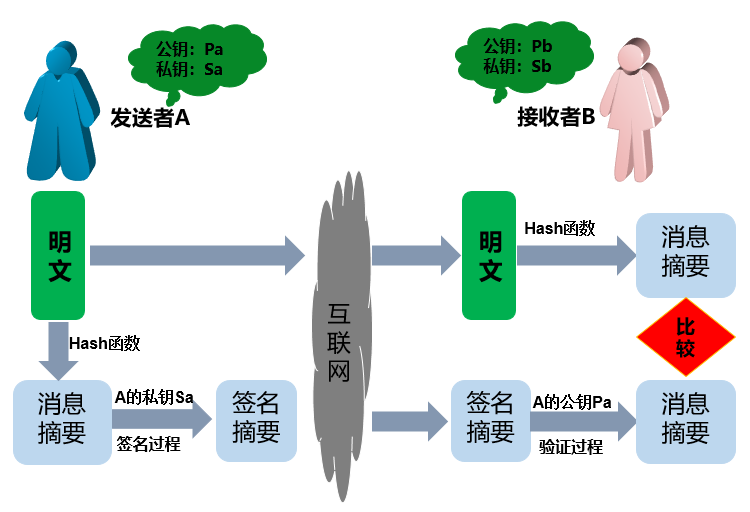
### 考点8、信息摘要与数字签名（★★）

#### 【考法分析】

##### 本知识点的考查形式主要有：根据情景描述，判断某个阶段所使用的秘钥及其所属的对象；或签名、认证相关的概念描述判断正误；或信息摘要相关的概念和算法识别。

#### 【要点分析】

##### 1、数字签名的过程如下图所示（发送者使用自己的私钥对摘要签名，接收者利用发送者的公钥对接收到的摘要进行验证）：



##### 2、常见的摘要算法：MD5(128位)，SHA(160位)。

#### 【备考点拨】

##### 1、掌握数字签名机制的过程；

##### 2、了解摘要的机制；

##### 3、了解常见的摘要算法。

### 考点9、数字证书（★★）

#### 【考法分析】

##### 本知识点常见的考查形式有：给定情景描述，判断数字证书中CA签名的作用；判断数字证书中公钥的作用；数字证书相关的概念描述判断正误。

#### 【要点分析】

##### 1、数字证书的内容包括：CA签名、用户信息（用户名称）、用户公钥等。

##### 2、CA签名验证数字证书的可靠性。

##### 3、用户公钥：客户端利用证书中的公钥加密，服务器利用自己的私钥解密。

#### 【备考点拨】

##### 1、掌握PKI的基本机制流程。

##### 2、掌握数字证书组成部分的作用。

### 考点10、网络安全协议（★★★）

#### 【考法分析】

##### 本知识点的考查形式主要有：判断协议所属的层次；HTTPS协议、PGP协议、SET协议的描述判断正误。

#### 【要点分析】

##### 1、安全协议分层如图所示：

##### 

##### 2、HTTPS协议是HTTP协议与SSL协议的结合，默认端口号443。

##### 3、PGP协议是邮件安全协议。

##### 4、SET协议是电子商务安全协议，涉及电子交易安全。

#### 【备考点拨】

##### 1、掌握协议分层；

##### 2、了解HTTPS、SSL、PGP、SET协议的作用，重点掌握HTTPS协议。

### 考点11、防火墙技术与网络攻击（★★★）

#### 【考法分析】

##### 本知识点的考查形式主要有：对于防火墙技术的描述判断正误；给定一些描述判断所属的网络攻击分类或具体的网络攻击方式（主要有拒绝服务、流量分析、重放等）。

#### 【要点分析】

##### 1、网络攻击分类如下图所示：

##### 

##### 2、常见的攻击行为

##### （1）拒绝服务：攻击者利用众多傀儡主机向服务器发送服务请求，导致服务器资源被耗尽，无法提供正常的服务，向其他访问者发送拒绝服务应答。

##### （2）重放攻击：攻击者抓取向服务器发送的有效数据包，并利用此数据包不断地向服务器发送，导致服务器一直应答此数据包，从而崩溃。

##### （3）业务流分析：通过长期监听被攻击者的数据流，从而分析出相关业务流，可以依此了解被攻击者的一些倾向，常见的广告推送就是建立在业务流分析基础上的。

##### 3、常见的防御手段（可以结合使用）

##### （1）防火墙技术：主要了解它的机制是防外不防内，对于DMZ非军事区主要放置应用服务器（如邮件服务器，WEB服务器）。

##### （2）漏洞扫描：入侵者可以利用系统漏洞侵入系统，系统管理员可以通过漏洞扫描技术，及时了解系统存在的安全问题，并采取相应措施来提高系统的安全性。

##### （3）入侵检测IDS：基于数据源的分类-审计功能、记录安全性日志。基于检测方法-异常行为检测。

#### 【备考点拨】

##### 1、了解常见的网络攻击手段和其分类；

##### 2、了解防火墙技术。

### 考点12、计算机病毒与木马（★★★）

#### 【考法分析】

##### 本知识点的考查形式主要有：给定一些关于病毒、木马的描述，判断正误；或给定一些描述，指出病毒、木马的分类。

#### 【要点分析】

##### 1、常见的病毒、木马命名：

##### 系统病毒（前缀：Win32、PE、W32，如：KCOM——Win32.KCOM）

##### 蠕虫病毒（如：恶鹰——Worm.BBeagle）

##### 木马病毒、黑客病毒（如：QQ消息尾巴木马——Trojan.QQ3344）

##### 脚本病毒（如：红色代码——Script.Redlof）

##### 宏病毒（如：美丽莎——Macro.Melissa）

##### 后门病毒（如：灰鸽子——Backdoor.Win32.Huigezi）

##### 病毒种植程序病毒（冰河播种者——Dropper.BingHe2.2C）

##### 破坏性程序病毒（杀手命令——Harm.Command.Killer）

##### 玩笑病毒（如：女鬼——Jioke.Grl ghost）

##### 捆绑机病毒（如：捆绑QQ——Binder.QQPass.QQBin）

##### 2、常见的病毒分类：

##### （1）文件型计算机病毒感染可执行文件（包括EXE和COM文件）。

##### （2）引导型计算机病毒影响软盘或硬盘的引导扇区。

##### （3）目录型计算机病毒能够修改硬盘上存储的所有文件的地址。

##### （4）宏病毒感染的对象是使用某些程序创建的文本文档、数据库、电子表格等文件。

##### 3、病毒的特性：计算机病毒的特性包括隐蔽性、传染性、潜伏性、触发性和破坏性等

#### 【备考点拨】

##### 1、掌握病毒的分类及相关特性；

##### 2、掌握常见病毒的命名，能够区分；