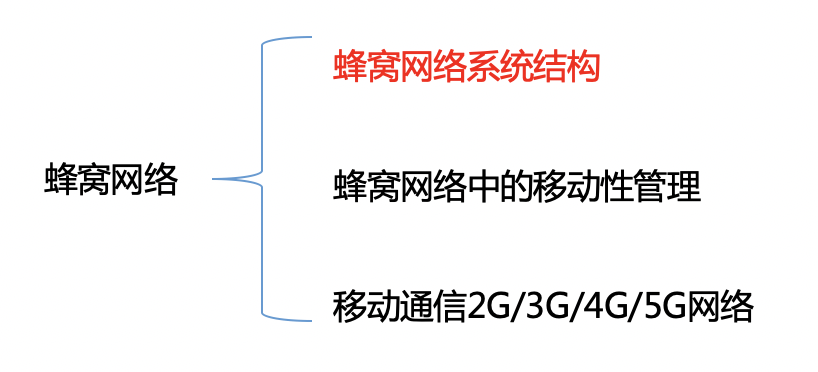
**《计算机网络原理》第十五节课官方笔记**

目录

1. 思维导图
2. 本章知识点
3. 配套练习题

**7.4 蜂窝网络**



【知识点1】蜂窝网络的系统结构

一、蜂窝网络。

1、小区(Cell)：蜂窝网覆盖的区域被分成的。

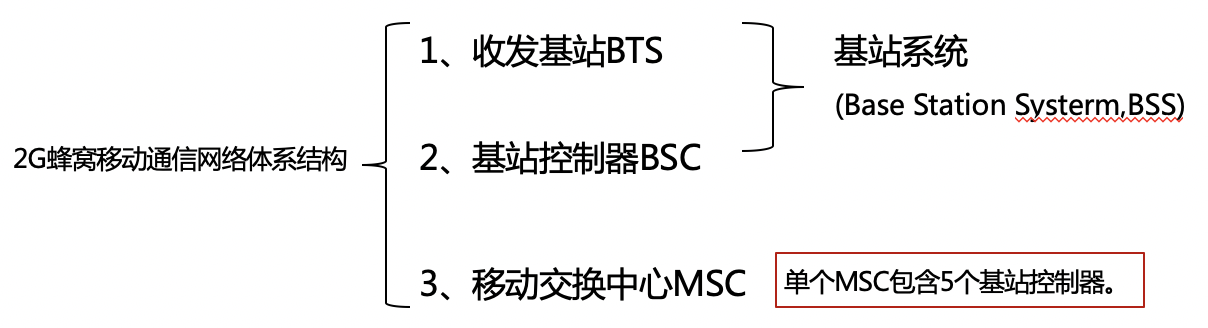
2、蜂窝：小区的地理覆盖区域。

二、以2G蜂窝移动通信网络为例的蜂窝网络体系结构

1、收发基站(Base Transceiver Station,BTS)：负责向小区内的移动站点发送或接收信号。

2、基站控制器(Base Station Controller,BSC )：服务于收发基站，为用户分配BTS无线信道、执行寻呼， 执行移动用户的切换。

3、移动交换中心(Mobile Switching Center , MSC)：在用户鉴别和账户管理以及呼叫建立和切换中起决定性作用。



三、蜂窝网络发展历史

1、第一代蜂窝移动通信(1G)：淘汰

2、第二代蜂窝移动通信(2G)：

GSM(Global System for Mobile Communication)系统；

短信服务；

GPRS(General Packet Radio Service , 通用分组无线服务技术)；

EDGE(Enhanced Data Rate for GSM Evolution ,增强型数据速率GSM演进技术）

3、3G，4G，5G

【知识点2：蜂窝网络中的移动性管理】

一、GSM标准采用的是间接路由选择方法管理移动性。

1、GSM的归属网络维护一个归属位置注册器(Home Location Register,HLR)的数据库：每个用户的永久蜂窝电话号码，用户个人信息，用户当前的位置信息。

2、GSM的被访网络维护一个访问位置注册器(Visitor Location Register,VLR)的数据库：为每一位当前在其服务网络的移动用户提供一个表项。

二、GSM通信过程

1、通信者拨打移动用户的电话号码。

2、归属移动交换中心收到该呼叫，查询归属位置注册器来确定移动用户的位置。并确定移动用户的漫游号码。

3、漫游号码确定后，归属移动交换中心通过网络呼叫被访网络的移动交换中心，被访网络的移动交换中心呼叫移动用户。

【知识点3：移动通信2G/3G/4G/5G网络】

一、2G网络

1、GSM系统是第二代移动电话系统的开端。

2、GSM业务，可以分为承载业务、电信业务、附加业务三大类。

3、GSM系统采用的是FDMA和TDMA混合接入的方式。

二、3G网络

1、国际电信联盟(ITU)提出并研究。

国际电信联盟(ITU)在2000年确定了WCDMA、CDMA2000和TD-SCDMA三大技术标准。

2、3G是采用宽带CDMA技术的通信系统。

三、4G/LTE网络

1、3GPP组织在2004年开始长期演进(Long Term Evolution,LTE)。在2008年9月开启LTE-Advanced项目。

2、4G特点：高速率传输，智能化，业务多样化，无缝接入，后向兼容，经济

四、5G网络

5G技术目的：构建网络社会。

网络社会：超高速率传输，足超高容量、超可靠性、随时随地可接入性。

**7.5 移动IP网络**

一、移动IP(Mobile IP)：国际互联网工程任务组（The Internet Engineering Task Force，IETF）开发，允许计算机移动到外地时，任然保持其原来的IP地址。

二、移动IP标准：代理发现；向归属代理注册，数据报的间接路由选择。

**【知识点1】代理发现**

一、代理发现：当移动IP站点到达一个新网络时，移动结点都必须知道相应的外部代理或归属代理的身份。

代理发现的实现方式：代理通告、代理请求。

1、代理通告(agent advertisement)：代理周期性的广播一个类型字段为9(路由器发现)的ICMP报文。

**【知识点2】向归属代理注册**

1. 移动 IP 定义了移动结点或外部代理向一个移动结点的归属代理注册或注销COA所使用的协议。一旦某个移动IP结点收到一个 COA，则该地址必须向归属代理注册。
2. 注册过程

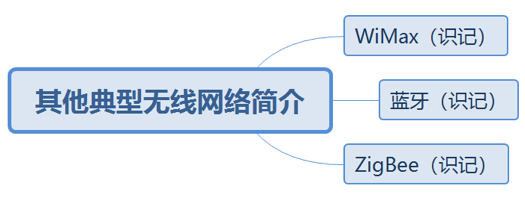
1、当收到一个外部代理通告后，移动结点向外部代理发送一个移动IP注册报文

2、外部代理收到注册报文并记录移动结点的永久IP地址，分配一个COA。并且把注册请求发送给归属代理。

3、归属代理接收注册请求并检查真实性和正确性

4、外部代理接收注册应答，然后将其转发给移动结点

**7.6 其他典型无线网络简介**



【知识点1】Wi Max

一、全球微波互联接入(World Interoperability for Microwave Access , Wi Max)：IEEE 802.16标准，宽带无线标准。

1、Wi Max优势：

更远的传输距离，可以达到50km

更高速的宽带接入，最高可达300Mbit/s 。

2、Wi Max劣势：

不能支持用户在移动过程中无缝切换、

产业基础薄弱、和传统的蜂窝网络无法完全兼容。

【知识点2】蓝牙

1、IEEE 802.15.1标准：无线个人区局域网(Wireless Personal Area Network,WPAN)标准。

2、工作在全球通用的2.4GHZ的频段。

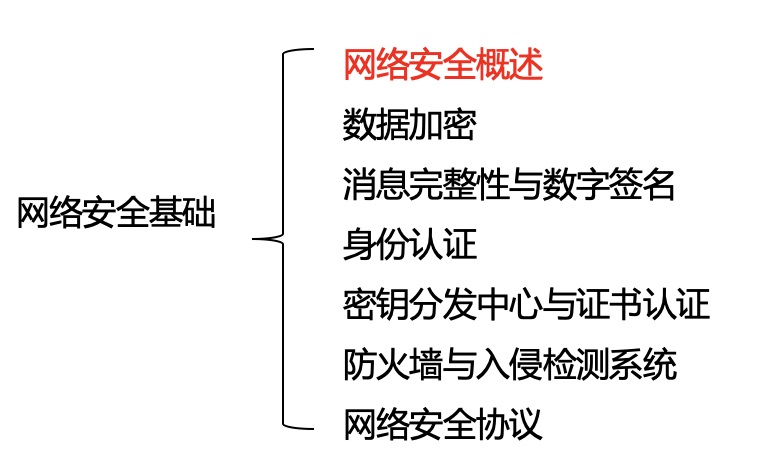
3、小范围，低功率、低速率和低成本运行。 （一小三低）

【知识点3】ZigBee

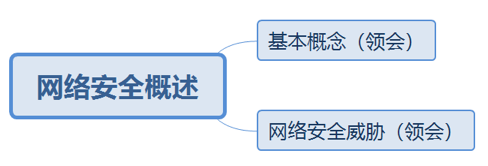
一、 IEEE 802.15.4标准：第二个个人区域网络标准。

1、低功率、低数据速率、低工作周期。

第8章 网络安全基础



**8.1 网络安全概述**



【知识点1】基本概念

一、网络安全通信需要的基本属性：

1、机密性：只有发送方和接收方能理解报文内容。

2、消息完整性：消息未被篡改，发生篡改一定会被检测到。

3、可访问性与可用性：对授权用户提供有效服务。

4、身份认证：双方确认彼此的真实身份。

二、典型的网络安全威胁：

1、报文传输方面：窃听、插入、假冒、劫持等安全威胁。

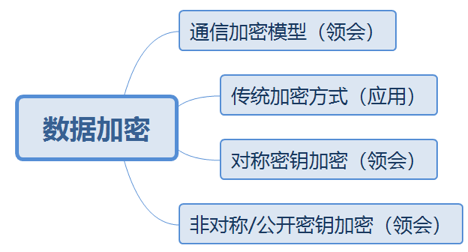
2、拒绝服务DoS以及分布式拒绝服务DDoS。

3、映射：Namp是国外广为使用的端口扫描工具之一。

4、分组“嗅探”：Wireshark是一个典型的分组嗅探软件。

5、IP欺骗

**8.2数据加密**



【知识点1】通信加密模型

一、

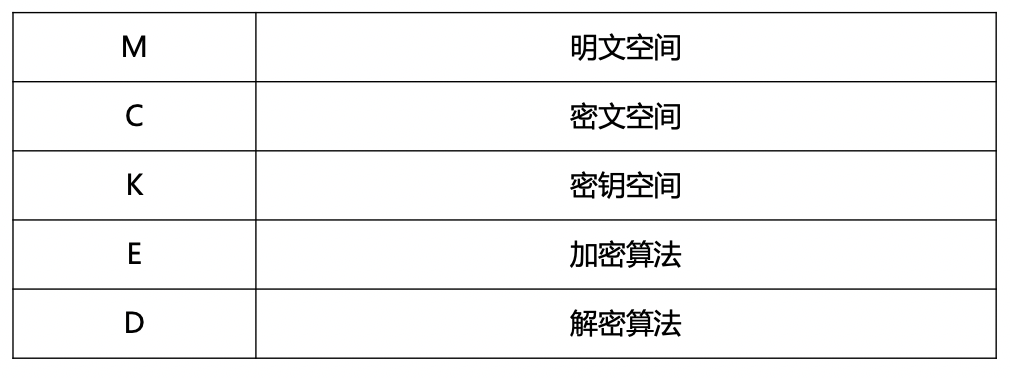
明文：未加密的消息。

密文：被加密的消息。

加密：明文转变为密文的过程。

解密：密文转变为明文的过程。

二、



三、根据密码体制的特点以及出现的先后时间可以将密码方式分类为：

1、传统加密方式：替代密码；换位密码

2、对称密钥加密

3、公开密钥加密（非对称秘钥加密）

【知识点2】传统加密方式

一、替代密码

凯撒密码是替代密码的典型应用。

例：如果对明文“bob,I love you,Alice”，利用k=3的凯撒密码加密，得到的密文是什么？

解：明文：“bob,I love you,Alice”

密文：“ere,L oryh brx,Dolfh”。

二、换位密码，又称置换密码

根据一定规则重新排列明文，以便打破明文的结构特性。只改变明文结构，不改变内容。

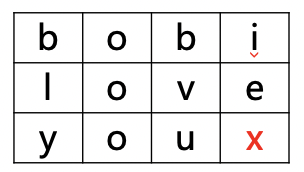
换位密码：列置换密码和周期置换密码

例：假设采用密钥K=nice的列置换密码，对明文“bob i love you”进行加密，加密得到的密文是什么？

**第一步：确定密钥长度（几个字母），并且确定字母在26个字母中的顺序。**

密钥K=nice，则密钥长度n=4，密钥的字母顺序为（ 4,3,1,2 ）

**第二步：将明文按顺序横向排列展开，具体展开有几列，由密钥长度决定。**密钥长度是4，就是有4列。



**第三步：输出顺序确定。看密钥字母顺序，和排列好后的表格对应。**

密钥K=nice，则密钥长度n=4，密钥的字母顺序为（ 4,3,1,2 ）



则，密文为bvu iex ooo bly。

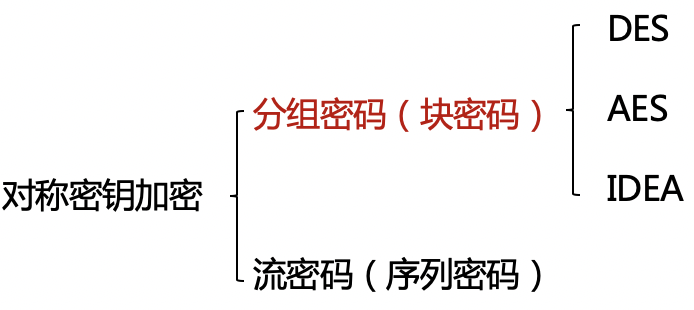
【知识点3】对称密钥加密

一、现代密码学可以分为：对称密钥密码和非对称密钥密码。

对称密钥密码：加密密钥和解密密钥是相同的。

非对称密钥密码：加密密钥和解密密钥是不同的。

二、对称密钥密码



三、DES加密算法

1、加密过程：使用56位的密钥，明文为64位分组序列，共进行16轮的加密。

2、三重DES：使用两个密钥，执行三次DES算法，密钥长度达到112位。

加密过程：加密(K1)-解密(K2)-加密(K1)

解密过程：解密(K1)-加密(K2)-解密(K1)

四、AES加密算法：高级加密标准(Advanced Encryption Standard,AES)

1、AES加密过程涉及4种操作：字节替代、行移位、列混淆、轮密钥加。

2、密钥长度：128/192/256位

3、特点：

分组长度和密钥长度均可变；循环次数允许在一定范围内根据安全要求进行修正；安全、效率、易用、灵活；抗线性攻击和抗差分攻击的能力大大增强；如果1秒暴力破解DES，则需要149万亿年破解AES。

五、IDEA加密算法

国际数据加密算法(International Data Encryption Algorithm,IDEA)

广泛应用在安全电子邮件PGP中。密钥长度为128位。

**【知识点4：非对称/公开密钥加密】**

一、非对称密钥密码(公开密钥密码、公钥密码)。

1、通信双方都有两个密钥：

公钥(任何人都可以得到)

私钥(只有自己知道)

2、典型的公开密钥加密算法：Diffie-Hellman算法和RSA算法。

3、Diffie-Hellman算法：基于数学中素数原根理论。

RSA算法：基于数论设计，安全性建立在大数分解的难度上。应用比较广泛，安全性高。

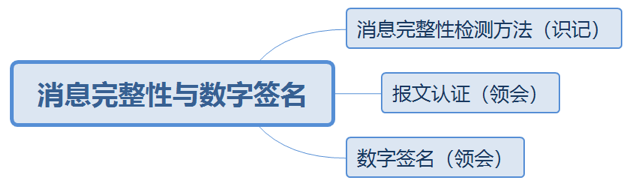
二、公开密钥密码加密过程：

Alice给Bob通信：

1、Alice用Bob的公钥加密明文，发送。

2、Bob收到密文后，用自己的私钥解密得到明文。

8.3 消息完整性与数字签名



【知识点1】消息完整性检测方法

一、报文/消息完整性(message integrity)，也称为报文/消息认证

1、证明报文确实来自声称的发送方；

2、验证报文在传输过程中没有被篡改；

3、预防报文的时间、顺序被篡改；

4、预防报文持有期被篡改；

5、预防抵赖。

二、消息完整性检测方法：用散列函数，对报文进行散列化。

1、密码散列函数的特性：

1）散列函数算法公开

2）快速计算

3）对任意长度报文进行散列产生定长输出

4）对于任意报文无法预知其散列值（抗弱碰撞性）

5）不同报文不产生相同的散列值（抗强碰撞性）

6）单向性

2、典型的散列函数

第一种：MD5(Message-Digest Algorithm 5)：128位散列值。

第二种：SHA-1：160位散列值。

【知识点2】报文认证

一、消息完整性检测重要目的：报文认证。

报文认证：消息的接受者能够检验收到的消息是否是真实的方法。

报文认证的目的有两个:1、消息源的认证;2、消息的认证。

二、对报文m应用散列函数H，得到固定长度的散列码，称为报文摘要，记为H(m)。报文摘要可以作为报文m的数字指纹(fingerprint)

**三、简单报文验证**

1、发送方对报文m应用散列函数，得到固定长度的散列码，获得报文摘要h，将扩展报文(m,h)发送给接收方。

2、接收方收到扩展报文后，提取出报文m和报文摘要h，同样对报文m应用散列函数H获得新的报文摘要H(m)，将H(m)和h比较。

3、若相同，报文认证成功。否则报文认证失败。

**四、报文认证码MAC（Message Authentication Code）**

1、发送方和接收方共享一个认证密钥s，发送方对报文m和认证密钥s应用散列函数H得到报文认证码h，将扩展报文(m,h)发送给接收方。

2、接收方收到扩展报文后，提取出报文m和报文认证码h，对报文m和认证密钥s应用散列函数H获得新的报文认证码H(m+s)，将H(m+s)与h比较。

3、若相等，则报文认证成功。否则失败。

【知识点3】数字签名

1. 数字签名：在公钥密码体制中，一个主体使用自己的私钥加密消息，得到的密文使用该主体的公钥解密来恢复成原来的消息。如此生成的密文对该消息提供认证服务。
2. 数字签名应满足：

1、接收方能够确认发送方的签名，但不能伪造。

2、发送方发出签名的消息给接收方后，就不能再否认他所签发的消息。

3、接收方对已收到的签名消息不能否认，有收报认证。

4、第三者可以确认收发双方之间的消息传送，但不能伪造这一过程

三、简单数字签名

1、Bob利用自己的私钥对报文m加密，创建签名报文。将扩展报文(报文，签名报文)发送给Alice。

2、Alice收到报文m以及签名报文。利用Bob的公钥解密签名报文，并检验解密后的签名报文和报文m是否一致。

3、若一致，则签名m的一定是Bob的私钥。

四、签名报文摘要

1、Bob对报文m应用散列函数H生成报文摘要H(m)，然后Bob通过其私钥对报文摘要进行加密生成加密的报文摘要，将扩展报文(报文，加密的报文摘要)发送给Alice。

2、Alice收到报文m以及加密的报文摘要。Alice利用Bob的公钥解密加密的报文摘要，并对m应用散列函数生成新的报文摘要。

3、如果两者一致，则签名报文m的一定是Bob的私钥。

**8.4 身份认证**

身份认证：身份鉴别。一个实体经过计算机网络向另一个实体证明其身份的过程。

1、基于共享对称密钥的身份认证；

2、基于公开密钥的身份认证；

**3、一次性随机数：避免重放攻击**

一、基于共享对称密钥的身份认证

1、Alice向Bob发送报文“我是Alice”

2、Bob选择一个一次性随机数R，然后把这个值发送给Alice

3、Alice使用她与Bob共享的对称秘密密钥加密这个一次性随机数，然后把加密的一次性随机数发回给Bob。

4、Bob解密收到的报文。

二、二、基于公开密钥的身份认证

1、Alice向Bob发送报文“我是Alice”

2、Bob选择一个一次性随机数R，然后把这个值发送给Alice

3、Alice使用她的私钥来加密R，然后把加密的一次性随机数发回给Bob。

4、Bob向Alice索要她的公钥。

5、Alice向Bob发送自己的公钥。

6、Bob利用Alice的公钥解密收到的报文。

**8.5 密钥分发中心与证书认证机构**



【知识点1】密钥分发中心

一、对称密钥分发的典型解决方案：通信各方建立一个大家都信赖的密钥分发中心(Key Distribution Center,KDC)，解决对称密钥安全可靠的分发。

二、方式一：通信发起方生成会话密钥

1、Alice和Bob进行保密通信。Alice随机选择一个会话秘钥。用Alice和KDC之间长期的共享密钥加密会话秘钥，发送给KDC。

2、KDC得到后，解密获得会话密钥，以及所希望通信方Bob。KDC利用其和Bob的长期共享密钥加密密钥，发送给Bob。

3、Bob解密，获得会话秘钥，并且得知期望和自己通信的是Alice。

三、方式二：KDC为Alice、Bob生成通信的会话秘钥

1、Alice在希望和Bob通信时，首先向KDC发送请求消息。

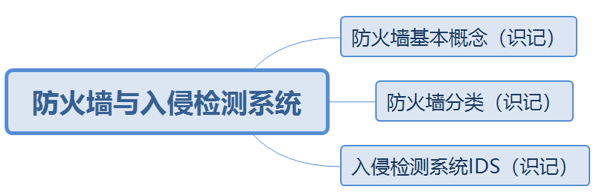
2、KDC收到请求消息后，随机选择一个会话秘钥，并将会话秘钥分别用和Alice、Bob的长期共享密钥加密，再分别发送给Alice、Bob。

3、Alice、Bob收到KDC的密文后，分别解密，获得会话秘钥。

【知识点2】证书认证机构

1. 认证中心（Certification Authority,CA）：将公钥与特定的实体绑定。
2. CA的作用：
3. CA可以证实一个实体的真实身份。
4. 一旦CA验证了某个实体的身份，CA会生成一个把其身份和实体的公钥绑定起来的证书，其中包含该实体的公钥及其全局唯一的身份识别信息等，并由CA对证书进行数字签名。

**8.6 防火墙与入侵检测系统**



【知识点1】防火墙

1. 防火墙：能够隔离组织内部网络与公共互联网，允许某些分组通过，而阻止其他分组进入或离开内部网络的软件、硬件或者软件硬件结合的一种设施。
2. 防火墙的分类

1、无状态分组过滤器:典型部署在内部网络和网络边缘路由器上的防火墙。路由器逐个检查数据报，根据访问控制表(Access Control Lists ,ACL)实现防火墙规则。

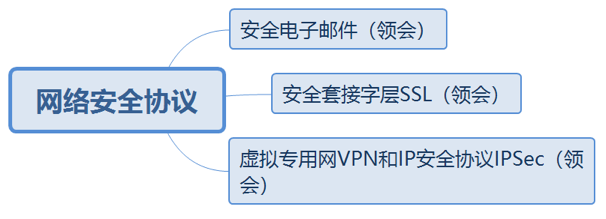
2、有状态分组过滤器:跟踪每个TCP连接建立、拆除，根据状态确定是否允许分组通过。

3、应用网关：应用网关实现授权用户通过网关访问外部网络的服务。

【知识点2】入侵检测系统(Intrusion Detection System,IDS)

一、IDS：当观察到潜在的恶意流量时，能够产生警告的设备或系统。

**8.7 网络安全协议**



【知识点1】安全电子邮件

一、电子邮件对网络安全的需求：

1、机密性

2、完整性

3、身份认证性

4、抗抵赖性

二、安全电子邮件标准：PGP标准(Pretty Good Privacy)

1、PGP提供的服务：

邮件加密；报文完整性；数字签名；

加密算法：公钥加密算法(如RSA)、对称加密算法(如3DES)、散列算法(如SHA-1)

【知识点2】安全套接字层SSL

一、一般Web服务器越强大，包含安全漏洞的概率越高。Web浏览器也会遇到各种各样的安全威胁。普通Web应用的应用层数据，在传输过程中都已明文形式传输，可能受到攻击。

二、在电子商务背景下，提出HTTP安全电子商务交易协议；

在传输层之上构件一个安全层：

**安全套接字层(Secure Socket Layer,SSL)**

传输层安全(Transport Layer Security,TLS)

三、SSL可以提供的服务

机密性、完整性、身份认证等安全服务。

四、SSL协议栈(协议的总和)：SSL是介于TCP和HTTP等应用层协议之间的一个可选层，大多数应用层协议直接建立在SSL协议之上，SSL是两层协议。



1、SSL握手协议：在握手过程中需要用到SSL握手协议、SSL更改密码规格协议、SSL警告协议。

主要作用：协商密码组和建立密码组；服务器认证与鉴别和客户认证与鉴别

2、SSL更改密码协议：通信双方修改密码组，标志着加密策略的改变。

3、SSL警告协议：为对等实体传递SSL警告或终止当前连接。

包含两个字段：警告级别和警告代码。

4、SSL记录协议：描述了信息交换过程中的消息格式，前面3个协议需要记录协议进行封装与传输。

【知识点3】虚拟专用网VPN和IP安全协议IPSec

一、虚拟专用网VPN

建立在公共网络上的安全通道，是用户通过公用网络建立的临时的、安全的连接。 实现远程用户、分支机构、业务伙伴等与机构总部网络的安全连接，从而构建针对特定组织机构的专用网络。

**虚拟专用网最重要的特点就是虚拟。**

虚拟专用网一般指的是构建在Internet上能够自我管理的专用网络

**关键技术：隧道技术，如IPSec。**

二、VPN涉及的关键技术：

1、隧道技术；2、数据加密；3、身份认证；

4、密钥管理；5、访问控制；6、网络管理。

三、隧道：通过Internet提供的点对点的数据传输的安全通道。

通过数据加密保证安全，数据进入隧道时，由VPN封装成IP数据报，通过隧道在Internet上传输；离开隧道后，进行解封装，数据便不再受VPN保护。

四、IPSec体系简介

1、IPSec是网络层使用最广泛的安全协议，但IPSec不是一个单一的协议，而是一个安全体系。

主要包括：

封装安全载荷协议( ESP)

认证头( AH)协议

安全关联(SA)

密钥交换与管理(IKE)：IPsec唯一的密钥管理协议

**这其中，ESP和AH是IPSec的核心。**

2、IPSec传输模式：传输模式和隧道模式

传输模式：主机模式。IPSec数据报的发送和接收都由端系统完成。

隧道模式：将IPSec的功能部署在网络边缘的路由器上，路由器之间建立安全隧道，数据报在其中封装传输。

3、传输模式和协议组合

传输模式AH

隧道模式AH

传输模式ESP

**隧道模式ESP：最广泛和最重要的IPSec形式。**

三、配套习题

1、下列关于2G/3G/4G/5G移动通信系统的特点说法错误的是（ B ）。

A:2G除了基本的语音通信，还能提供短信服务

B:3G中最关键的技术是多媒体技术

C:4G技术具有高速率传输、业务多样化、经济等特性

D:5G技术的目的是构建网络社会

1. 第二代蜂窝移动通信(2G)的代表性体制就是最流行的（ D ）系统。

A:FDMA B:CDMA C:LTE D:GSM

1. 蜂窝网络移动性管理采用的是（ B ）。

A:直接路由选择方法 B:间接路由选择方法

C:静态路由选择方法 D:动态路由选择方法

4、1、IEEE颁布的宽带无线协议是（ D ）。

A:IEEE802．11a B:IEEE802．11b

C:IEEE802．11b+  D:IEEE802．16

1. 下列不是网络安全通信所需要的基本属性的是（ C ）。

A:机密性 B:消息完整性 C:时效性 D:身份认证