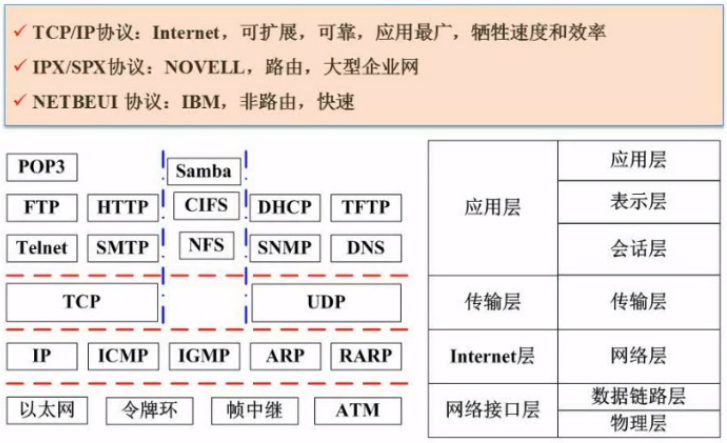
网络和信息安全

网络概述

ISO/OSI模型

- **应用层**: 具体功能的实现
- **表示层**: 数据的格式与表达,加密/解密,压缩
- **会话层**: 报文. 建立和终止会话
- **传输层**: 报文. 端到端连接 TCP.UDP
- **网络层**: 包, 分组传输和路由选择 ,三层交换机.路由器. ARP/RARP, IP, ICMP,IGMP
- **数据链路层**: 帧, 传输以帧为单位的信息 网卡,交换机,网桥. PPTP,L2TP,SLIP,PPP
- **物理层**: 比特, 二进制传输. 中继器,集线器

网络协议



ip地址分类

类别	点分十进制	二进制	
A类	0.0.0.0	最低	00000000 00000000 00000000 00000000
	127.255.255.255	最高	01111111 11111111 11111111 11111111
B类	128.0.0.0	最低	10000000 00000000 00000000 00000000
	191.255.255.255	最高	10111111 11111111 11111111 11111111
C类	192.0.0.0	最低	11000000 00000000 00000000 00000000
	223.255.255.255	最高	11011111 11111111 11111111 11111111
D类 组播	224.0.0.0	最低	11100000 00000000 00000000 00000000
	239.255.255.255	最高	11101111 11111111 11111111 11111111
E类 保留	240.0.0.0	最低	11110000 00000000 00000000 00000000
	255.255.255.255	最高	11111111 11111111 11111111 11111111

子网划分

例题1

将B类地址168.195.0.0 划分成27个子网,子网掩码是多少?

解题

- 划分子网的问题,考虑的是网络位从主机位借多少的问题?
- $2^4 < 27 < 2^5$.也就是网络号从主机号借5位就行了. 原本B类掩码是16,+5后是21位. 11111111 11111111 11111000 00000000 转成10进制是(255-7) = 248(*二进制的111就是10进制的7*),最终的子网掩码就是255.255.248.0

例题2

将B类地址168.192划分成若干子网,每个子网内有主机700台,则子网掩码为多少?

解题

- 这类问题是考察主机位从网络位借多少的问题?
- 子网要求700台主机. 由于8位主机位能容纳254台主机,不够,向上借一位是256*2-2=512-510.不够.再借一位256*4-2=1022,够了,主机位就是10位,向网络位借了2位.那网络掩码就是24-2=22, 22位子网掩码是11111111 11111111 11111100 00000000 转成10进制是(255-3) = 252.(*二进制的11就是10进制的3*)最终的子网掩码就是255.255.252.0

例题2

分配给某公司的地址块是210.115.192.0/20,该网络可以被划分为多少个c类的子网?

解题

- c类的子网,掩码是24. 24-20=4, $2^4 = 16$,答案就是16个子网(虽然有全0和全1的2个不可用,但仍然是子网)

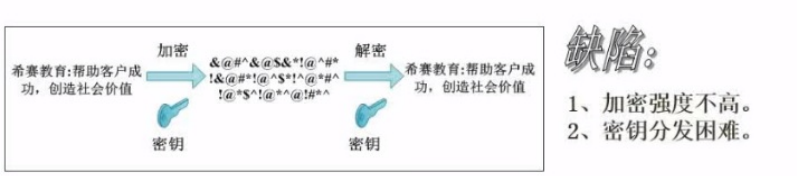
特殊含义ip地址

IP	说明
127网段	回播地址
网络号全0地址	当前子网中的主机
全1地址	本地子网的广播
主机号全1地址	特定子网的广播
10.0.0.0/8	10.0.0.1 至10.255.255.254
172.16.0.0/12	172.16.0.1 至 172.31.255.254
192.168.0.0/16	192.168.0.1 至 192.168.255.254
169.254.0.0	保留地址，用于DHCP失效(Win)
0.0.0.0	保留地址，用于DHCP失效(Linux)

网络安全

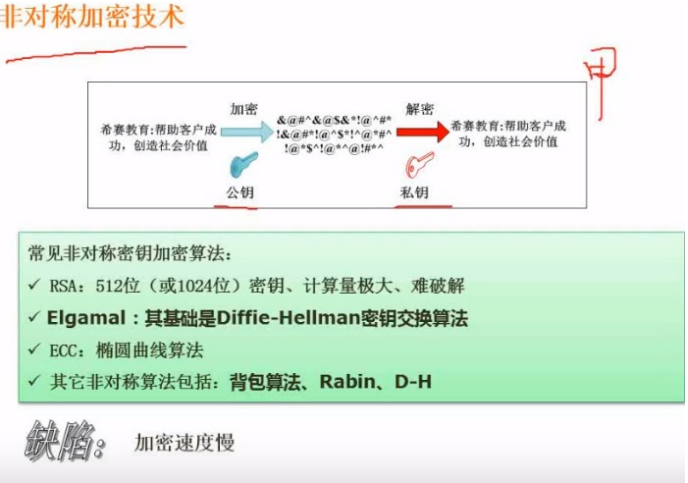
加密技术

对称加密技术

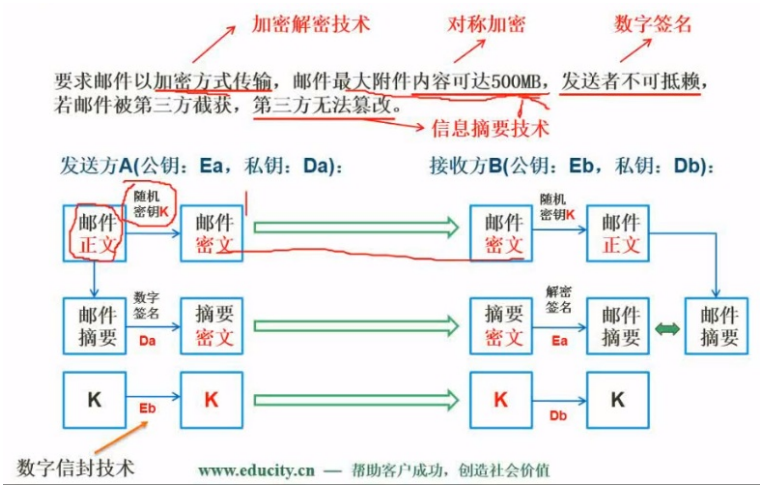


常见对称密钥加密算法：
✓ DES：替换+移位、56位密钥、64位数据块、速度快、密钥易产生
3DES(三重DES)：两个56位的密钥K1、K2
加密：K1加密->K2解密->K1加密
解密：K1解密->K2加密->K1解密
✓AES：高级加密标准Rijndael加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES。对其要求是"至少与3DES一样安全"。
✓ RC-5：RSA数据安全公司的很多产品都使用了RC-5。
✓ IDEA算法：128位密钥、64位数据块、比DES的加密性好、对计算机功能要求相对低，PGP。

非对称加密技术



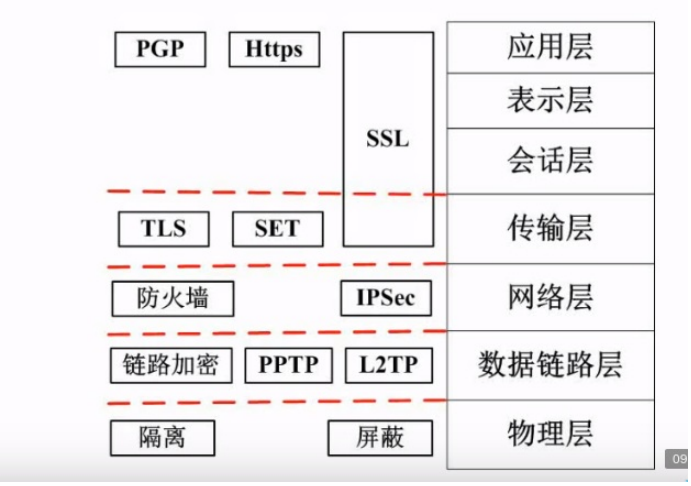
例题



解题

- 邮件内容的大小很大,说明正文需要对称加密技术.
- 而对称加密技术需要发送密钥.密钥尺寸小,可以采用非对称加密技术提高安全性.使用数字信封技术.这时**发送时采用接收放的公钥进行加密,接收方用自己的私钥解密**
- 为了防止正文被修改,生成了系统摘要.为了保证发送者不可抵赖,采用了数字签名技术.**发送者使用自己的死要加密,接收方使用发送方的公钥解密**.保证了不可抵赖的特性.

不同网络层次的安全问题



常见网络威胁

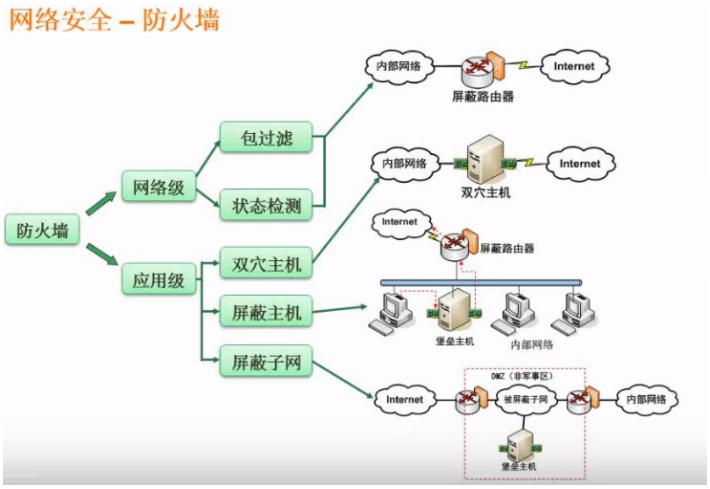
威胁名称	描述
重放攻击（ARP）	所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送。
拒绝服务（DOS）	对信息或其它资源的合法访问被无条件地阻止。
窃听	用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如对通信线路中传输的信号进行搭线监听，或者利用通信设备在工作过程中产生的电磁泄露截取有用信息等。
业务流分析	通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。
信息泄露	信息被泄露或透露给某个非授权的实体。
破坏信息的完整性	数据被非授权地进行增删、修改或破坏而受到损失。
非授权访问	某一资源被某个非授权的人、或以非授权的方式使用。

威胁名称	描述
假冒	通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒进行攻击。
旁路控制	攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本应保密，但是却又暴露出来的一些系统“特性”。利用这些“特性”，攻击者可以绕过防线守卫者侵入系统的内部。
授权侵犯	被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其它非授权的目的，也称作“内部攻击”。
特洛伊木马	软件中含有一个察觉不出的或者无害的程序段，当它被执行时，会破坏用户的安全。
陷阱门	在某个系统或某个部件中设置了“机关”，使得当提供特定的输入数据时允许违反安全策略。
抵赖	这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。

注意各种威胁的关键词.这是考试中的考点.比如业务流分析和窃听的长期

防火墙技术

网络安全 – 防火墙


防火墙
网络级
应用级
包过滤
状态检测
双穴主机
屏蔽主机
屏蔽子网
内部网络
Internet
屏蔽路由器
双穴主机
Internet
屏蔽路由器
堡垒主机
内部网络
DMZ（非军事区）
Internet
被屏蔽子网
内部网络
堡垒主机