**网络安全复习题**

1. 名词解释 5\*3`
   1. 身份鉴别P101
2. 身份鉴别是**验证主体的真实身份与其声称的身份是否符合的过程**，主体可以是**用户、进程和主机**等。网络环境下，主体必须有**能够证明其身份**，且**可以通过网络传输**的**主体身份标识信息**。
3. 鉴别方式可以分为三种：
   1. 单向鉴别
   2. 双向鉴别
   3. 第三方鉴别
4. 主体身份标识信息主要包括：
   1. 密钥
   2. 用户名和口令
   3. 证书和私钥
   4. 防火墙 P297-298
5. 定义：一种位于**网络之间**或者**用户终端与网络之间**，对网络之间或网络与用户终端之间传输的**信息流实时控制的设备**。这个设备可以是单独的装置，也可以集成在路由器和主机中。
6. 作用：**阻断有害信息**从一个网络进入另一个网络，或者是通过网络进入终端。
   1. 网络入侵安全检测机制的安全策略 P356-357
7. 指定**需要检测的信息流**
   1. 在**流经网络入侵检测系统**的**一组IP分组**中指定**需要实施入侵检测的IP分组**
   2. 安全策略通过指定IP分组的**源IP地址范围**和**目的IP地址范围**来确定实施入侵检测的IP分组
8. 指定**检测机制和检测内容** 
   1. 检测机制分为**协议译码、攻击特征检测和异常检测**
   2. 协议译码:
      1. 需要通过***定义*服务指定*完成*服务进行**的**信息交换过程**
      2. 通过检测**IP分组内容**、**TCP报文内容**和**HTTP消息内容**，确定流经网络入侵检测系统的信息是为完成HTTP服务交换的信息
   3. 攻击特征检测：
      1. 需要**按照网络入侵检测系统保护的服务器类型**指定需要检测的攻击特征
      2. 可以通过指定**攻击特征库**来指定需要检测的攻击特征
   4. 异常检测：
      1. 首先需要制定一组规则，然后将**特性与规则相符的信息流**作为异常信息
      2. 可以通过指定**交互信息**来指定**需要检测具有交互特性的异常信息**，同时指定**标识交互信息特征的规则**
9. 指定**对入侵信息的反制动作**
   1. **丢弃**包含入侵信息的**IP分组**
   2. **复位**包含入侵信息的**TCP报文所属的TCP连接**
   3. **阻塞源IP地址**等
   4. 认证中心
10. 认证中心是一个**具有公信力的权威机构**
11. 当用户B希望通过认证中心来认证它所发布的公钥PKB不是伪造的时,用户B**需要携带希望认证的公钥PKB和证明自己身份的证件**到认证中心
12. 认证中心确认用户B的真实身份后,提供一份证书,证书分为两部分:**一部分是用明文方式给出的用于确认公钥PKB和用户B之间绑定关系的证明**。**另一部分是用认证中心的私钥SKCA对上述明文的报文摘要进行解密运算后生成的密文()**。
    1. VPN
13. 一种**保证**多个通过Internet**实现互联的内部网络**之间、连接在Internet上的**终端与内部网络**之间**传输的信息的保密性和完整性的技术**。
    1. 服务控制
14. 服务控制就是通过**制定相应的安全策略**,只允许**网络间相互交换和特定服务相关的信息流**
    1. 以太网技术有关
15. 什么是以太网安全技术？P179
    1. 以太网安全技术是**集成在交换机**中，用于**增强以太网安全功能的安全技术**（用于**抵御针对以太网的网络攻击**的安全技术）。
    2. 以太网技术有关
16. 什么是以太网接入控制技术？P180
    1. 以太网接入控制技术是一种建立在**终端与交换机端口之间**物理连接的情况下，确定**该终端能否通过它所连接的交换机端口实现与连接在以太网上的其他终端之间**的**MAC帧传输过程**的安全技术。
    2. 拒绝服务攻击和流量管制
17. 拒绝服务攻击是一种**通过消耗链路宽带与结点（主机、交换机和路由器等）的资源和处理能力**，达到**使互联网丧失服务功能的目的**的**攻击行为**。
18. 防御拒绝服务攻击的**有效办法**就是**管制与拒绝服务攻击相关的信息流量**
19. 流量管制就是一种**将属于特定应用的IP分组**的**传输速率**限定**在某个设定值**的技术
    1. NAT技术
20. 内部网络终端在与公共网络终端通信过程中，使用两个不同的IP地址：
    1. **在内部网络中使用的私有IP地址**
    2. **在公共网络中使用的全球IP地址**
21. 互连**内部网络和公共网络**的边界路由器需要实现**两个地址之间的转换**，路由器实现这两个地址之间转换的技术称为**网络地址转换技术（NAT）**
22. 选择题 5\*3`
23. 网络环境下的信息安全目标不包括（ D ）

A、可用性 B、保密性 C、完整性 D、可抵赖性

1. （ B ）可以由内部网络中的终端发起访问互联网的过程，但不能由互联网中的终端发起访问内部网络的过程。

A、防火墙 B、VPN C、网络入侵检测系统 D、网络病毒防御

1. 网络安全的实质和关键是保护网络的（ C ）安全。

A、系统 B、软件 C、信息 D、网站

1. 下列不属于网络被动攻击的是
2. 嗅探信息 B、非法访问 C、数据流分析 D、篡改信息
3. 下列属于欺骗攻击的是
4. MAC地址欺骗攻击 B、DHCP欺骗攻击 C、APP欺骗攻击 D、生成树欺骗攻击
5. 下列属于防御ddos攻击的办法是
6. 连接在互联网上的手机系统，能够具备防御病毒和黑客入侵的能力
7. 主机系统拒绝响应ICMP ECHO请求报文
8. 网络具有统计目的，IP地址相同的 icmp echo响应报文
9. 关闭计算机
10. 黑客攻击包含哪几个阶段
11. 信息收集 B、扫描 C、渗透 D、攻击
12. 下列不属于黑客攻击中扫描阶段的是？
13. 获取网络拓扑结构
14. 获取主机生产日期
15. 获取操作系统版本和类型
16. 获取应用程序版本和类型
17. 下列统称为病毒的是？
18. 病毒 B、蠕虫 C、僵尸 D、爬虫
19. 以下算法中属于非对称算法的是（ B ）p81
20. Hash算法 B、RSA算法 C、IDEA D、三重 DES
21. 以下不属于非对称密码算法的特点是（ D ）p80
22. 计算量大 B、处理速度慢 C、运算过程复杂 D、适合大量数据加密
23. 就目前计算机设备的计算能力而言，数据加密标准DES不能抵抗对密钥的穷举搜索攻击，其原因是 （　Ｂ　）p69
24. DES 算法是公开的
25. DES的密钥较短
26. DES除了其中S盒是非线性变换外，其余变换均为线性变换
27. DES算法简单
28. 以下哪一项是报文摘要算法特点（C）？P85页最上
29. 碰撞性 B、低灵敏性 C、单向性 D、不易于实现
30. 报文摘要算法的（A）的特点是用报文摘要实现完整性检测的前提？P85页上
31. 抗碰撞性 B、易于实现 C、单向性 D、高灵敏度
32. 以下不属于身份鉴别方式的是（C）P101

A.单向鉴别B.双向鉴别C.直接鉴别D.第三方鉴别

1. 不属于PPP接入控制过程的是（A）P112

A.物理链路建立

B.用户身份鉴别

C.网络层协议设置

D.终止PPP链路

1. 以下关于接入控制和访问控制的内容叙述哪一项是不正确的（B）

A..鉴别用户身份的协议有口令鉴别协议PAP和挑战握手鉴别协议CHAP.P110

B.PPP本身不是一种用于传输鉴别协议鉴别用户身份所需消息的载体协议，而是一种鉴别协议。P113

C.RADIUS是一种可以实现接入控制设备等鉴别者与鉴别服务器之间双向身份鉴别和身份标识信息鉴别者与鉴别服务器之间安全传输的应用层协议。P121

D.Kerberos统一由鉴别服务器完成用户身份鉴别功能，统一由票据授权服务器完成用户访问权限鉴别功能。P131

1. 以下哪一项不是安全协议的安全功能()

A.端到端的可靠传输

B.双向身份鉴别

C.数据完整性检测

D.数据加密

答案：选A，端到端传输不是，在书上134页

1. IPsec中安全关联(SA)的三元组包括()

A.安全参数索引SPI、源IP地址、数字证书

B.安全参数索引SPI、目的IP地址、数字证书

C.安全参数索引SPI、目的IP地址、安全协议

D.安全参数索引SPI、源IP地址、安全协议

答案：选C，IPsec中安全关联SA用安全参数索引SPI、目的IP地址、安全协议唯一标识；在书上136页

1. ESP采用和AII相同的MAC算法鉴别数据，但计算鉴别数据时覆盖的字段不包括下列哪一项？（）

A.ESP手部

B.净荷

C.ESP尾部

D.外层IP首部中的不变字段

答案：选D，包括ESP手部、净荷、ESP尾部；在书上142页

1. 解决无线局域网安全问题的基本方法不包括（B）。

A接入控制 B数字签名和源端检测 C加密 D完整性检测

1. 关于WEP,以下哪一项描述是错误的?(D）

A.用循环冗余码检测数据完整性

B.伪随机数生成算法作为产生一次性密钥的单向函数

C.采用流密码体制

D.一次性密钥不会重复

由于所有终端共享个一次性密钥,因此很容易导致一次性密钥重复使用。

1. 以下哪项不属于频段开放性和空间开放性带来的安全问题（D）。

A重放攻击 B信道干扰 C嗅探和流量分析 D ARP欺骗攻击

1. 以下哪一项不是路由器的的功能（D） P229 2.路由器的作用

A、用于互联多个类型互不相同的网络

B、建立用于指明通往互联网中每一个网络的传输路径的路由项

C、实现IP分组的转发过程

D、信息处理速度比网桥快

【解析】D选项错误。交换机、网桥要比路由器快，因为交换机靠硬件，高速芯片来进行处理，而路由器靠软件处理，比较慢。

1. 有关NAT与PAT之间的差异，下列哪一项正确?（D）P243第二段

A、PAT使用多个的源端口号区分不同的转换。

B、静态NAT可让一个非注册地址映射为多个注册地址。

C、动态NAT可让主机在每次需要外部访问时接收相同的全局地址。

D、PAT使用唯一的源端口号区分不同的转换。

【解析】D选项正确。内部网络终端发送的IP分组，进入Internet时，以边缘路由器连接Internet端口的全球IP地址为源IP地址，为了正确鉴别源终端，用内部网络唯一的源端口号取代IP分组终端唯一的源端口号。

1. 网络管理员应该使用哪种NAT来确保外部网络一直可访问内部网络中的web服务器？（C） P246静态NAT第一段

A、静态PAT

B、动态PAT

C、静态NAT

D、动态NAT

【解析】静态NAT将建立本地地址和全球IP地址的固定关联，这样，允许外部网络终端随时通过该全球IP地址访问和该全球IP地址建立固定关系的本地地址所标识的内部网络终端。

1. 建立安全传输通道的加密算法是（C） P269 10.2.3

A.AES B.DSA C.3DES D.IDEA

1. 以下哪些是互联网实现互联的网络结构特点(D) P260 10.1.2

接入方便费用低廉传输速率不是固定的通过互联网完成数据传输过程

私有IP地址和全球IP地址

A.B.C. D.

1. 以下不属于VPN分类中的是(A) P262 10.1.3

A.第一类隧道和IPsec B.第二类隧道和IPsec C.第三类隧道和IPsec D.SSL VPN

1. 以下哪个属于IPSec和安全传输过程？（B） P269 10.2.3

A.IPSec密钥传输过程 B.安全关联建立过程 C.远程终端接入内部网络过程D. 传统拨号接入过程

1. 以下哪个不是L2TP建立第二层隧道的过程？(D) P277 3

A.L2TPv3控制消息格式 B.控制连接建过程 C.第二层隧道建立过程 D.远程接入网络过程

1. 以下哪个是经过第二层隧道传输PPP帧的过程？(A) P280 4

A.LAC向LNS传输PPP帧过程

B.ACK向LNS传输PPP帧过程

C.ICRP向LAC传输PPP帧过程

D.ESP向LNS传输PPP帧过程

1. (多选)Cisco Easy VPN的接入过程有哪些? (ABCD) P287 3

A.路由器R配置的参数 B.注册用户信息C.安全关联相关的信息 D.本地IP地址池

1. （多选）互联网实现互联的网络结构需要解决的问题有(ABCD) P261 10.1.2

A.私有IP地址 B.保密性和完整性 C.双向身份鉴别 D.服务质量

1. (多选)SSL VPN的实现过程有哪些？（ABC） P293 2

A.建立远程终端与SSL VPN网关之间的TCP连接

B.建立远程终端与SSL VPN网关之间的SSL会话

C.远程终端登录SSL VPN网关

D. 生成SSL VPN网关密钥

1. （多选）第二层隧道和IPSec的缺陷有(ABCDE) P290 10.4.1

A.VPN对远程终端的访问权限没有限制

B.家庭局域网中的终端无法访问其他内部网络

C.需要专用客户端

D.远程终端可以发现内部网络拓扑结构

E.无法实现基于用户授权

1. 防火墙作为一种被广泛使用的网络安全防御技术，其自身有一些限制，它不能阻止（ A ） P302

A、内部威胁和病毒威胁

B、外部攻击

C、外部攻击、外部威胁和病毒威胁

D、外部攻击和外部威胁

1. 防火墙把网络划分为几个不同的区域，一般把对外提供网服务的设备（如Web服务器、FTP服务器）放置于 （ D ）区域 P310

A.信任网络

B.非信任网络

Ｃ.半信任网络

Ｄ.DMZ（非军事化区）

1. 防火墙在进行分组过滤时，通常不会依据的是( D ) P302

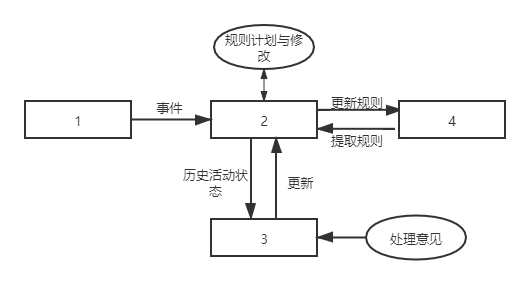
A.目的IP地址

B.目的端口号

C.源IP地址

D.TTL

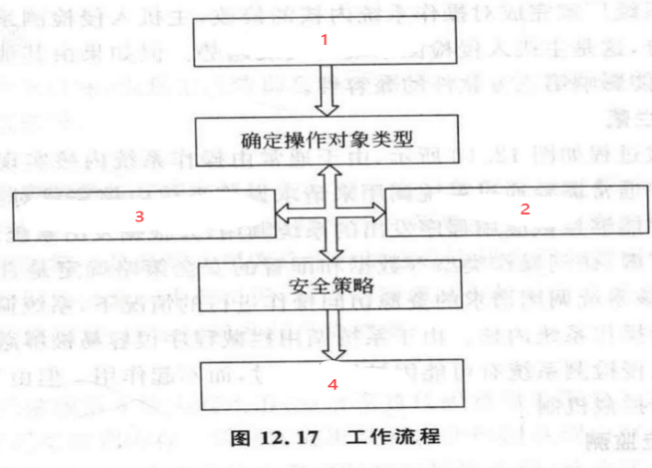
1. 下图中1和4分别是()和()。 P338 结构图



A:事件发生器 B:事件分析器 C:相应单元 D:时间数据库

图中数字对应答案为：1A,2B,3C,4D 记住通用框架结构

1. 主机入侵检测系统工作流程中1，4分别是()和() P367 工作流程图



A:拦截操作请求 B:系统状态 C:采集和操作相关信息 D:操作决策

对应答案：1A,2B,3C,4D

1. 以下关于宏病毒说法正确的试:( B )
2. 宏病毒主要感染可执行文件
3. 宏病毒仅向办公自动化程序编制的文件进行传染
4. 宏病毒主要感染软盘、硬盘引导扇区或主引导扇区
5. CIH病毒属于宏病毒
6. 下列选项中不属于计算机病毒防御技术的是？（D）
7. 基于特征的扫描技术
8. 基于线索的扫描技术
9. 基于行为的扫描技术
10. 基于保密性检测的扫描技术
11. 判断题 5\*2`
12. TCSEC将计算机系统的安全类别从低到高分为三类。 （ × ）

原因：TCSEC将系统分成ABCD四类7个安全级别

1. 安全理论包括各种密钥生成算法、加密解密算法和报文摘要算法等，以及这些算法引申出的鉴别机制和数字签名方法。 （ √ ）
2. 安全模型是以建模的方式清楚地描述网络安全实现过程所涉及的因素及这些因素之前的相互关系。 （ √ ）
3. 被动攻击是指以各种方式有选择的破坏信息的有效性和完整性 （ × ）

原因：被动攻击一般只破坏信息的保密性，而主动攻击，可以破坏信息的保密性。完整性和可用性等

1. 黑客成功入侵的前提有两个，一是存在黑客终端与攻击目标之间的传输通路，二是攻击目标存在漏洞 （ √ ）
2. DHCP，可以用来为每台设备自动分配IP地址 （ √ ）
3. 破坏网络环境下的信息系统的保密性，可用性和可查性，成为病毒的主要目的 （ × ）

原因：破坏网络环境下的信息系统的保密性，完整性和可用性，逐渐成为主流病毒类型

1. 拒绝服务是指攻击者通过各种非法手段占据大量的服务器资源，致使服务器系统没有剩余资源，提供给其他的合法用户使用 （ √ ）
2. 分组密码体制允许反复使用同一密钥，但需要将明文分割成固定长度的数据段后，再进行加密运算。

（ √ ）

1. 流体密码体制每一次加密过程使用不同的密钥，且这些密钥之间没有相关性. （ √ ）
2. RAS的加密密钥可以公开，解密密钥也是公开的。 （ × ）
3. PKI包括整数的生成、更新、撤销和交叉认证机制。（P95页下） （ √ ）
4. 利用报文摘要算法生成的报文摘要的目的是对传输数据进行加密，防止数据被窃听（P84） （ × ）

原因：报文摘要是用来保证数据的完整性的。传输的数据一旦被修改，那么计算出来的摘要就不同，只要对比两次摘要就可以确定数据是否被修改过。因此其目的是为了防止发送的报文被篡改。

1. 访问控制的基础是身份鉴别和授权，只允许授权用户访问该用户授权访问的资源。 （√）P131
2. 鉴别协议定义了示证者和鉴别者之间为完成身份鉴别过程需要交换的信息内容和工作过程。 （×）P131
3. Kerberos中存在4种角色，分别是用户（也称客户端）、鉴别服务器、票据授权服务器和应用服务器。 （√）P131
4. IPSec属于传输层的安全解决方案（）

答：错，IPSec属于网络层的安全解决方案，书上135页，最下面一段话的第一句，IPSec是网际层实现IP分组端到端的安全传输的机制，由一组安全协议组成。

1. SMTP只能传输7位ASCII码，无法传输由任意二进制位流构成的邮件体（）

答案：对；书上171页

1. 传输模式用于保证数据端到端安全传输，并对数据源端进行鉴别。（）

答案：对；书上137页传输模式第一句话。

1. WPA2有企业模式和个人模式。这两种工作模式的加密和数据完整性检测机制相同,双向身份鉴别机制不同。 （√）

WEP是一种有着比802.11i更强安全功能的无线局域网安全协议。 （×）

1. 802.1x用EAP作为鉴别协议，因此可以使用EAP协议的多种鉴别机制。 （×）
2. 安全路由技术用于保障路由器路由项的正确性和完整性，保证终端之间IP分组的正确传输 （√） P230 9.2 第一段

【解析】解决连接在不同类型的传输网络上的终端之间的通信问题的关键是建立任何两个终端之间的IP层传输路径。安全路由技术就是一种用于保障路由器路由项的正确性和完整性，以此实现连接在不同网络上的终端之间通信过程的安全技术。

1. VRRP作用的网络只有以太网、令牌环网和FDDI。（×） P248 9.5.2 第一段

【解析】VRRP作用的网络可以是任意支持广播的网络，如以太网、令牌环网和FDDI。

1. 只要能够限制某类报文的流量，就能够抑制拒绝服务攻击。（√）P235 第三段

【解析】拒绝服务攻击的共同点是黑客终端向攻击目标超量发送报文，因此，只要能够限制某类报文的流量，就能够抑制拒绝服务攻击。

1. ESP 是封装安全载荷协议，主要提供的功能有数据机密性，数据完整性 ， 数据来源认证，  重放 （X）

原因：/ “重放”->“反重放”/

1. 关于安全联盟SA，IKE是单向（单向或双向）IPSEC SA是双向（单向或双向）（X）

原因：/“单向->双向”/ /“双向->单向”/

1. IPSE的两种工作方式是tunnel和transport (√)
2. 防火墙是存在于网络安全体系中一个独立的部分，它可以抵御一定程度上黑客的攻击。 （×） P302
3. 远程终端接入内部网络时，LNS需要完成对远程终端用户身份鉴别同时分配远程终端用户访问内部网络资源的权限。 （×） P321
4. 应用层网关的应用环境：必须保证所有终端传输给特定服务器的请求消息经过应用层网关。（√） P330
5. 入侵检测系统评价指标分别是：入侵检测系统减少误报、入侵检测系统减少漏报。 P346 12.1.9

答案：错，还有捕获和检测信息流的能力。

三个指标分别是正确性，全面性和性能，但是可以进一步精确解释这三个指标是什么。

1. 目前，用于拦截操作请求的机制有修改系统内核，系统调用拦截和网络信息流检测等。

答案：对 P361 12.3.4拦截机制

1. 主机资源是攻击目标，也是主机防御系统的保护对象，它主要包括网络，内存，进程，文件和系统配置信息等。

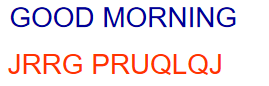
答案：对 P363 12.3.5主机资源

1. 计算题 5`+10`
   1. 凯撒密码

凯撒密码完成**明文至密文**的转换过程如下：将构成文本的每一个字符用字符表中**该字符*之后*的第三个字符**代替。

凯撒密码完成**密文至明文**的转换过程如下：将构成文本的每一个字符用字符表中**该字符*之前*的第三个字符**代替。





换位密码：换位密码是一种通过**改变明文中每一个字符的位置**，完成将明文转换成密文过程的加密算法。



加密过程 解密过程

换位规则(2,4,1,3) 换位规则(3,1,4,2)

(1,2,3,4) (1,2,3,4)

* 1. 第三组试题Diffie-Hellman

设素数P=71，原根α=7，用户A选择XA=5，用户B选择XB=12，求用户A和用户B用Diffie-Hellman密钥交换算法同步密钥K。

(1)选择素数p=71,原根α=7。

(2)用户A选择XA=5,求出。

(3)用户B选择XB=12,求出。

(4)用户A求出。

(5)用户B求出。

(6)

1. 解答题 3\*10`
   1. 网络安全下的信息安全目标

信息安全目标：信息安全目标包括**信息的可用性、保密性、完整性、不可抵赖性和可控性**

1. 可用性

可用性是**信息被授权实体访问并按需使用**的特性。

1. 保密性

保密性是**防止信息泄露给非授权个人或实体，只为授权用户使用**的特性。

1. 完整性

完整性是**信息未经授权不能改变**的特性。

1. 不可抵赖性

不可抵赖性是**信息交互过程中，所有参与者不能否认曾经完成的操作或承诺**的特性 。

1. 可控制性

可控制性是**对信息的传播过程及内容具有控制能力**的特性。

* 1. 三种防火墙特点：

1. **分组过滤器,电路层代理和应用层网关**是三种**作用在不同层次**的防火墙
2. 分组过滤器主要作用在**网际层**,也检测**传输层的源和目的端口号**。
3. 电路层代理主要作用在**传输层**。
4. 应用层网关主要作用在**应用层**,每一种应用层协议有着对应的应用层网关,因此,应用层网关是与特定网络应用相关的。
   1. VPN与NAT的三点区别与联系
5. VPN目标：**公共网络实现内部网络各个子网之间的互连**，同时也保障内部网络和各个子网的互连。

NAT目标：实现**从内部网络到外部网络的IP地址的转换**

1. VPN是从**外部对内部**，NAT是**从内部到外部**。若NAT只对内网进行互连，不走外网，则NAT对于公网是透明的。
2. **VPN本身不需要NAT技术**，如果需要内部网络互连，只能**借助于隧道和IPSec技术**，在其中**增加NAT技术**。
3. 论述题15`
   1. 双重签名P162画图有加分
4. 持卡人完成一次电子交易**需要向商家列出购买的商品清单和支付凭证**，支付凭证中给出持卡人拥有的信用卡信息及付款对象和金额，由于信用卡信息对商家是保密的，因此，**商家只能验证该支付凭证，不能读取支付凭证中有关信用卡账户的信息**。同时，为了日后避免纠纷，**无论商家还是持卡人都需要将每一次电子交易涉及的购物清单和支付凭证绑定在一起**。持卡人每一次电子交易中给出的**购物清单称为订货信息(Order Information，OI），支付凭证称为支付信息(Payment Information，PI)**，这两种信息通过交易标识符关联在一起，即**这两种信息中必须包含相同的交易标识符**。持卡人必须能够向商家和支付网关证明这一次电子交易中涉及的两组信息确实由持卡人给出，为此，持卡人的数字签名不仅需要证明这一次电子交易中涉及的两组信息确实由持卡人给出，还须将这两组信息绑定在一起，实现这一功能的数字签名称为双重签名(Dual Signature，DS)。
5. **简答题目：**
   1. 写出双重签名的表达式并简单画图描绘出其生成过程。
   2. 双重签名的简单验证过程。（对商家和支付网关分别说明）
6. **可能用到的符号：**

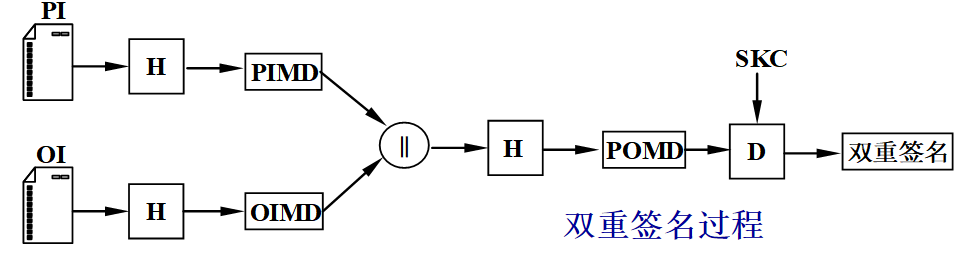
**DS：**双重签名 **OI：**订货信息 **PI：**支付信息 **H：**报文摘要算法

**PIMD：**支付信息的报文摘要 **OIMD：**订货信息的报文摘要 **||：**串接操作符

**POMD：**两组信息的报文摘要 **E：RSA**加密算法 **D：RSA**解密算法

1. **参考答案：**
   1. **表达式：**

**过程示意图：**



对于商家：由于**商家是不允许获得PI**的，在这种情况下，为验证双重签名，需要**向商家提供支付信息的报文摘要（PIMD）**，商家通过比较和，在时,确认双重签名，不相等则持卡人双重签名失败。

对于支付网关：**支付网关并不需要OI**，为了验证双重签名，需要向支付网关提供**订货信息的报文摘要（OIMD）**，支付网关比较与是否相等，若，确认双重签名，不相等则持卡人双重签名失败。