NSP Review

ypa

Contents

1. 基本概念

1.1. 概念，定义，名词

网络安全特征: 机密性、完整性、可用性、可认证、不可否认、可控性

常见的不安全因素

- 物理因素：物理设备的不安全，电磁波泄漏等
- 系统因素：系统软、硬件漏洞，病毒感染，入侵
- 网络因素：网络协议漏洞，会话劫持、数据篡改，网络拥塞，拒绝服务
- 管理因素：管理员安全意识淡漠，误操作

导致不安全的原因

- 自身的缺陷：系统软硬件缺陷、网络协议的缺陷
- 开放性
  - 系统开放：计算机及计算机通信系统是根据行业标准规定的接口建立起来的。
  - 标准开放：网络运行的各层协议是开放的，并且标准的制定也是开放的。
  - 业务开放：用户可以根据需要开发新的业务
- 黑客攻击

常见攻击手段: 社会工程、口令破解、地址欺骗、连接盗用、网络窃听、数据篡改、恶意扫描、基础设施破坏、拒绝服务、数据驱动攻击

总结为四种：

- 中断：可用性
- 窃听：机密性
- 修改：完整性
- 伪造：可认证性

主要概念和术语的规范中英文, TODO

1.2. 基本的安全模型、安全体系结构

1.2.1. 安全体系结构

安全攻击(区别在于会不会主动改变数据流)：

- 主动攻击：篡改、伪装、重放、拒绝服务
- 被动攻击：窃听、流量分析

安全机制：加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制、公证

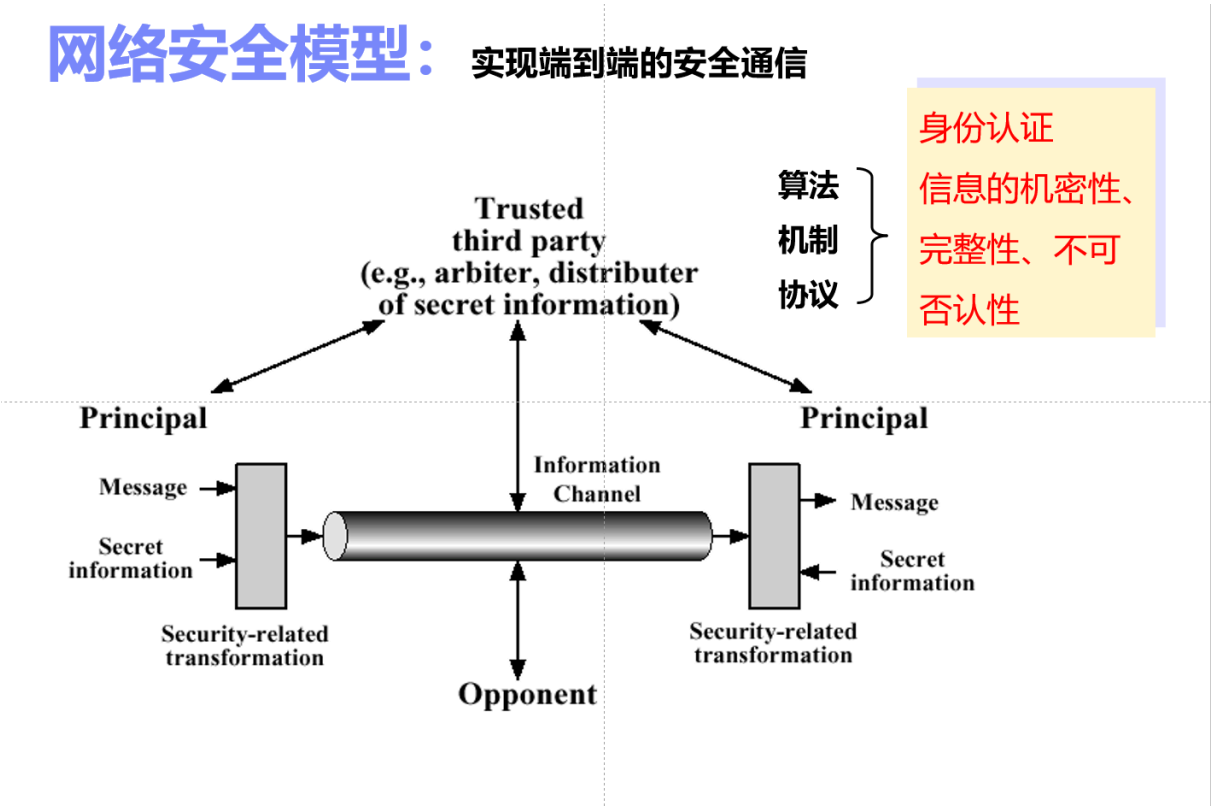
安全服务：X.800 定义了 5 类 14 种安全服务

- 认证：对等实体认证、数据源认证(重点，需要了解两者差别)
  - 区别：对等实体认证是对通信双方的认证，数据源认证是对数据的认证
- 访问控制
- 数据机密性：连接保密性、无连接保密性、选择域保密性、流量保密性
- 数据完整性：具有恢复功能的连接完整性、无恢复功能的连接完整性、选择域连接完整性、无连接完整性、选择域无连接完整性
- 不可否认性：源点的不可否认性、信宿的不可否认性

安全攻击，机制，服务三者之间的关系：在 X.800 中定义为安全攻击、安全机制、安全服务三个层面。用一种或多种安全机制来实现安全服务，安全服务致力于抵御安全攻击。

1.2.2. 基本的安全模型

- 网络安全模型:
  - 实现端到端的安全通信（安全通道建立，数据传输）.
  - 算法机制协议：身份认证、信息的机密性、完整性、不可否认性



- 网络访问安全模型
  - 保护信息系统免遭恶意访问
  - 保证网络的可用性，可控性
  - （访问控制、权限管理、安全通道建立、数据传输）

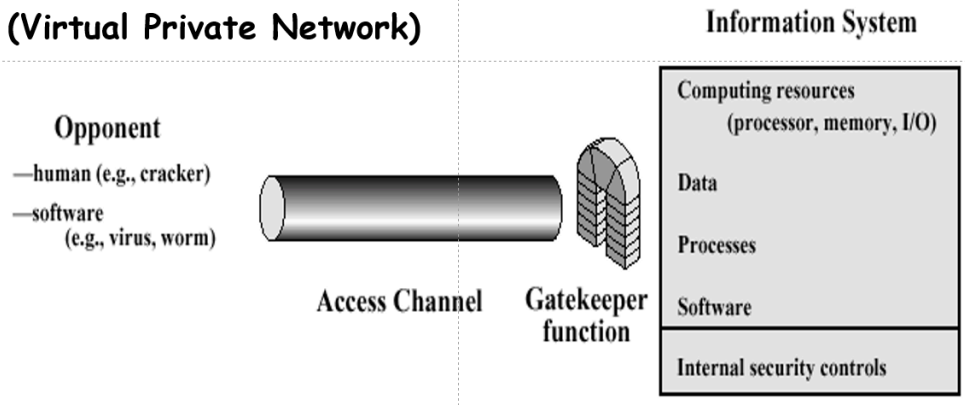
网络访问安全模型： 保护信息系统免遭恶意访问

保证网络的
可用性、可控性

Firewalls and Security Gateways

IDS (Intrusion Detection System)

VPN (Virtual Private Network)



1.3. 基本的加密、认证、密钥交换算法

1.3.1. 用户认证（基于挑战应答：对称加密、签名、非对称加密、HMAC）

基于挑战/应答（Challenge/Response）方式的身份认证系统就是每次认证时认证服务器端都给客户端发送一个不同的"挑战"字串，客户端程序收到这个"挑战"字串后，做出相应的"应答",以此机制而研制的系统.认证过程为：

1. 客户向认证服务器发出请求，要求进行身份认证；
2. 认证服务器从用户数据库中查询用户是否是合法的用户，若不是，则不做进一步处理；
3. 认证服务器内部产生一个随机数，作为"提问"，发送给客户；
4. 客户将用户名字和随机数合并，使用单向 Hash 函数（例如 MD5 算法）生成一个字节串作为应答；
5. 认证服务器将应答串与自己的计算结果比较，若二者相同，则通过一次认证；否则，认证失败；
6. 认证服务器通知客户认证成功或失败。

1.3.2. 数据源认证（签名、HMAC）

数据机密性、完整性保护等的基本方法

1.4. 密码学课程中涉及的常见加密算法

对称、非对称、哈希函数、HMAC 等等

哈希函数：

- MD5(128bit)
- SHA-1(160bit)
- SHA-2

  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
  - SHA-512/224
  - SHA-512/256
- SHA-3

1.5. 分组密码算法的工作模式

IV 值的使用和作用（即使相同明文亦可得到不同密文）

典型加密模式的操作和差错的影响

1.6. DH 密钥交换算法

步骤：

1. 选择素数 p 和底数 g
2. Alice 和 Bob 各自选择私钥 X_A 和 X_B，并计算公钥 $Y_A = g^{X_A} \bmod p$ 和 $Y_B = g^{X_B} \bmod p$
3. Alice 和 Bob 交换公钥，计算共享密钥 $K = Y_B^{X_A} \bmod p = Y_A^{X_B} \bmod p$

2. 公钥基础设施 PKI

2.1. PKI 基本概念

1. 是什么？
   - 公钥基础设施, Public Key Infrastructure
   - 用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施。是一种遵循标准的利用公钥加密技术为电子商务的开展提供安全基础平台的技术和规范。能够为所有网络应用提供采用加密和数字签名等密码服务所需要的密钥和证书管理。
2. 为什么要有？
   - 电子政务、电子商务对信息传输的安全需求，统一标准
   - 对可信第三方的需要（CA）
   - 在收发双方建立信任关系，提供身份认证、数字签名、加密等安全服务
   - 收发双方不需要事先共享密钥，通过公钥加密传输会话密钥（数字信封）
3. 基本功能和其他功能: 没找到，ppt 上没有

基本服务：

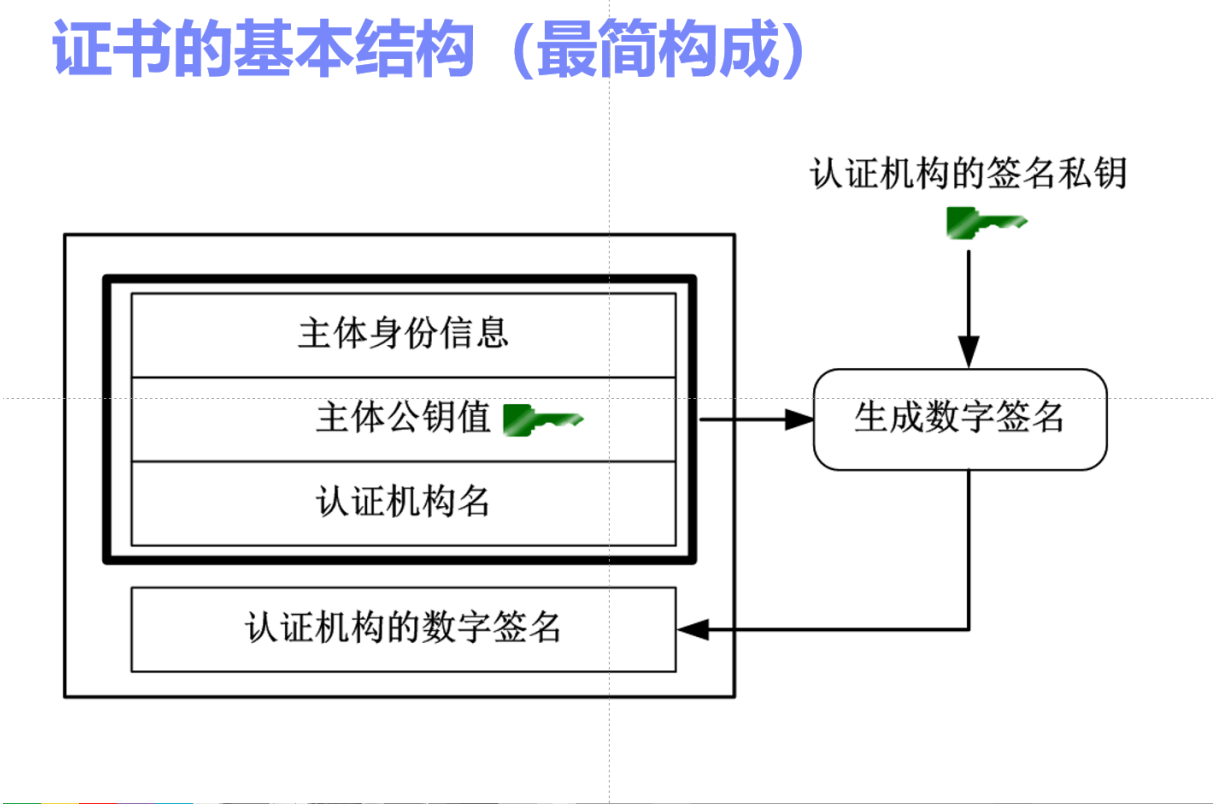
- 认证：实体认证，数据源认证
- 完整性：哈希+数字签名技术,消息认证码(数字信封传输对称密钥)
- 机密性：数字信封传递会话密钥
- 不可否认性：数字签名、时间戳
- 公证：CA 充当可信第三方

2.2. PKI 体系基本组成

- 认证中心 CA(Certification Authority)：证书的签发机构，它是 PKI 的核心构件，是 PKI 应用中权威的、可信任的、公正的第三方机构。

- 注册机构 RA(Registration Authority)：按照特定的政策和管理规范对用户的资格进行审查，并执行是否同意给该申请人发放证书。撤销证书等操作，应注意的是 RA 不容许直接颁发证书或 CRL。RA 作为 CA 的延展，可以增强可扩展性
- 证书库(Certification Library)：CA 颁发证书和证书撤销列表 CRL 的集中存放地，提供公众查询，常用目录服务器提供服务
- 密钥备份及恢复系统：
  - 签名密钥对：签名私钥相当于日常生活中的印章效力，为保证其唯一性、抗否认性，签名私钥不作备份。签名密钥的生命期较长。
  - 加密密钥对：加密密钥通常用于分发会话密钥，为防止密钥丢失时无法解密数据，解密密钥应进行备份。这种密钥应频繁更换。
- 证书作废处理系统：证书由于某种原因需要作废，终止使用，这将通过证书作废列表(CRL, Certification Revocation List)记录
- 自动密钥更新：无需用户干预，当证书失效日期到来时，启动更新过程，生成新的证书
- 密钥历史档案：由于密钥更新，每个用户都会拥有多个旧证书和至少一个当前证书，这一系列证书及相应私钥（除签名私钥）组成密钥历史档案

2.3. 证书的基本结构和基本内容、其他主要内容



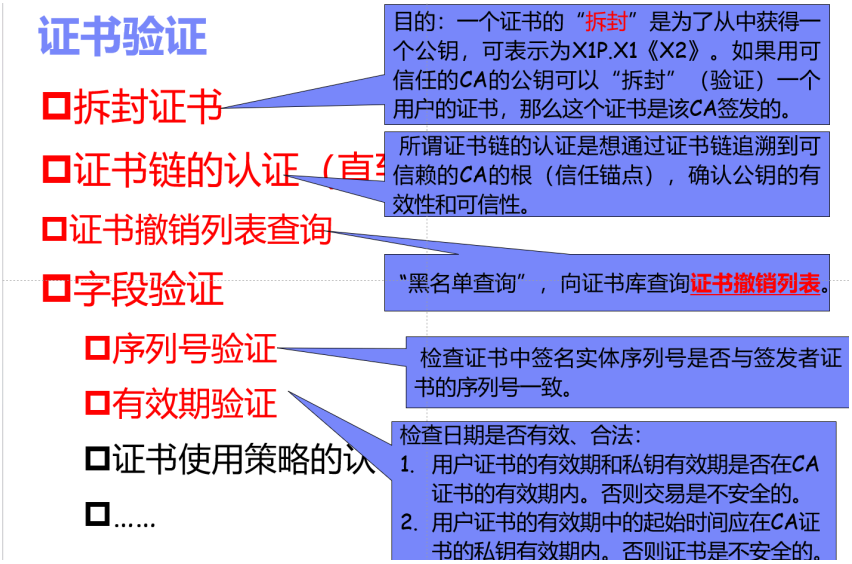
- 基本内容：证书版本, 序列号, 签名算法, 颁发者, 有效期, 主体, 主体公钥, 主体唯一标识, 扩展字段, 签名值
- 其他主要内容，TODO

2.4. 证书生命周期、证书链、交叉认证

生命周期：初始化 → 使用(证书获取, 证书验证, 密钥恢复, 密钥更新) → 撤销

如何产生证书，获取证书的基本流程： 没找到，自己写的 主体将身份信息，公钥和认证机构生成摘要，用 CA 的私钥签名附在证书上

如何验证证书



什么情况下需要撤销证书，如何撤销一个证书

- 私钥泄露、关系终止、CA 签名私钥泄露或者变更
- 存档：维持一个 CRL 和有关历史证书的记录，以便过期的密钥资料加密的数据能够被解密。审计信息: 出于对密钥历史恢复、审计

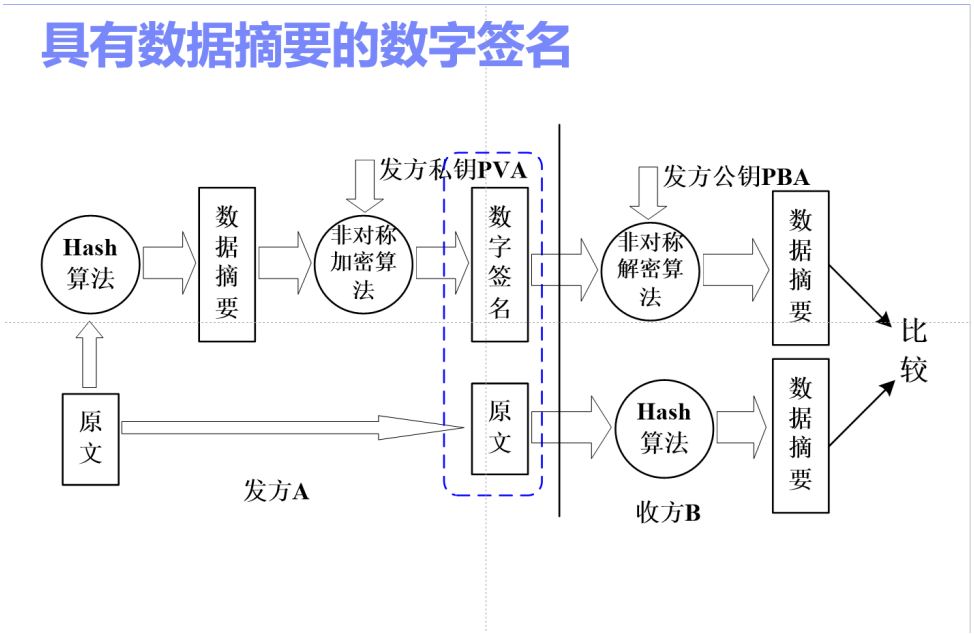
公钥加密、数字签名的密钥对在证书维护上的区别

- 签名密钥不做备份，生命期较长。加密密钥需要备份且经常更换

2.5. 数字签名，数字信封，数字证书

2.5.1. 数字签名

数字签名: 对待发的数据首先基于 Hash 生成一段数据摘要，再采用己方私钥基于非对称加密算法进行加密，结果附在原文上一起发送，接收方对其进行验证，判断原文真伪。从计算开销的角度，这种数字签名方法适用于对大文件的处理。提供数据完整性保护和提供不可否认性服务

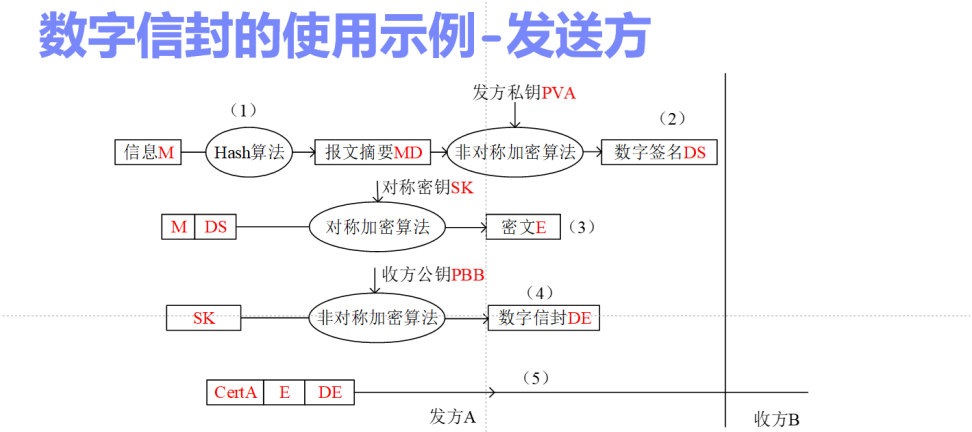


2.5.2. 消息(报文)认证码 MAC

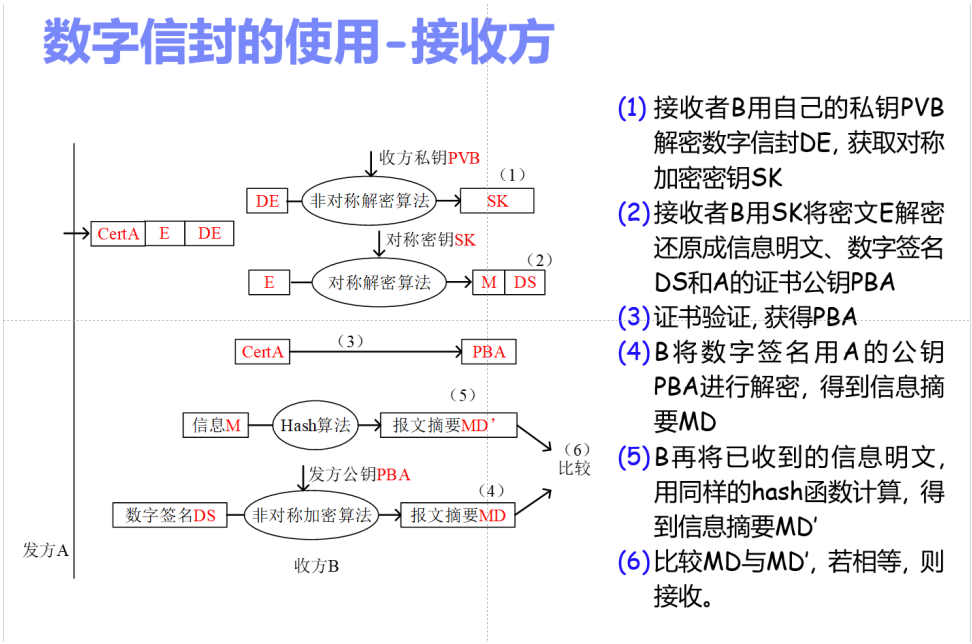
单向哈希函数，数据完整性保护～

2.5.3. 数字信封

- 发送端采用接收端的公钥，将一个通信密钥（即对称加密使用的对称密钥）就行加密，生成一个数字信封。
- 接收端用己方私钥对数字信封进行解密操作，获取该对称密钥，用它来解密收到的基于对称加密的加密信息。



(1) 将要传输的信息进行hash操作后，得到一个数据摘要MD，MD=hash（信息）
(2) 发送者A用自己的私钥PVA对数据摘要MD进行加密，得到A的数字签名DS
(3) 发送者A将信息明文、数字签名和它的证书上的公钥三项信息，通过对称算法，用对称密钥SK进行加密，得密文E
(4) 发送者在发送信息之前，必须事先得到接受方B的证书公钥PBB，**用PBB加密SK，形成一个数字信封DE**
(5) E+DE+CertA就是将密文与数字信封连接起来，并可选地附带证书，既A所发送的内容



3. IPSec: AH, ESP 与 IKE

3.1. 安全关联 SA

SA(Security Association)定义：为使通信双方的认证/加密算法及其参数、密钥的一致，相互间建立的联系被称为安全组合或安全关联

SA 由一个三元组唯一地标识，该三元组为安全参数索引 SPI、一个用于输出处理的目的 IP 地址和协议（如 AH 或 ESP）

注：三元组唯一标识 SA, 相当于一个主键, 而非 SA 由三个元素组成. SA 有以下域：

- 序列号计数器：32 位整数，用于生成 AH 或 ESP 头中的序列号
- 序列号溢出：一个标志，标识是否对序列号计数器的溢出进行审核。
- 抗重放窗口：使用一个 32 位计数器和位图确定一个输入的 AH 或 ESP 数据包是否是重放包
- AH 的认证算法和所需密钥
- ESP 的认证算法和所需密钥
- ESP 加密算法，密钥，初始向量（IV）和 IV 模式
- IPSec 操作模式：传输模式或者隧道模式
- 路径最大传输单元(Path Maximum Transfer Unit, PMTU)
- SA 生存期

安全参数索引(Security Parameter Index, SPI):

- SPI 是为了唯一标识 SA 而生成的一个 **32 位整数**，由**目的端**确定。包含在 AH 头标和 ESP 头标中，其值 1～255 被 IANA 留作将来使用，0 被保留，目前有效的值为 256 ~ $2^{32}-1$
- 有了 SPI，相同源、目的节点的数据流可以建立多个 SA，也可以方便地各自被唯一标识

不同方向可能存在不同的策略，因此 SA 是**单向的**，在双向通信时要建立两个 SA。对于某一主机来说，某个会话的输出数据和输入数据流处理需要两个独立的 SA。

3.2. 安全关联 SA（包含的基本内容）、SAD、SPD

SAD(Security Association Database)：存储 SA 的数据库，每个 SA 由三元组 (相当于主键)进行索引

安全策略数据库（SPD）：SPD 中包含一个策略条目的有序表，通过使用一个或多个选择符来确定每一个条目。选择符可以是五元组（目的/源地址，协议，目的/源端口号），或其中几个，理论上可以根据数据包的任何一个域来确定。条目中包含：

- 策略（是否需要 IPSec 处理）：丢弃，绕过不使用 IPSec，加载 IPSec
- SA 规范
- IPSec 协议（AH/ESP）
- 算法
- 操作模式
- 对外出处理，应在 SPD 中查找指向 SAD 中 SA 的指针

3.3. AH/ESP 在源端和目的端的处理流程

- AH(Authentication Header, 认证头标)：无连接的数据完整性、数据源认证和抗重放保护服务. 不提供保密性
  - 源端外出处理:
  1. 使用相应的选择符(目的 IP 地址、端口号和传输协议等)查找安全策略数据库 SPD 获取策略。如需要对分组进行 IPSec 处理，且到目的主机的 SA 已经建立，那么符合分组选择符的 SPD 将指向外出 SA 数据库（SAD）的一个或者多个 SA。如果 SA 还未建立，IPSec 将调用 IKE 协商一个 SA，并将其连接到 SPD 条目上。
  2. 产生或增加序列号，当一个新的 SA 建立时，序列号计数器初始化为 0，以后每发一个分组，序列号加 1
  3. 计算 ICV（完整性校验值）
  4. 转发分组到目的节点
  - 目的端进入处理:
  1. 如 IP 分组中无 IPSec 选项，则分组中的选择符进入 SPD 查找一条与选择符匹配的策略，检查策略是否相符。如果无需进行 IPSec 处理则放行，否则丢弃
  2. 使用 IP 分组头中的 SPI 值、目的 IP 地址以及 IPSec 协议在进入的 SA 数据库中查找 SA，如果查找失败，则抛弃该分组，并记录事件。
  3. 使用已查到的 SA 进行 IPSec 处理。
  4. 检查序列号，确定是否为重放分组
  5. 使用 SA 指定的 MAC 算法计算 ICV，并与认证数据域中的 ICV 比较，如果两值不同，则抛弃分组

- ESP(Encapsulating Security Payload, 封装安全载荷): 数据保密、无连接完整性（可选，不覆盖 IP 头标）、数据源认证、抗重放攻击
  - 源端外出处理:
  1. 使用分组的相应选择符（目的 IP 地址、端口、传输协议等）查找安全策略数据库（SPD）获取策略，如分组需要 IPSec 处理，且其 SA 已建立，则与选择符相匹配的 SPD 项将指向安全关联数据库（SAD）中的相应 SA，否则则使用 IKE 建立 SA。
  2. 生成或增加序列号
  3. 加密分组，SA 指明加密算法，一般采用对称密码算法
  4. 计算完整性校验值(可选)
  - 目的端进入处理:
  1. 使用目的 IP 地址、IPSec 协议、SPI 进入 SAD 检索特定 SA，如果查找失败，则丢弃分组
  2. 策略验证：使用分组的选择符进入 SPD 中查找与之匹配的策略，根据策略检查该分组是否满足 IPSec 处理要求
  3. 检查抗重放功能

4. 如 SA 指定需要认证，则检查数据完整性
5. 解密

3.4. AH, ESP 头标，保护范围

- AH 的认证范围是整个 IP 分组（除了头标中的可变域）
- ESP 的认证范围不包括头标，加密范围包括除了 IP 头标和 ESP 头标的部分

3.5. AH, ESP 同时使用的顺序问题

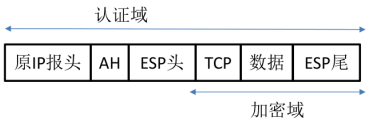
先用 ESP 加密，再用 AH 认证. 理由：若先 AH 再 ESP，接收方需要先解密后验证，接收方需要在不确定数据是否正确的情况下执行解密操作,增加计算开销 (hw9.8)

新 IP 头	AH 头标	原 IP 头	ESP 头标	TCP 头标	数据	ESP 尾标	ESP 认证数据

习题9.7 两个主机之间实现端对端加密和认证

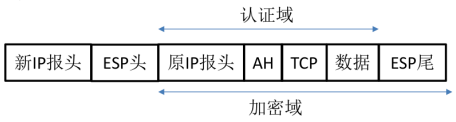
9.7 在两个主机之间需要实现端对端加密和认证。请画出类似于图 9.8 的示意图来说明：
a. 传输邻接，先加密后认证。
b. 一个隧道 SA 中有一个传输 SA，先加密后认证。
c. 一个隧道 SA 中有一个传输 SA，先认证后加密。

a.传输邻接，先加密后认证

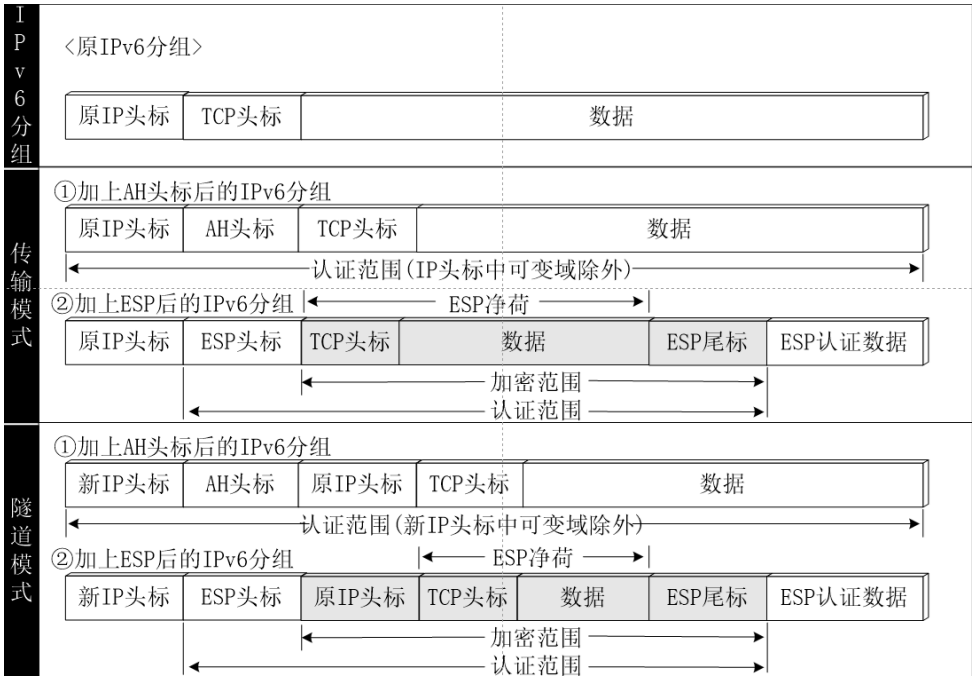


b.一个隧道SA中有一个传输SA，先加密（ESP）后认证（AH）

c.一个隧道SA中有一个传输SA，先认证（AH）后加密（ESP）



3.6. 工作模式：传输模式和隧道模式



隧道模式理解：

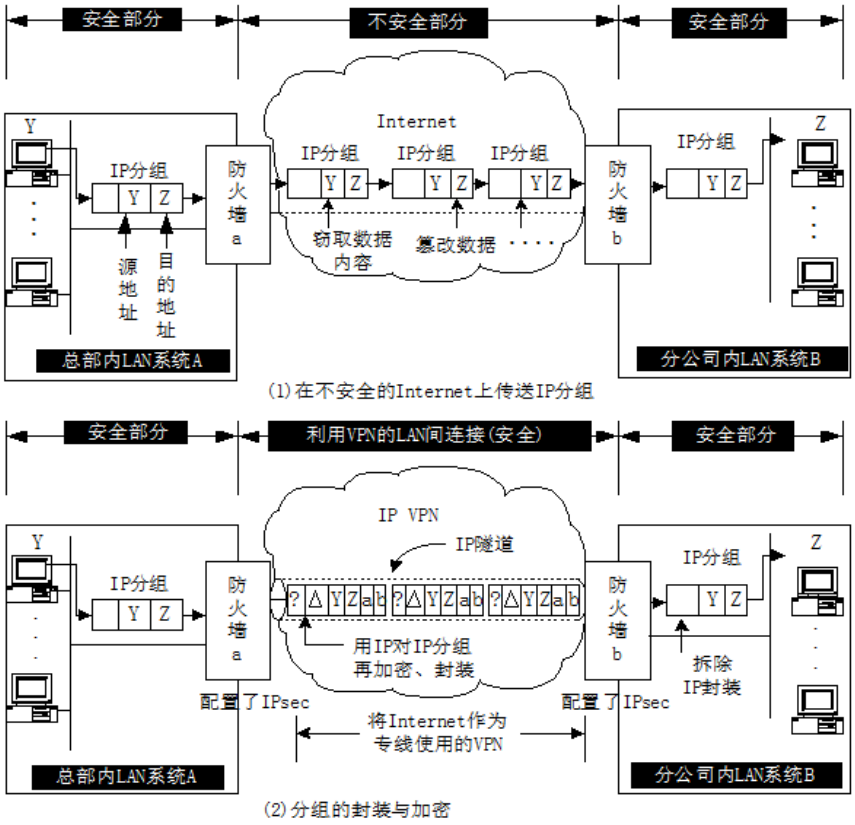
- 使用场景: IPSec VPN, 即使用公用网络建立私有网络. 把一个包从一个子网发出后, 需要经过公网然后再进入另一个子网, 到新子网里去寻找主机. 为了防止接收端主机的 IP 地址被泄露, 在公网搭建一个隧道, 新 IP 头是新子网的入口路由器的 IP 地址, 旧 IP 头是原始的 IP(目的主机)地址. 这样, 从公网看, 数据包是从入口路由器发出的, 从而隐藏了接收端主机的 IP 地址.
- 故需要将原 IP 头进行封装，加上新的 IP 头，这样的模式称为隧道模式

3.7. IPSec 与 NAT 产生冲突的原因

NAT-PT 通常在防火墙或网关上实现，对过往的 IP 地址、端口号进行转换。具有 AH 头标或 ESP 头标的的 IP 分组不能穿越 NAT 和 NATPT

- 地址的修改使得接收端的 AH 认证失败
- 上层端口号信息的 ESP 加密，使得端口无法被得知，无法进行 NAT-PT
- 上层 TCP/UDP 中校验和计算涉及伪头标，包括 IP 地址和端口，通过 ESP 认证，校验和字段不能被修改，上层会校验验证失败
- 针对 ESP 问题，IETF 的解决方案：在 ESP 头标前插入一个 UDP 头标

3.8. IPSec VPN

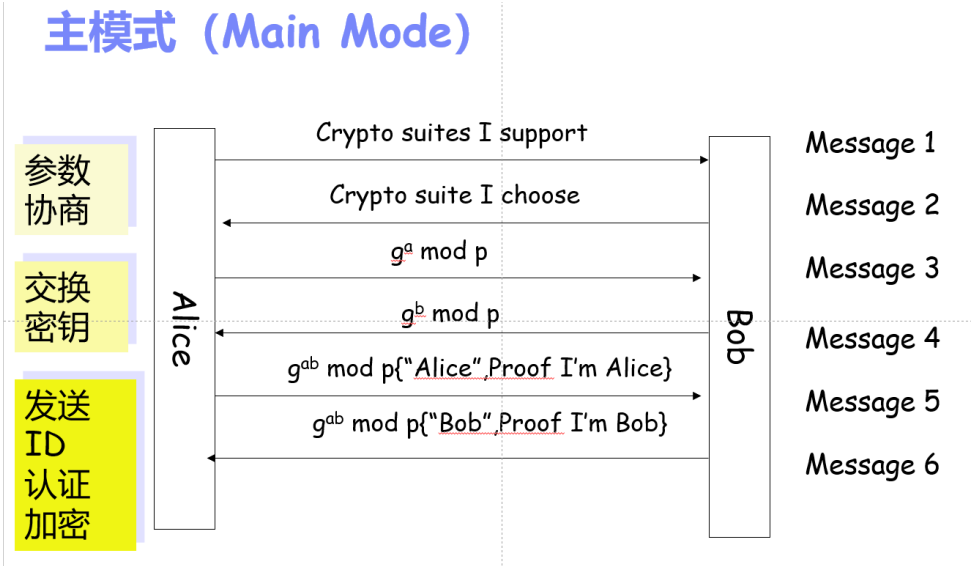


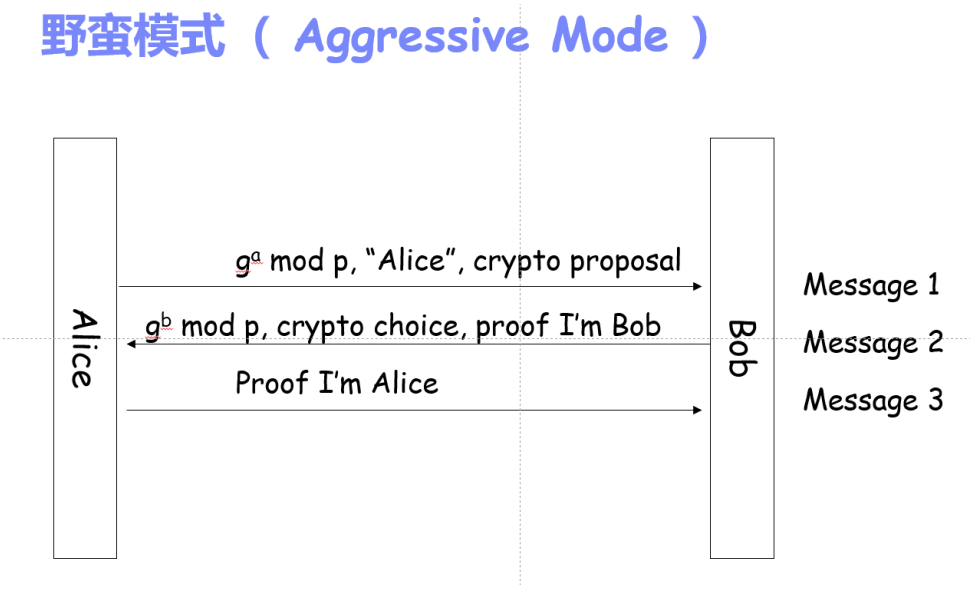
3.9. IKE（不拘泥于协议细节的记忆）

IKE（Internet Key Exchange, 因特网密钥交换协议): 是一个以受保护的方式动态协商 IPsec SA 的协议。

IKE 的功能：使用某种长期密钥进行双向认证并建立短期会话密钥

3.9.1. 不同模式存在的原因、大致流程（主模式和野蛮模式）





4. SSL/TLS

4.1. SSL 的基本层次结构、安全服务

- 底层：记录协议
- 上层：握手协议、密码变化协议、警告协议、用户数据

SSL 协议的基本描述: SSL 协议是一种基于公钥加密技术的安全协议，它在应用层和传输层之间提供了一种安全的通信机制。SSL 协议的基本功能是为通信双方提供数据的机密性、完整性和不可否认性。

SSL 解决的问题：

- 客户对服务器的认证：SSL 服务器允许客户的浏览器使用标准的公钥加密技术和一些可靠的认证中心（CA）的证书，来确认服务器的合法性。
- 服务器对客户的认证：公钥+证书/用户名+口令
- 建立服务器与客户之间安全的数据通道：SSL 要求客户与服务器之间的所有发送的数据都被发送端加密、接收端解密，同时还检查数据的完整性

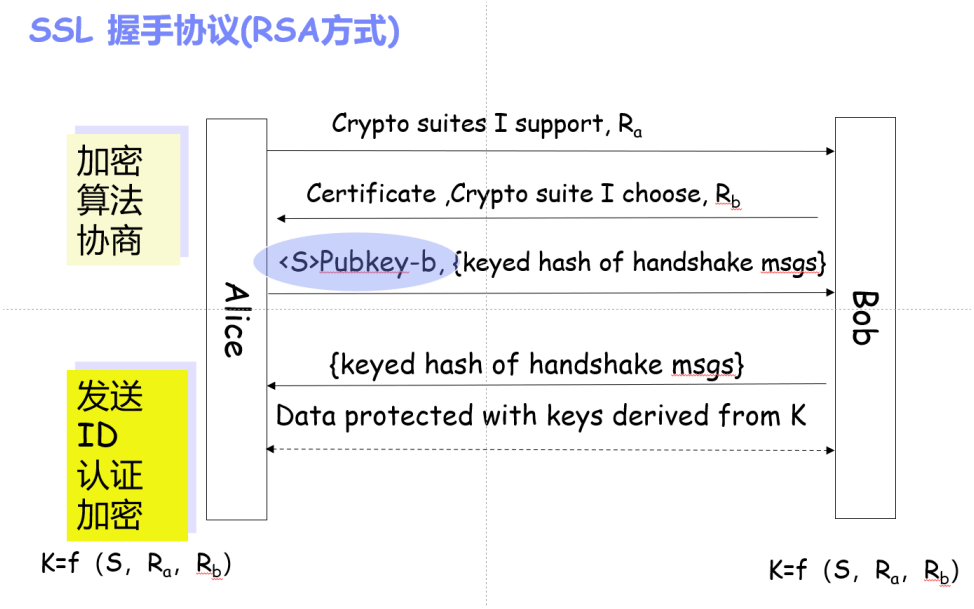
SSL 提供的服务：

- 用户和服务器的合法性认证：X.509 数字证书
- 传输数据机密性：DES, 3DES, RC2, RC4, IDEA…
- 传输数据完整性：MAC-MD5, MAC-SHA1…

4.2. 安全操作流程：握手协议、会话重用

4.2.1. 握手协议

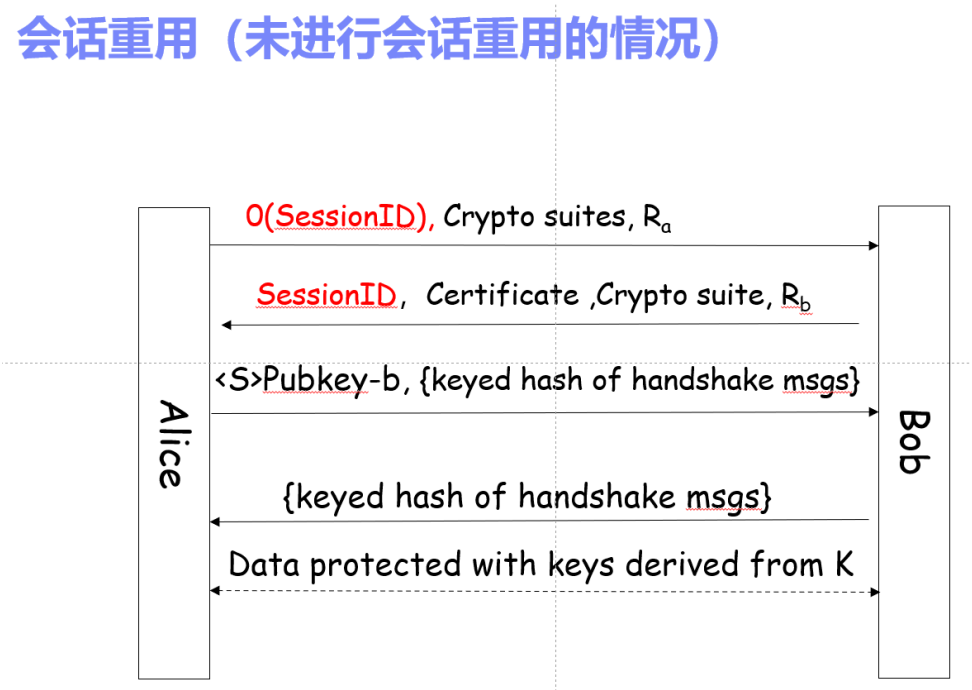
下图中的<S>Pubkey-b 是用 Bob 公钥加密的 pre-master key。最终主密钥 $K = f(S, R_a, R_b)$ 。对于每个连接，每个方向上各三个密钥，分别为加密密钥、完整性保护密钥、IV：$g_i(K, R_a, R_b)$，利用主密钥派生。



上述步骤有点省略，文字详解如下：

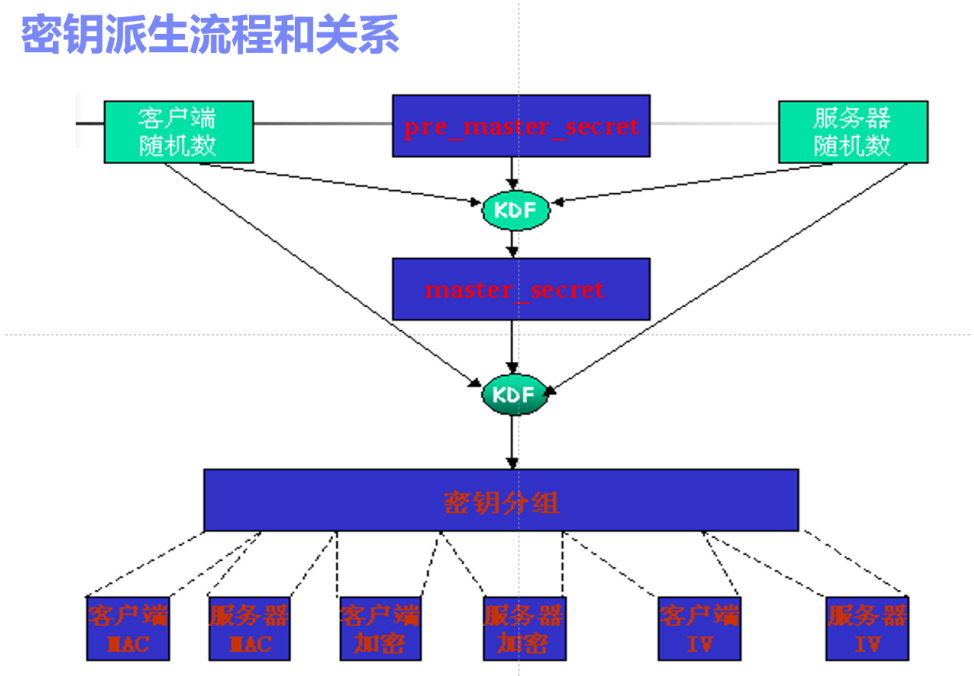
1. Alice 和 Bob 相互发送自己的随机数 R_a 和 R_b和 SSL/TLS 版本号
2. Alice 找一个预主密钥(pre-master **key**, K_{pre}), 用 B 的公钥 P_B 加密得到 pre-master **secret** $S = E(K_{\text{pre}}, P_B)$, 发送给 Bob. 同时 Alice 计算出主密钥 $K = f(S, R_a, R_b)$, 用 K 加密握手信息的哈希值发送给 Bob
3. Bob 计算出主密钥 $K = f(S, R_a, R_b)$, 用 K 加密握手信息的哈希值发送给 Alice

4.2.2. 会话重用



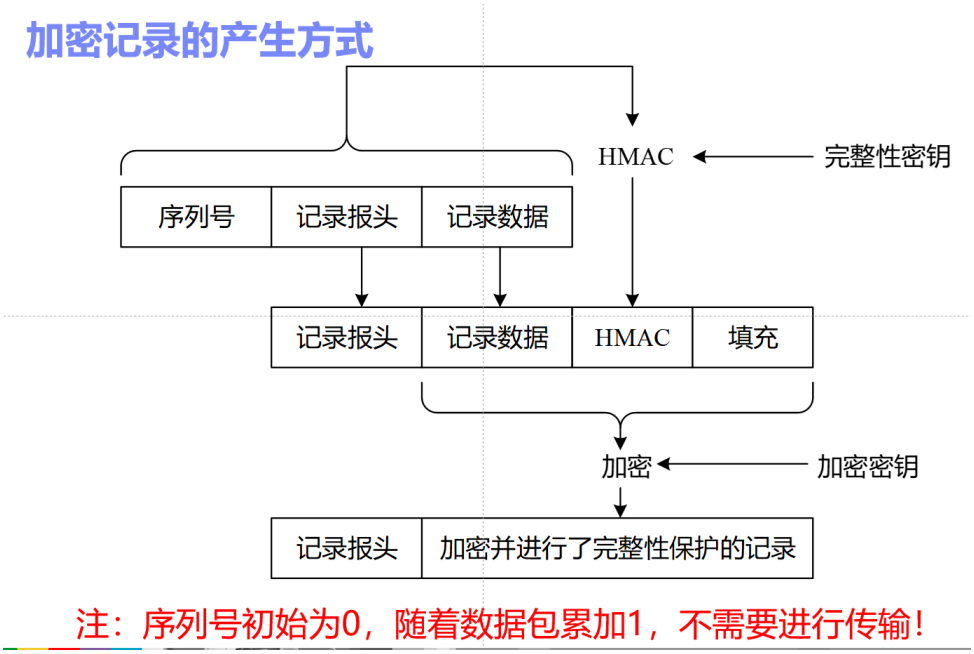
Bob返回相同的Session代表同意会话重用，返回不同的Session则和未进行重用的情况一样操作

4.2.3. 密钥派生



4.3. SSL 的数据保护原理

数据处理过程：加密和完整性保护（加密记录的产生方法） 序列号的使用



5. 防火墙和 NAT

5.1. 防火墙种类、功能

- 包过滤型防火墙
- 状态检测防火墙
- 应用级网关型防火墙
- 代理服务型防火墙(电路级网关)
- 复合型防火墙

功能：

- 访问控制：隔断、过滤、代理
- 状态检测
- 加密
- 授权认证
- 地址翻译（NAT）
- VPN
- 负载均衡
- 内容安全：病毒扫描、URL 扫描、HTTP 过滤
- 日志记帐、审计报警
- 攻击防御

5.1.1. （重点）包过滤型和状态检测型

5.1.1.1. 包过滤型

通常在路由器的网络层实现，实际上是一种网络层的访问控制机制

工作原理：

- 过滤的规则以五元组，即 IP 和传输层的头中的域(字段)为基础，包括源和目标 IP 地址、IP 协议域、源和目标端口号。区分出入

- 过滤器往往建立一组规则，IP 包自上而下进行匹配，根据 IP 包是否匹配规则中指定的条件来作出决定。
  - 如果匹配到一条规则，则根据此规则决定转发或者丢弃
  - 如果所有规则都不匹配，则根据缺省策略（放行 or 丢弃）

5.1.1.2. 状态监测型

通过建立一个出网的 TCP 连接目录而加强 TCP 数据流的检测规则(连接记录)。即状态检测防火墙 = 包过滤防火墙 + 连接记录。报文过滤机制只允许那些和目录中某个连接匹配的数据流通过防火墙

5.1.2. 单宿主主机、双宿主主机以及屏蔽子网结构

单宿主主机（屏蔽主机结构）: 包过滤路由器和堡垒主机一起构成安全系统，堡垒主机暴露在外网攻击下，只允许堡垒主机与外部直接通信，内部其他主机与外部通信必须经过堡垒主机。

适用于只对外提供较少的服务，外部的来的连接比较少，以及内部主机安全性配置较好的环境

缺点：

- 堡垒主机与其他主机在同一个子网
- 一旦包过滤路由器被攻破或被越过，整个内网和堡垒主机之间就再也没有任何阻挡。

双宿主主机：

- 有两块网卡
- 可以是包过滤软件/硬件、应用层代理
- 增加了单一故障点，影响网络吞吐量
- 只有同时攻破堡垒主机和路由器内部才是不安全的
- 使用环境：去往 Internet 流量小，可靠性要求不高，不对外提供服务
- 难点：如何保证双宿主主机安全

屏蔽子网结构： DMZ（Demilitarized Zone），非军事区或者停火区：

- 包含两个包过滤路由器
  - 外部路由器：只允许对 DMZ 的访问，拒绝所有以内部网络地址为目的地址的包进入内部网络。
  - 内部路由器：保护内部网络，防止来自 Internet 或 DMZ 的非法访问，拒绝外部发起的一切连接，只允许内部对外的访问，在特定需要前提下，可以允许从堡垒主机来的访问，从内部往外的访问也可以限制为必须通过堡垒主机。
- 在内部网络和外部网络之间创建了一个新的子网，可能只包含堡垒主机，也可能还包含一个或者多个信息服务器（所有对外服务在 DMZ 完成）
- 内外网通信必须经过堡垒主机

5.1.3. 基本状态检测型防火墙对 FTP 主动和被动连接处理上的区别

好像是作业题

5.2. NAT 的基本原理、类型、功能

NAT（网络地址转换）可以划分为以下两种类型（从发起者的报文）：

- 源网络地址转换(SNAT，即 IP 伪装)：复用内部的全局地址，解缓 IP 地址不足的压力。同时可以向外部隐藏内部 IP
  - 对于传出数据包，源 IP 地址(专用地址)被映射到 ISP 分配的地址(公用地址)，并且 TCP/UDP 端口号也会被映射到不同的 TCP/UDP 端口号，建立映射表信息。

    - 对于传入数据包，根据映射表信息，目标 IP 地址(公用地址)被映射到源 Internet 地址(专用地址)，并且 TCP/UDP 端口号被重新映射回源 TCP/UDP 端口号。
- 目的网络地址转换(DNAT)：在实现 SNAT 的环境下进行有效的服务访问，以及流量均衡

实现方式：

- NAT
    - 静态 NAT（Static NAT）：内部网络地址与 NAT 地址和端口号一一对应
    - 动态 NAT（Dynamic NAT）：多对多
- NAT-PT：过载：一对多

注：静态 NAT 和动态 NAT 不是 SNAT 和 DNAT 的同义词

5.2.1. SNAT、DNAT 的基本作用、内核中处理位置

- SNAT(Source NAT):
    - 复用内部的全局地址，解缓 IP 地址不足的压力
    - 向外部网络隐藏内部网络的 IP 地址
- DNAT(Destination NAT):
    - 在实现 SNAT 的环境下进行有效的服务访问
    - 流量均衡

5.2.2. Iptables/netfilter 的基本使用

PPT 没有，就当不考

5.2.3. 基本组网原理：交换机、路由器等的基本概念

计网学了，不写了

6. VPN

6.1. VPN 种类、功能（简单了解）

- 可以实现不同网络的组件和资源之间的相互连接。虚拟专用网络能够利用 Internet 或其它公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。
- 并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。
- 是通过隧道技术在公共数据网络上虚拟出一条点到点的专线技术。

用来保证安全的技术：隧道技术, 加解密技术, 密钥管理技术, 认证技术, 访问控制

VPN 分类：

- 按照隧道协议分类：
    - 基于第二层隧道技术的 VPN：L2F，PPTP，L2TP
    - IPSec VPN
    - SSL VPN
    - MPLS VPN
    - GRE VPN
- 按照应用类型分类：远程访问型, LAN 间互连

6.2. IPSec VPN （重点）

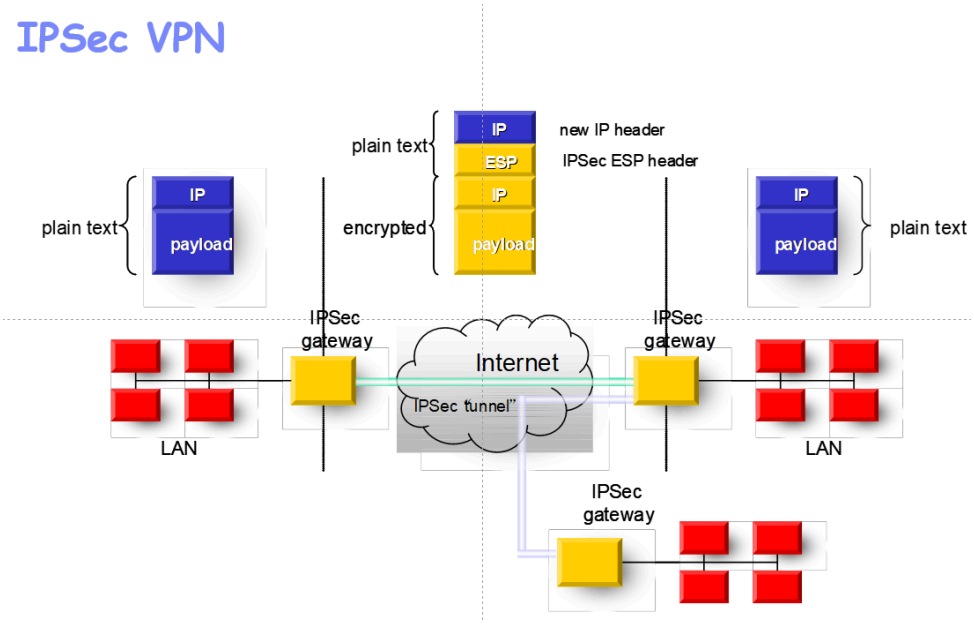
IPSec 不是一个单独的协议，而是一套协议包，包括三个基本协议

- AH 协议提供信息源验证和完整性保证；
- ESP 协议提供信息源验证、机密性和完整性保证；

- IKE 提供密钥协商（IKEv1、IKEv2）

注：IPSec 在网络层上提供安全服务：定义了两个协议 AH 和 ESP；IPSec 在 IP 层提供安全服务，使得系统可以选择所需要的安全协议，确定该服务所用的算法，并提供安全服务所需任何加密密钥

- 提供安全的网络传输服务
- 主要适用于 LAN 间 VPN（隧道模式）
- IKE 支持动态密钥交换，采用预共享密钥或公钥机制认证身份，协商加密、认证密钥
- 具有数据传输的完整性认证、加密功能
- 实现方式
  - VPN 专用设备
  - 将 IPSec 嵌入到防火墙软件
  - 将 IPSec 嵌入到路由器软件
  - 动态 IP 地址的 IPSec VPN（利用动态域名服务器



6.3. MPLS(不考)

7. PGP, SET, WEP

7.1. PGP(Pretty Good Privacy)

7.1.1. 基本功能、安全服务、操作原理

安全业务：

- 加密：发信人产生一次性会话密钥，以 IDEA、3-DES 或 CAST-128 算法加密报文，采用 RSA 算法用收信人的公钥加密会话密钥，并和消息一起送出。
- 认证：用 SHA-1 对报文杂凑，并以发信人的私钥签字，签名算法采用 RSA 或 DSS 。
- 压缩：ZIP，用于消息的传送或存储. 流程: 签名 ⟶ 压缩 ⟶ 加密。在压缩前签名，压缩后加密。原因：之所以在压缩前签名是因为不同时刻压缩结果可能不同，若在压缩后签名可能

导致认证失效。之所以在签名后加密是因为接收端保留明文和签名，而不会保存会话密钥，这么操作有利于接收方随时验证签名。
- 兼容性：由于历史原因，Email 只被允许传送 ASCII 字符。采用 Radix-64 可将加密的报文转换成 ASCII 字符，将原报文扩展了 33%.
- 数据分段：PGP 具有分段和组装功能，适应最大消息长度限制

7.1.2. 公钥环, 私钥环

加密密钥和密钥环：PGP 使用四种类型的密钥：一次性会话对称密钥，公钥，私钥，基于对称密钥的口令，需求：
- 需要生成不可预测的会话密钥（随机算法）
- 需要某种手段来标识具体的密钥（一个用户可拥有多个公钥/私钥对，以便随时更换且让对方知道来自哪个密钥对）
  - 将公钥与消息一起传送
  - 将一个标识符（KeyID = KUa mod 2^{64}）与一个公钥关联，对一个用户来说做到一一对应
- 每个 PGP 实体需要维护一个保存其公钥/私钥对的文件和一个保存通信对方公钥的文件
  - 存储该节点拥有的公钥/私钥对私钥环（口令保护密钥）
  - 存储本节点知道的其他用户的公钥环

7.1.3. 密钥的标识 KeyID（公钥的低 64 位）

- 一个用户有多个公钥/私钥对时，接收者如何知道发送者是用了哪个公钥来加密会话密钥，方法：
  - 将一个标识符（KeyID）与一个公钥关联，对一个用户来说做到一一对应即可
- 定义 KeyID 包括 64 个有效位，(KUa mod 2^{64})

7.1.4. 私钥的保存

每个 PGP 实体需要维护一个保存其公钥/私钥对的文件和一个保存通信对方公钥的文件，该文件存储该节点拥有的公钥/私钥对，私钥环（口令保护密钥）和本节点知道的其他用户的公钥环

7.2. SET 协议

基本概念：
- 安全电子交易协议 SET（Secure Electronic Transaction）是由 Visa 和 Master Card 所开发的，为了在 Internet 上进行在线交易时，保证信用卡支付的安全性而设计的开放规范，已得到 IBM、HP、Microsoft 等大公司的支持，已成为事实标准，并获得 IETF 标准认可（RFC3538）
- SET 提供了消费者、商家和银行之间的认证，确保了网上交易数据的保密性，数据的完整性以及交易的不可抵赖性。特别是能保证不将消费者银行卡号暴露给商家，不将消费者的购物信息暴露给银行等优点，因此它成为目前公认的信用卡/借记卡网上交易安全标准
- SET 采用公钥密码体制，遵循 X.509 数字证书标准

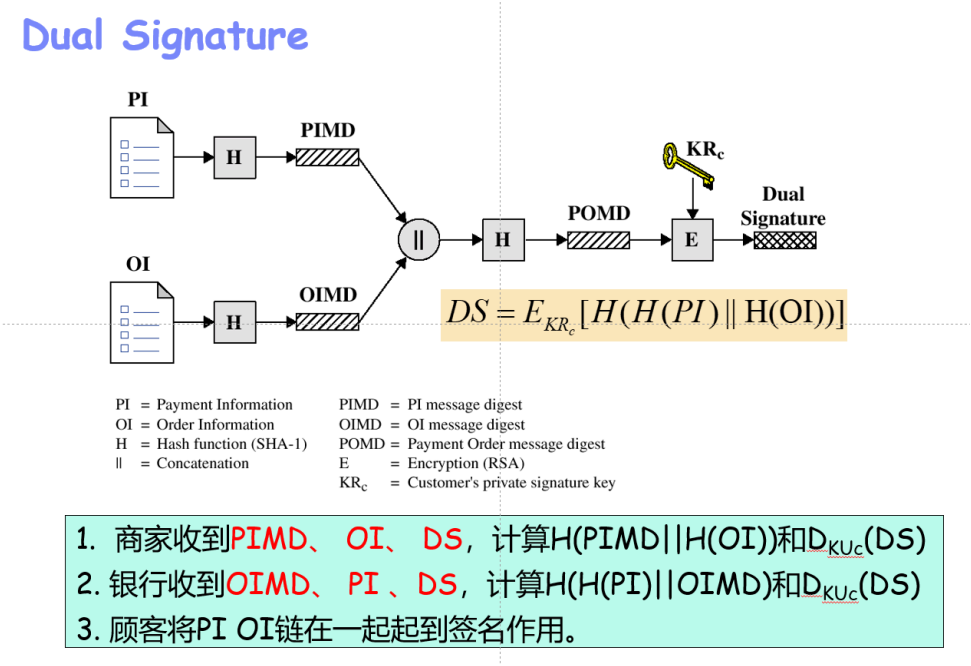
参加 SET 协议的主要实体有：持卡人，商家，支付网关 **注：**主要实体跟上面的"消费者，商家和银行不一样", 2022 年期末填空题有

7.2.1. 数字信封

上面讲了

7.2.2. 双重数字签名

- 发送者寄出两个相关信息给接收者，对这两组相关信息，接收者只能解读其中一组，另一组只能转送给第三方接收者，不能打开看其内容。这时发送者就需分别加密两组密文，并针对两组明文信息联系起来并进行签名，称其双重数字签名。
- 应用场合：电子商务购物、付款。是 SET 和 non-SET 中常用



1. 商家收到PIMD、 OI、 DS，计算H(PIMD||H(OI))和D_{KUc}(DS)
2. 银行收到OIMD、 PI 、DS，计算H(H(PI)||OIMD)和D_{KUc}(DS)
3. 顾客将PI OI链在一起起到签名作用。

7.3. WEP(Wired Equivalent Privacy)

7.3.1. WLAN 的基本概念，安全需求

WLAN 标准：802.11 系列 建立方式：

- Ad-hoc：一群使用无线网卡的 Station，直接相互连接，资源共享，无需通过接入点（AP）
- Infrastructure Mode：所有 Station 通过接入点连接成网络实现资源共享

安全需求 无线网络安全缺陷：物理链路开放，窃听、通信阻断、注入攻击、中间人攻击、客户端/AP 伪造

7.3.2. 杂项

- 漫游认证、切换认证的区别，可能的方法
- 802.1x 基本认证架构和流程
- Radius 功能和参与认证的操作流程
- WEP 安全服务：RC4+CRC32
- 增强方案举例：WPA、802.11i(WPA2)、WAPI

8. 计算机网络、密码学基础

- TCP、UDP、IP 协议，FTP、Email 相关协议，交换机、路由器等相关设备
- 基本的密码学算法
  - 对称、非对称、Hash 函数、HMAC
  - 对称加密数据，公钥加密会话密钥（数字信封）、私钥签名（结合 Hash）、HMAC 提供数据源认证和完整性保护

附录 A 2022 年期末自制题解

1. 填空题(20 分)

1. 被动攻击不易被察觉的原因是不会改变网络数据
2. 3A 的构成认证(Authentication)、授权(Authorization)、记账(Accounting)
3. 证书的构成：主体信息、主体公钥值、认证机构名、认证机构的数字签名
4. IPsec 协议中, 提供密钥协商的是 IKE, 提供认证服务的是 AH, 提供保密性服务的是 ESP
5. SET 协议参与的主要实体是持卡人、商家、支付网关
6. 对于 WEP 协议升级改进的两个版本，其中国际提出的是 WPA, 国内提出的是 WAPI
7. 会话重用的判断条件是 Session ID
8. 同时实现 AH 和 ESP 需要 4 个 SA
9. 在计网和网络安全协议中防火墙实验采用的软件是这我哪知道啊，盲猜 iptables
10. PKI 中发放证书的是 CA，进行资格审查的是 RA

2. 不定项选择题(20 分)

1.关于防火墙提供的服务说法不正确的是 (D)
A. 不能阻止那些绕开防火墙的攻击
B. 不能防止内部攻击
C. 不能防止病毒感染程序或文件的传输
D. 不能防止使用端-端加密的过程

2.下面选项中防火墙一般不检测的是 (D)
A.端口号 B.IP 地址 C.协议号 D.载荷

3.SA 三元组内容不包括 (D)
A.安全参数索引 B.目的 IP 地址 C.协议 D.源 IP 地址

4.检查一个证书的内容（即需要检查什么）

5.WEP 协议的相关内容

6.VPN 的适用场景

7.数字签名的使用条件（即采用什么方法）（记不清了，不确定）

8.下列不是 AH 协议提供的服务是 (D)
A.无连接的数据完整性 B.抗重放保护 C.数据源认证 D.保密性服务

9.下列不是 PRF 伪随机数函数起到的作用是(B)
A.协商主密钥 B.协商预主密钥 C.协商 MAC 密钥 D.协商 IV

10.下面说法正确的有 (D)
A.PGP 中的基 64 转换扩展率为 50%，目的是为了兼容性
B.SSL 是基于 UDP 的协议
C.SSL 中服务器端认证是可选择的，客户端认证是必须的
D.PGP 中加密、压缩、签名的先后顺序为: 签名 ⟶ 压缩 ⟶ 加密
E.?

3. 解答题(60 分)

1.(8 分)

(1) 什么是数字信封?
数字信封是指将一个会话密钥用接收者的公钥加密，然后将密文和明文一起发送给接收者，接收者用自己的私钥解密得到会话密钥，再用会话密钥解密密文。
(2) Alice 向离线的 Bob 发送一个 200M 的文件，设计一个方案使之满足完整性、保密性、?（还有一个忘了）
方案: 数字信封

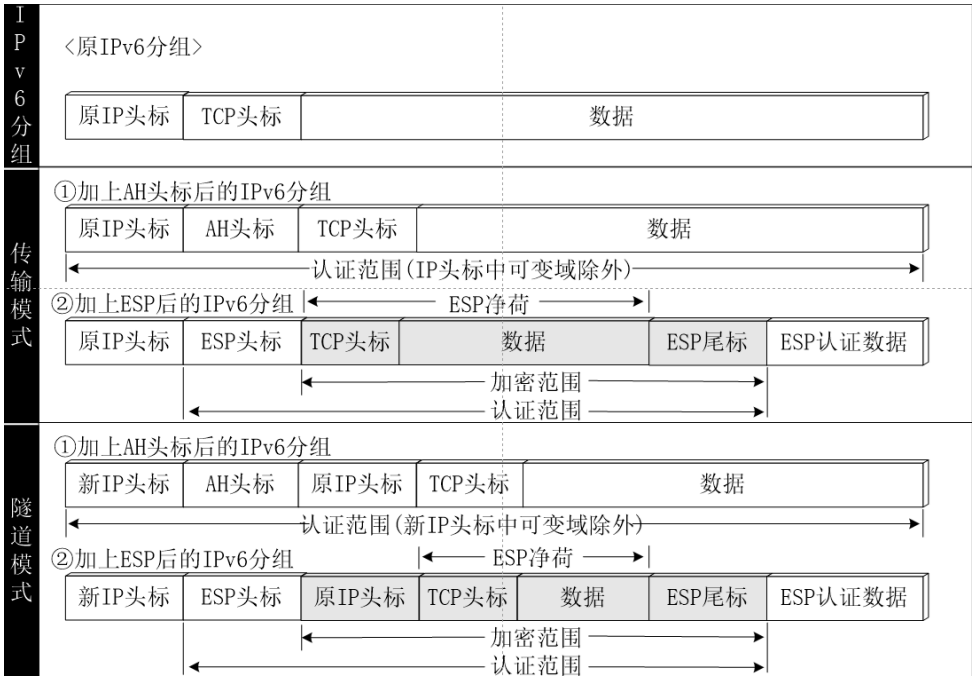
2.(6 分)数据完整性保护的基本方法有两种，叙述之，并说明源端的处理办法以及适用场景（小测原题）

- 两种方法：数字签名和 MAC
- 数字签名：发送方用自己的私钥对消息摘要(MD)进行签名，接收方用发送方的公钥验证签名，适用于需要保证数据源的场景
- MAC：发送方用密钥对消息进行计算，生成一个固定长度的值

3.(5 分)叙述 SNAT 和 DNAT 的作用

- SNAT：将内部网络的私有地址映射到公共地址，解决了地址不足的问题，同时隐藏了内部网络的 IP 地址
- DNAT：在实现 SNAT 的环境下进行有效的服务访问，以及流量均衡

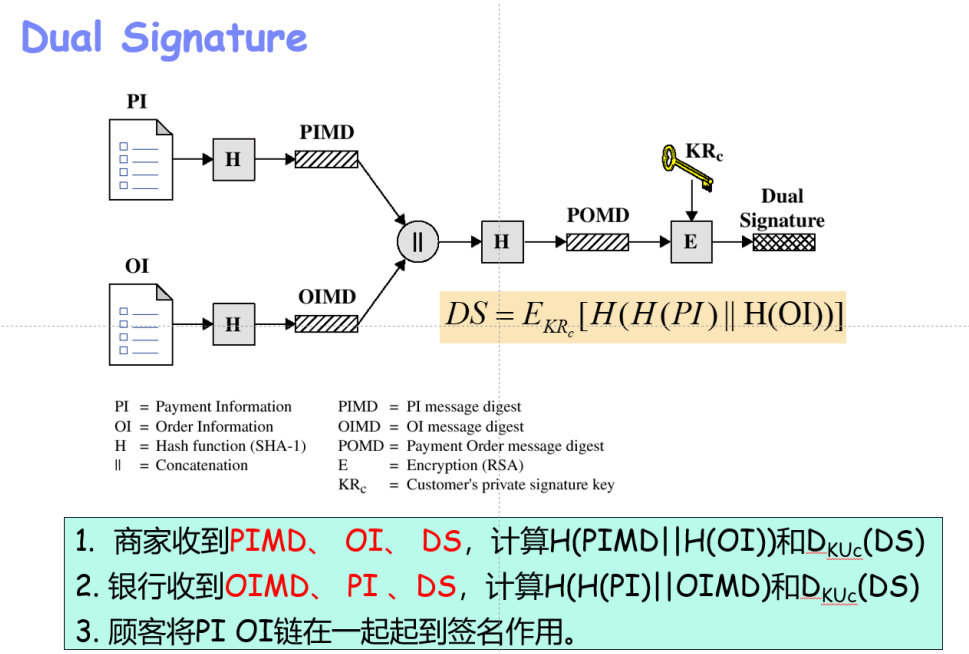
4.(4+4 = 8 分)画出 AH 头标在传输模式和隧道模式下的位置，以及相应的认证范围



5.(6 分)给出非对称加密（不是数字签名）下的一种提供身份认证的办法（小测原题）

- 挑战应答：将随机数用接收方的公钥加密发送给对方，要求其使用私钥解密并返还此随机数

6.(6 分)双重数字签名的实现方法



7.(3+3=6 分)(整个题目背景是 PGP)

(1) 怎么保存一个私钥?

每个 PGP 实体需要维护一个保存其公钥/私钥对的文件和一个保存通信对方公钥的文件，该文件存储该节点拥有的公钥/私钥对，私钥环（口令保护密钥）和本节点知道的其他用户的公钥环

(2) 多个密钥对怎么具体识别是哪一个?

将公钥与消息一起传送；将一个标识符(KeyID)与一个公钥关联，对一个用户来说做到一一对应即可

8.(3+3+3=9 分)

(1) 证书的撤销和过期的区别?

证书的过期是指证书的有效期到了，不能再使用，证书的撤销是指证书的有效期还没到，但是由于某些原因，证书不能再使用

(2) 证书的撤销条件（场景）

私钥泄露, 关系终止, CA 签名私钥泄露或者变更

(3) 如何撤销一个证书?

CA 生成一个撤销列表，将证书的序列号加入撤销列表，然后将撤销列表发布到 CRL 中

sjk 答案：维持一个 CRL 和有关历史证书的记录，以便被过期的密钥资料所加密的数据能够被解密，出于对密钥历史恢复、审计和解决争议的考虑所进行的密钥资料的安全第三方长期储存

9.(3+3=6 分)

(1) 密钥派生的好处?

减少多次协商密钥的开销；密钥派生可以避免密钥泄露，提高安全性

(2) 如何派生密钥?

KDF.

附录 B 2024 春第一次小测

1.数字证书的功能以及所包含的最为基本的内容是什么，大概描述其他还包括什么?技术上 CA 如何生成一个数字证书。以及讨论一下什么情况下需要撤销一个证书，以及如何撤销一个证书?

(1) 功能:实现主体身份和主体公钥之间的绑定关系
(2) 最基本内容:主体身份信息、主体公钥值、认证机构名、认证机构的数字签名
(3) 其他:证书序列号、版本，有效期等
(4) 生成证书: CA 用自己私钥签名证书摘要附在证书之后
(5) 撤销原因:私钥泄漏、关系终止、CA 私钥泄漏
(6) 如何撤销:维持一个 CRL 和有关历史证书的记录，以便被过期的密钥资料所加密的数据能够被解密，出于对密钥历史恢复、审计和解决争议的考虑所进行的密钥资料的安全第三方长期储存

2.分组加密算法不同工作模式中都涉及到 IV 值的使用，一句话描述其主要作用是什么。在分组加密算法的应用中，怎么保证只需要一个较短的 IV 值就可以应对特别长的明文数据?简要说明在两者的保密通信中可采用哪些方法保证 IV 值是一致的。

(1) 作用:使得相同明文加密之后的密文不同，增强加密的安全性
(2) 如何保证:分组加密算法中除了 ECB 之外，在第一轮使用的是所给 IV,后续 IV 都是基于算法生成的
(3) 如何保持一致: 数字签名、数字信封、D-H 密钥交换都可以

3.两个用户协商会话密钥的基本方法通常有哪两种?简要描述分别是如何进行的。

(1) 方法:数字信封、D-H 密钥交换
(2) 略

4.构建安全通道用于数据安全传输，通常要求实现加密和完整性保护功能，一般是 由对称加密和 HMAC 来执行的，源端在加密操作和完整性保护操作上有没有特别的考虑，做简要的合理性说明。

- 显然是先加密后完整性保护, 如果完整性被破坏，不需要进行解密操作，直接丢包即可

附录 C 2024 春第二次小测

1.简单描述 IPSec 隧道模式和传输模式的区别?

- Ans1:
  (1) 传输模式:为 IP 载荷提供认证、完整性和机密性。
  (2) 隧道模式:保护整个 IP 分组，提供认证、完整性和机密性。
- Ans2:
  (1) 在传输模式中, AH 和 EP 头标插入 IP 头之后, TCP 头之前，是对载荷的认证和加密以及完整性保护。
  (2) 在隧道模式中, AH 和 ESP 头插入原 IP 之前,并在 AH, ESP 前新建一个 IP 头,是对整个原来分组的保护。

2.IPSec 如何防御重放攻击? SSL/TLS 如何防范数据传输过程中的重放攻击? (重 点数据传输，另外还有握手过程)

(1) IPSec 维护一个序列号窗口，当数据包序列号在窗口左边时直接丢弃。
(2) Ans1: SSL/TLS 数据传输过程主要靠序列号来抗重放(握手过程中使用随机数); Ans2: 使用随机数，序列号，时间戳

3.AH 计算 MAC 时，外层 IP 首部中哪些字段不包含在内?可选的 ESP 认证的覆盖范围和 AH 的有什么差别?

(1) Ans1: 字段:可变不可预测的，例如跳数; Ans2: 可变域不包含在内，一般置零，比如下一跳地址，生存周期
(2) Ans1: 覆盖范围: ESP 不包括 IP 首部; Ans2: AH 基本覆盖整个 IP 分组(除 IP 可变域外), ESP 认证仅覆盖 ESP 头,TCP,数据.

4.为什么 ESP 包含一个填充域?除了 ESP 填充的功能之外，填充在协议设计中还有什么其他作用?

(1) 32 位对齐
(2) 加密算法要求分组为某字节的整数倍
(3) 某些字段要求为某字节的整数倍(例如段偏移)
(4) 隐藏真实长度，抗流量分析

5.SSL/TLS 中会话重用和密钥派生的作用和方法?

(1) 会话重用:
    - 方法:发送端发送之前的 SessionID 接收端回复相同的 SessionID,则表示会话重用
    - 作用:减少重新协商会话参数产生的开销
(2) 密钥派生:
    - 方法:客户端和服务器产生随机数，双方协商或客户生成预共享密钥,利用密钥派生函数(KDF) 派生; Ans2: 双方使用共享的主密钥, 按选定的方法生成加密密钥, 签名密钥, IV 等
    - 作用:利用协商出来的预共享密钥，结合协商过程中双方的随机数计算后面的加密以及完整性保护密钥; Ans2: 减少密钥协商次数减少开销

6.IPSec AH/ESP、SSL/TLS 中普遍不采用签名来提供完整性和数据源认证，为什么?

- Ans1: 因为之前已经协商了共享对称密钥，基于该对称密钥可以使用 HMAC 提供完整性和数据源认证，相比于使用非对称密码的私钥签名计算效率更高，开销更小(非对称模幂运算与对称密钥计算速率相差两个数量级)
- Ans2: 签名一般需要生成公私钥对, 并且计算开销比使用对称密钥大的多, IPsec AH/ESP, SSL/TLS 提供了方便使用共享密钥进行 MAC 操作的框架, 密钥生成以及计算上开销都远于签名。