NSP期末复习

- Chap1：网络安全综述
  - 概念、定义、名词
    - 常见的不安全因素：
    - 不安全的原因：
    - 网络安全的特征：
    - 3A标准
    - 安全模型、安全体系结构
      - 安全体系结构
        - 安全攻击
        - 安全机制
        - 安全服务
      - 安全模型
        - 建立安全通道和数据传输
        - 访问控制、权限管理、安全通道建立、数据传输
    - 基本的加密、认证、密钥交换算法
      - 用户认证
      - 数据源认证
        1. 签名
        2. 消息认证码
      - 数据机密性、完整性保护等基本方法
        - 数据机密性
        - 完整性保护
    - 常见加密算法
      - 对称、非对称、哈希函数、HMAC（三类四种）
    - 分组密码算法中的工作模式
      - IV值的使用和作用
      - 典型加密模式的操作和差错的影响
- Chap2:公钥基础设施PKI
  - PKI基本概念
    - 是什么：
    - 为什么要PKI：
    - 提供的服务：
  - PKI的基本组成
  - 证书的基本结构
  - 数字信封
  - 证书生命周期、证书链、交叉认证
    - 证书的产生
    - 证书验证过程
    - 证书链
- Chap3:IPsec

- 双宿主主机
- 屏蔽子网结构
  - 双热设备
- 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
- NET基本原理、作用
  - NAT可以划分为以下两种类型（从发起者的报文）：
  - 实现方式(从地址转换的对应关系看)：
- 工作原理
- 作用
- iptables、netfilter
- netfilter
- iptables

Chap7:虚拟专用网技术VPN

- VPN种类、功能（简单了解）
  - 是什么：
  - VPN分类：
- IPSec VPN（重点）
  - IPSec VPN
  - 实现方式

Chap8：应用层安全协议

- 电子邮件发送时多个接收者时该怎么办?
- PGP
- 基本功能、安全服务、操作原理
  - PGP提供的安全业务：
  - 操作原理
  - 压缩
  - 基64转换
- 公钥环、私钥环
  - 加密密钥
  - 需求
  - 公钥管理
- PGP消息生成、接受操作流程
- 私钥的保存
- SET协议
- 基本概念
  - SET的系统组成
- 数字信封
- 双重数字签名
  - 双重签名
  - 双重签名流程
    - 持卡人发送购买请求
  - 商家验证过程

NSP期末复习

Chap1：网络安全综述

概念、定义、名词

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

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**

网络安全的特征：

- **机密性**：信息不泄漏给非授权的用户、实体或者过程的特性。
- **完整性**：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏的特性。
- **可用性**：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。
- **可认证性**：完整性存在关联，要求数据来自所声称的实体，或者合法用户
- **不可否认性**：做过的行为和接受过的信息不能抵赖，该能力有时又被称为可审计性Accountability，要求可事后追溯，不可否认
- **可控性**：对网络信息的传播及内容具有控制能力

常见攻击：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。总的来说有：

- **中断：可用性**
- **窃听：机密性**
- **修改：完整性**
- **伪造：可认证性**

3A标准

- **认证（Authentication）**
- **授权（Authorization）**
- **计费（Accounting）**

安全模型、安全体系结构

安全体系结构

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**。

安全攻击

- 主动攻击：篡改、伪装、重放、拒绝服务

- 被动攻击：窃听、流量分析
- 区别在于会不会主动改变数据流（也是被动攻击很难识别的原因）

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

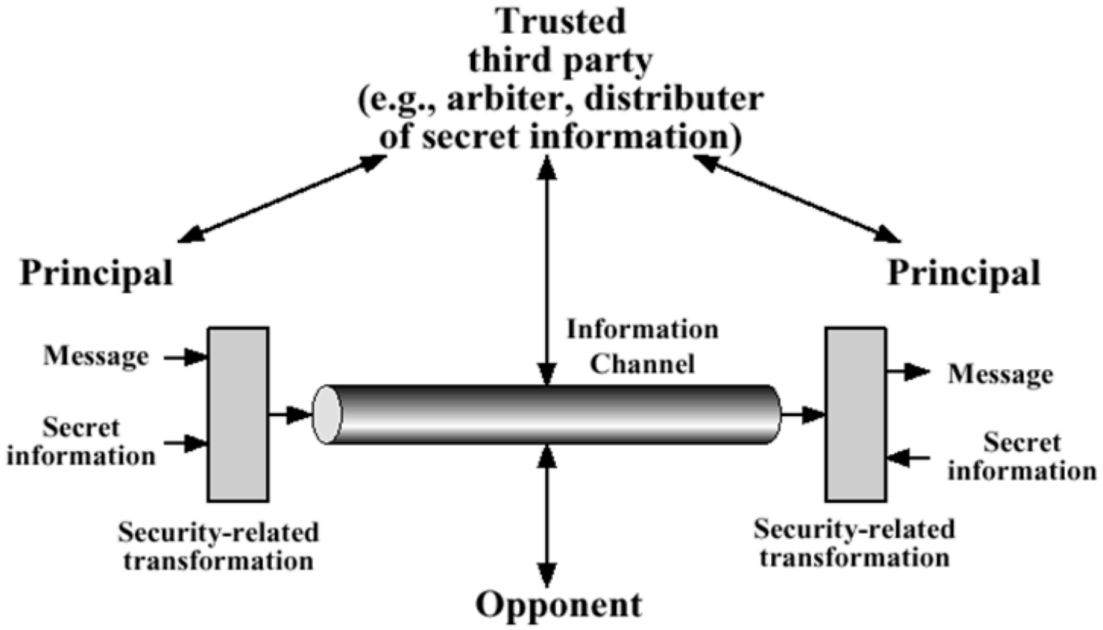
安全服务

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
- **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、选择与连接完整性、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

安全模型

- 网络安全模型：实现端到端的安全通信。安全通道等



1. **主体（Principal）**：指参与通信的各方（用户、系统或设备）。
2. **消息（Message）**：从一个主体传输到另一个主体的信息或数据。

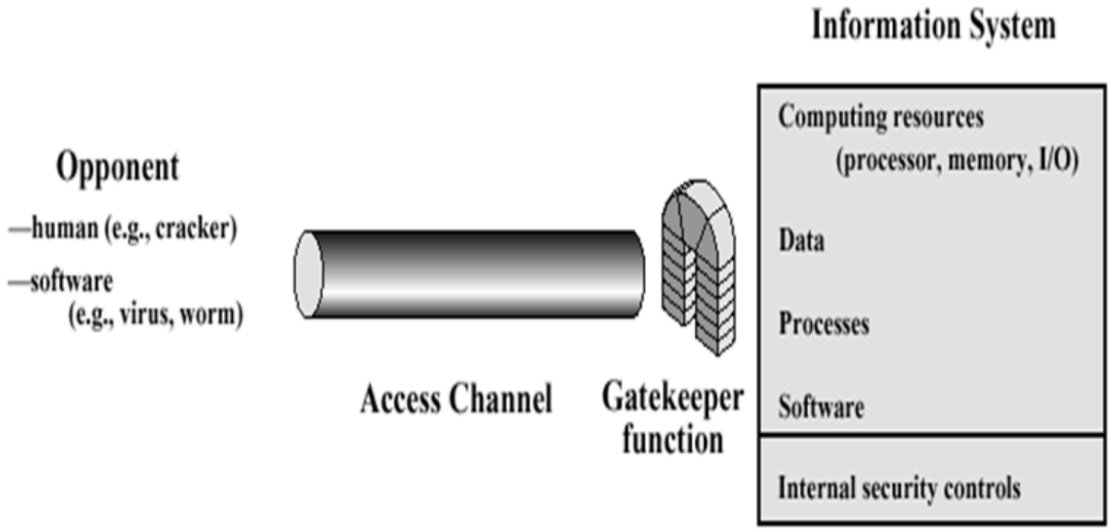
3. **秘密信息（Secret Information）**：用于确保消息机密性和完整性的敏感信息（如加密密钥）。
4. **安全相关转换（Security-related Transformation）**：使用秘密信息对消息进行安全机制（如加密）处理的过程，以确保其机密性和完整性。
5. **可信第三方（Trusted Third Party）**：负责分发秘密信息或作为仲裁者，确保主体之间的信任。
6. **信息通道（Information Channel）**：传输加密消息的媒介，假定其可能不安全。
7. **对手（Opponent）**：指可能在传输过程中拦截、修改或篡改消息的潜在对手。

建立安全通道和数据传输

要建立安全的通信通道，通常涉及以下步骤：

1. **初始化**：主体同意使用特定的安全协议，可能涉及可信第三方来分发加密密钥或其他秘密信息。
2. **安全相关转换**：每个主体使用秘密信息对消息应用安全机制（如加密）。
3. **传输**：通过信息通道传输加密消息。
4. **接收和解密**：接收方使用共享的秘密信息解密加密消息，以恢复原始消息。
5. **验证**：接收方验证消息的完整性和真实性，以确保在传输过程中没有被篡改。

- 网络访问安全模型：**保护信息系统免遭恶意访问**。防火墙等



1. **对手（Opponent）**：
   - **人类（human）**：例如，黑客（cracker）。
   - **软件（software）**：例如，病毒（virus）、蠕虫（worm）。
2. **访问通道（Access Channel）**：对手可能通过此通道尝试访问信息系统。

3. **守门人功能（Gatekeeper Function）**：这是一个保护机制（如防火墙、入侵检测系统），用于监控和控制通过访问通道的所有流量，防止未经授权的访问。
4. **信息系统（Information System）**：
    - **计算资源（Computing resources）**：处理器、内存、输入/输出（I/O）设备。
    - **数据（Data）**：存储和处理的信息。
    - **进程（Processes）**：正在执行的任务或程序。
    - **软件（Software）**：操作系统、应用程序等。
    - **内部安全控制（Internal security controls）**：内部用于保护系统和数据的安全机制。

访问控制、权限管理、安全通道建立、数据传输

1. **访问控制**：限制和控制谁能访问信息系统，以及能访问哪些资源。这通常通过用户认证和授权来实现。
2. **权限管理**：定义和管理用户或系统进程对资源的访问权限，包括文件、数据和系统功能的读/写/执行权限。
3. **安全通道建立**：使用加密协议（如SSL/TLS）来确保在传输过程中的数据保密性和完整性。
4. **数据传输**：通过安全通道进行数据传输，确保数据在传输过程中不被拦截或篡改。

基本的加密、认证、密钥交换算法

用户认证

用户认证**基于挑战应答**的四种机制（**对称加密、签名、非对称加密、HMAC**）各有不同的实现方法和适用场景。

1. **对称加密（Symmetric Encryption）**：
    - **过程**
        1. 服务器生成一个随机数（挑战），并发送给用户。
        2. 用户使用预先共享的对称密钥加密这个随机数，并将结果发送回服务器。
        3. 服务器使用相同的对称密钥解密接收到的密文，并将其与原始随机数进行比较。如果匹配，则认证通过。
2. **签名（Digital Signature）**：
    - **过程**
        1. 服务器生成一个随机数（挑战），并发送给用户。
        2. 用户使用自己的私钥对这个随机数进行数字签名，并将签名结果发送回服务器。

3. 服务器使用用户的公钥验证签名。如果签名有效，则认证通过。

3. **非对称加密（Asymmetric Encryption）**：
    - **过程**
        1. 服务器生成一个随机数（挑战），并使用用户的公钥加密后发送给用户。
        2. 用户使用自己的私钥解密这个随机数，并将解密后的明文发送回服务器。
        3. 服务器将接收到的明文与原始随机数进行比较。如果匹配，则认证通过。
4. **消息认证码（HMAC, Hash-based Message Authentication Code）**：
    - **过程**
        1. 服务器生成一个随机数（挑战），并发送给用户。
        2. 用户使用预先共享的密钥和一个哈希函数生成HMAC，将结果发送回服务器。
        3. 服务器使用相同的密钥和哈希函数生成自己的HMAC，并与接收到的HMAC进行比较。如果匹配，则认证通过。

数据源认证

在数据源认证中，**签名**和**HMAC**是常用的两种技术手段。它们都用于确保数据的完整性和真实性，但实现方式有所不同。

1. 签名

过程：

- **数据生成**：数据源生成要发送的数据。
- **生成摘要**：使用哈希函数对数据进行哈希运算，生成数据摘要（hash）。
- **签名生成**：数据源使用其私钥对数据摘要进行加密，生成数字签名。
- **数据发送**：将数据和数字签名一同发送给接收方。
- 签名验证：
    - 接收方接收到数据和签名后，使用数据源的公钥对签名进行解密，得到数据摘要。
    - 接收方对接收到的数据使用相同的哈希函数生成新的数据摘要。
    - 将新生成的摘要与解密后的摘要进行比较，如果一致，则验证通过，数据完整且真实。

2. 消息认证码

过程：

- **数据生成**：数据源生成要发送的数据。

- **生成HMAC**：使用预先共享的对称密钥和哈希函数对数据进行运算，生成HMAC值。
- **数据发送**：将数据和HMAC值一同发送给接收方。
- HMAC验证
    - 接收方接收到数据和HMAC值后，使用相同的对称密钥和哈希函数对数据生成新的HMAC值。
    - 将新生成的HMAC值与接收到的HMAC值进行比较，如果一致，则验证通过，数据完整且真实。

数据机密性、完整性保护等基本方法

数据机密性

完整性保护

签名 HMAC

常见加密算法

对称、非对称、哈希函数、HMAC（三类四种）

分组密码算法中的工作模式

IV值的使用和作用

作用：使用IV可以使得相同明文加密之后的密文不相同，增强加密的安全性。

典型加密模式的操作和差错的影响

①电码本模式(ECB)
②密码分组链接模式(CBC)

- 如果某一块密文出现差错，那么这个差错会影响到两个连续的明文块：**当前块和下一个块。**

③密码反馈模式(CFB)

- 如果某一块密文出现差错，这种差错会一直传播到**后续所有的明文块。**

④输出反馈模式(OFB)

- 如果某一块密文出现差错，这种差错只会**影响当前块**

⑤计数器模式(CTR)

- 如果某一块密文出现差错，**这种差错只会影响当前块**

Chap2:公钥基础设施PKI

PKI基本概念

是什么：

- 公钥基础设施
- 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**。

为什么要PKI：

- 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**）

提供的服务：

- **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

PKI的基本组成

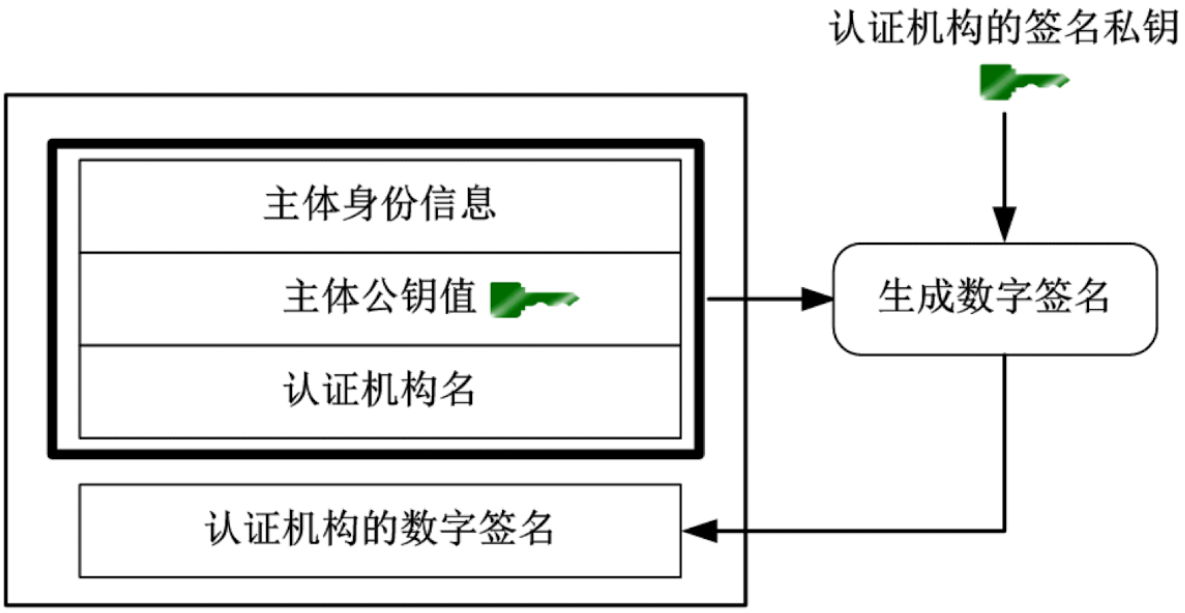
- **认证中心CA**：证书的签发机构，它是PKI的**核心构件**，是PKI应用中权威的、可信任的、公正的第三方机构。
- **注册机构RA**：按照特定的政策和管理规范对用户的资格进行审查，并执行是否同意给该申请人发放证书。撤销证书等操作，应注意的是RA**不容许直接颁发证书或CRL。**
- **证书库**：CA颁发证书和证书撤销列表CRL的集中存放地，提供公众查询，常用目录服务器提供服务
- **密钥备份及恢复系统：**

    - **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**证书撤销列表（CRL）**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。

证书的基本结构

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

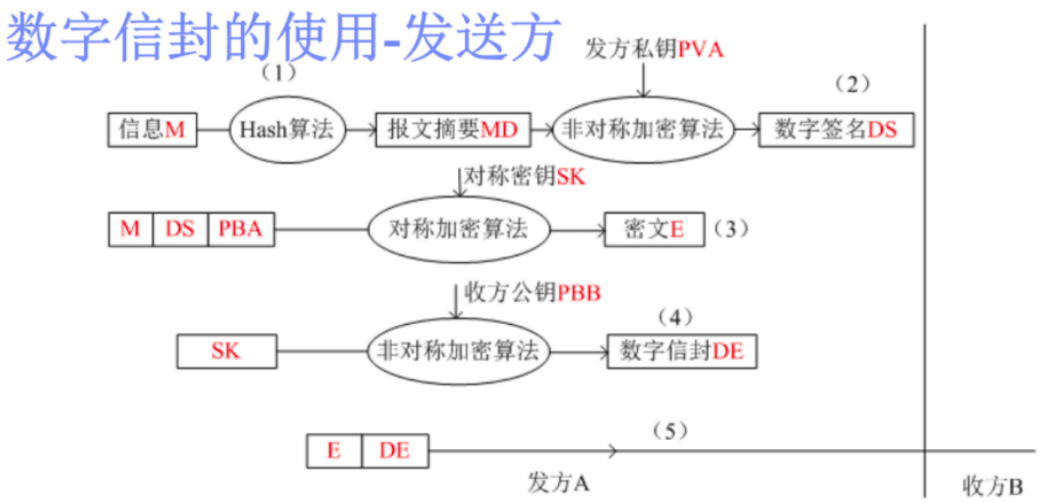
通过可信CA的签名实现主体身份和主体公钥之间的绑定关系



数字信封

- **概述：**①发送端：用接收端的**公钥**，将通信密钥（**对称密钥**）加密，生成**数字信封**。②接收端：用私钥打开数字信封，获取对称密钥SK。
- **使用：**

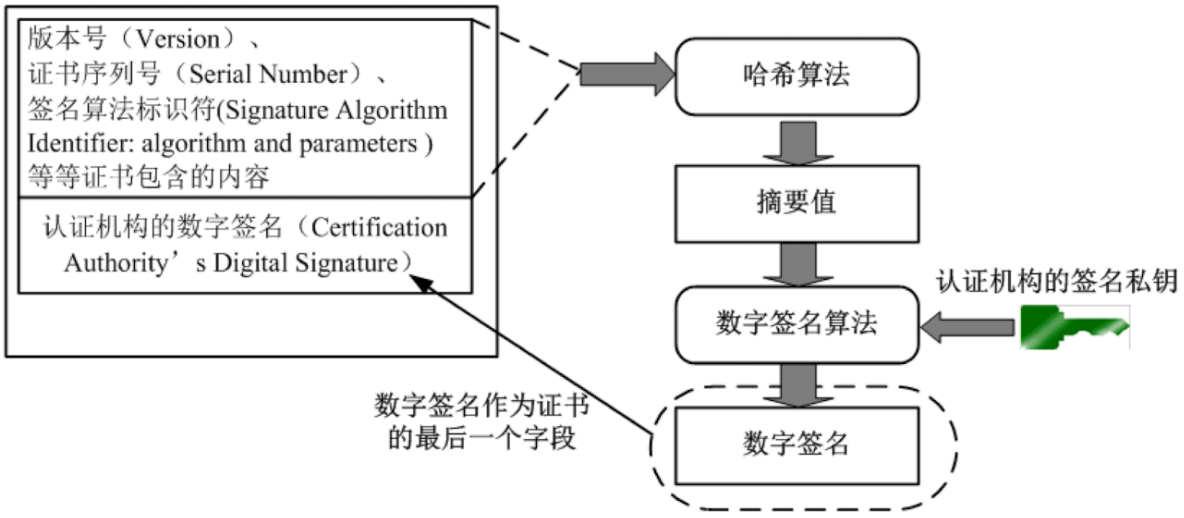
- 发送方：（客户端）
  - **信息hash**：生成数据摘要，防止传输过程数据被篡改。
  - **签名摘要**：①信息长度可能非常长，直接签名非常耗时，因此签名摘要。②签名目的是防止中间人攻击，以保证信息的可靠性。③抗否认。
  - **明文加密**：将明文、2的数字签名、发送方证书上的公钥，加密生成密文。发送方的公钥用于接收方验证签名。
  - **生成数字信封**：使用证书中的公钥加密对称密钥，生成数字信封。
  - **发送密文和信封**



考虑接收端开销的角度，这里是有错误的，不能够先签名后加密，否则接收方每次都需要解密才能判断有没有出错。

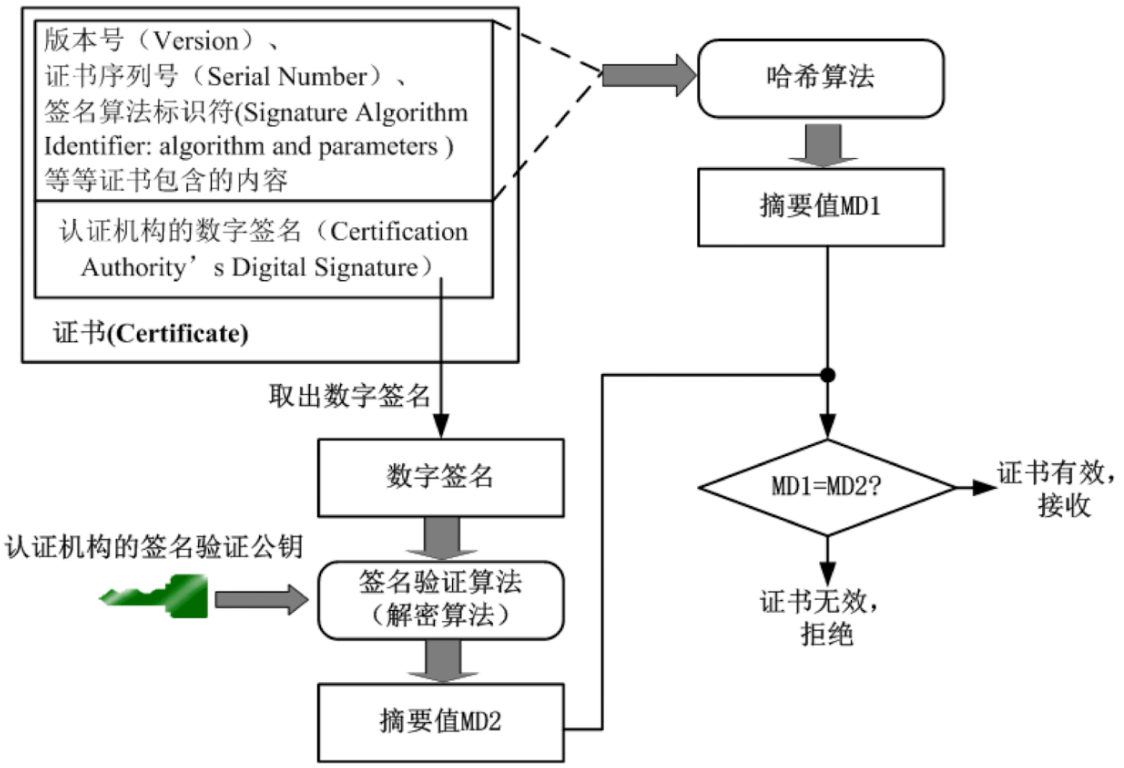
证书生命周期、证书链、交叉认证

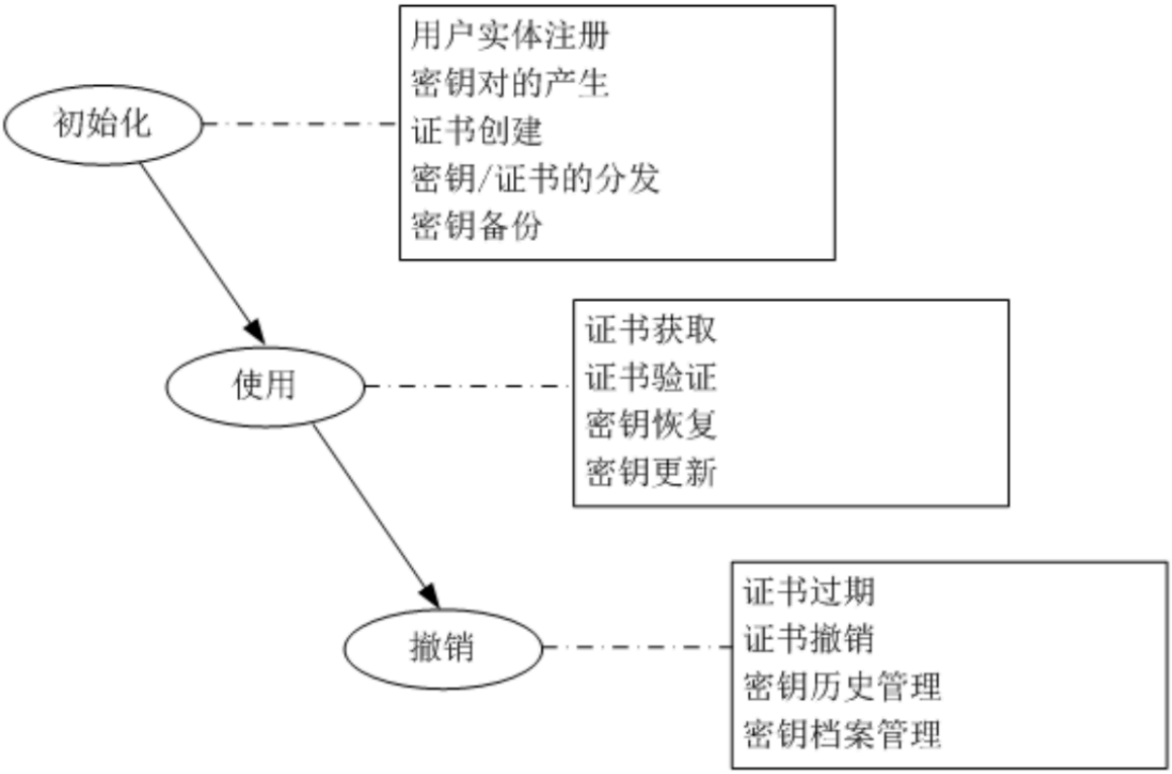
证书的产生



证书验证过程

简单来说就是类似完整性验证操作





- **初始化：**终端实体在使用PKI提供服务之前，必须先初始化。
- **使用：**
- **撤销：**
  撤销场景：
  - **证书过期**
  - **证书撤销**：**私钥泄露、关系终止、CA私钥泄露**等

  撤销阶段：
  - **过期：**证书生命周期自然结束。
  - **撤销**：证书在过期之前被撤销（非过期）
  - **存档：**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**
  - **审计：**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**
- **验证：**

证书链

证书链由不同CA创建的证书序列组成，其中每个连续的证书都是由一个CA颁发的证书，用于证明链中下一个CA的公钥

Chap3:IPsec

安全关联SA、SAD/SPD

SA：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**

- 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。
- SA是通过**密钥管理协议（如IKE）**在通信双方之间进行协商，协商完毕后，双方都在它们的**安全关联数据库（SAD）**中存储该SA参数。
- 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）**。
    - SPI是为了唯一标识SA而生成的一个**32位**整数，包含在AH/ESP头标中。SPI为同一个源与目的之间建立多个SA提供可能

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**

安全关联数据库（SAD）：包含现行的SA条目，每个SA由三元组索引，一个SAD条目包含下面域：

- 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：是一个标志，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/ESP所需的认证算法和密钥
- ESP加密算法和IV

- IPSec操作模式
- SA生存期
- 路径最大传输单元（PMTU）

AH/ESP头标

认证头标AH

AH协议提供**无连接的完整性（覆盖IP头标除可变域的部分）、数据源认证和抗重放保护服务。不提供保密性服务**。AH使用**消息认证码（MAC）**对IP进行认证。

封装安全载荷头标ESP

ESP提供**数据保密（对称密码）、无连接完整性**（可选，**不覆盖IP头标**）、**抗重放攻击**服务，用对称密码体制提供保密性。使用**消息认证码（MAC）**对IP进行认证和完整性保护。

ESP使用时要填充，目的：

- 32位对齐
- 分组密码要求长度是某个长度的整数倍
- 抗流量分析

源端和目的段处理

AH处理

源端外出处理

- **策略检查**：
  - 使用相应的选择符查找**安全策略数据库（SPD）**，获取与该分组匹配的安全策略。
  - 如果SPD条目指示分组需要IPSec处理，并且到目的主机的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）**中的一个或多个SA。
  - 如果SA尚未建立，IPSec将调用**IKE**协商一个SA，并将其连接到SPD条目上。
- **产生或增加序列号**：
  - 每个新的SA建立时，序列号计数器初始化为0。在每发送一个分组时，序列号加1。
- **计算ICV（完整性校验值）**：
  - 根据SA指定的MAC算法计算分组的完整性校验值（ICV）。
  - 将计算得到的ICV添加到AH头部。

- **封装并转发分组**：
  - 将AH头部插入到原始IP分组中，形成新的IPSec AH分组。
  - 将分组转发到目的节点。

目的端进入处理

- **策略验证**：
  - 如果IP分组中无IPSec选项，则使用分组的选择符在**安全策略数据库（SPD）**中查找与之匹配的策略。
  - 检查策略是否相符，如果无需进行IPSec处理则放行分组，否则丢弃。
- **查找SA**：
  - 使用IP分组头中的SPI值、目的IP地址以及IPSec协议在**进入SA数据库（SAD）**中查找SA。
  - 如果查找失败，丢弃分组并记录事件。
- **IPSec处理**：
  - 使用查找到的SA进行IPSec处理，包括序列号检查和数据完整性验证。
- **检查序列号**：
  - 验证序列号是否在允许的窗口内，确保分组未被重放。如果序列号检查失败，丢弃分组。
- **数据完整性验证**：
  - 使用SA指定的MAC算法重新计算ICV，并与分组中的ICV进行比较。
  - 如果两者不匹配，丢弃分组。

ESP处理

源端外出处理

- **策略检查**：
  - 使用分组的选择符（如目的IP地址、端口、传输协议等）查找**安全策略数据库（SPD）**，获取与该分组匹配的安全策略。
  - 如果SPD条目指示分组需要IPSec处理，且安全关联（SA）已建立，则SPD条目会指向**安全关联数据库（SAD）**中的相应SA。
  - 如果SA尚未建立，则使用IKE协议建立SA。
- **生成或增加序列号**：
  - 每个ESP分组都有一个序列号，防止重放攻击。序列号在每次发送新分组时增加。
- **加密分组**：

    - 根据SA指定的加密算法对数据进行加密。
- **计算完整性校验值（可选）**：
    - 如果SA要求数据完整性检查，则使用HMAC计算完整性校验值，并将其附加到ESP分组中。

目的端进入处理

- **策略验证**：
    - 使用分组的选择符在**安全策略数据库（SPD）**中查找与之匹配的策略。
    - 根据SPD条目检查分组是否满足IPSec处理要求，如果不满足则丢弃。
- **查找SA**：
    - 使用三元组在**安全关联数据库（SAD）**中检索特定的SA。
    - 如果查找失败，丢弃分组。
- **检查抗重放功能**：
    - 验证序列号是否在允许的窗口内，确保分组未被重放。如果检查失败，丢弃分组。
- **数据完整性检查（如适用）**：
    - 如果SA要求认证，验证ESP分组的完整性校验值，确保数据未被篡改。
- **解密**：
    - 使用SA指定的加密算法和密钥解密ESP数据。

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**。

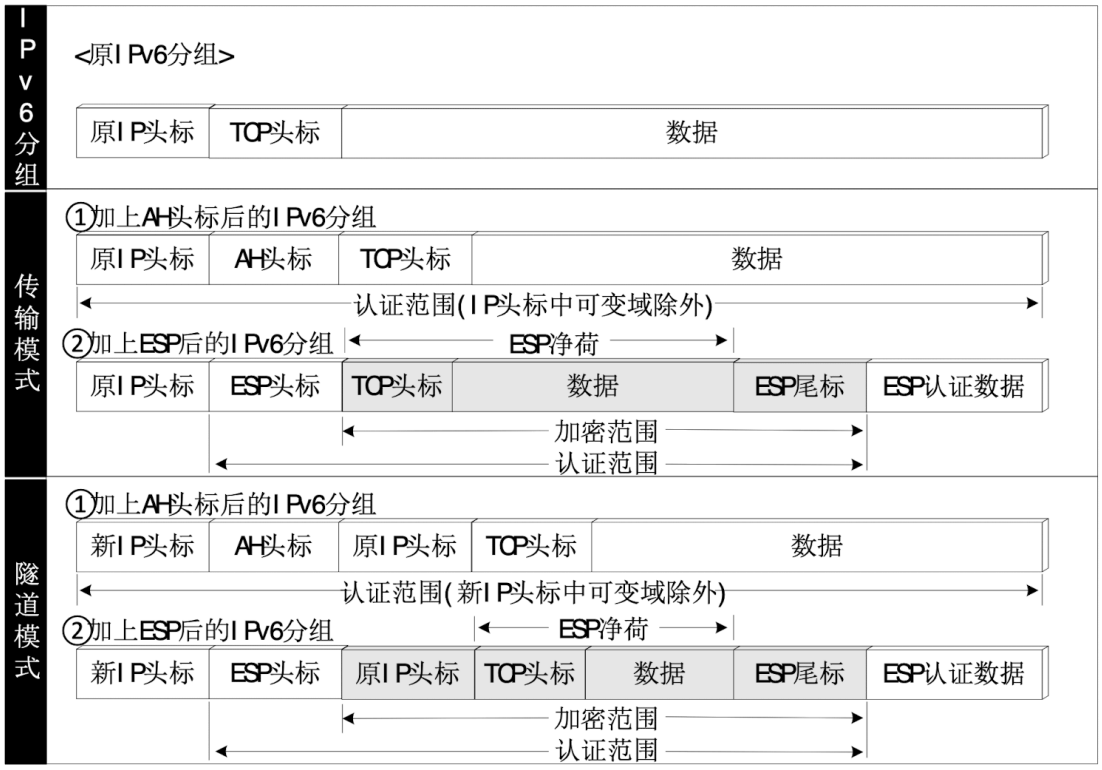
AH/ESP同时使用的顺序

先加密后认证，所以是先ESP后AH

传输模式和隧道模式

传输模式：AH和ESP头标被插在IP头标及其他选项（或扩展头标）之后，但在传输层协议之前。它**保护净荷的完整性和机密性**。(保护载荷)
隧道模式：AH或ESP头标插在IP头标之前，另外生成一个**新的IP头**放在前面，隧道的起点和终点的网关地址就是新IP头的源/目的IP地址，**保护整个IP分组**。（保护所有）

IPSec的传输模式与隧道模式



IPSec与NAT

NATPT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。原因：

- 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**

IPSec VPN

IPSec VPN就是利用IPSec技术在Internet上建立的VPN

Chap4:IKE

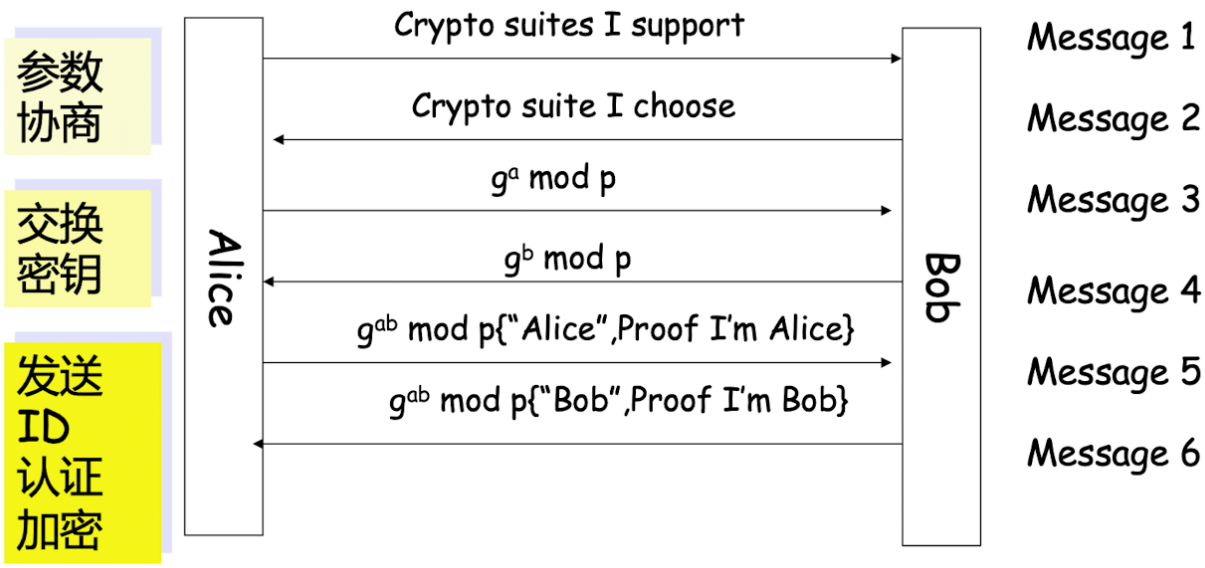
功能

使用某种**长期密钥**进行**双向认证**并建立**短期会话密钥**。

主模式和野蛮模式

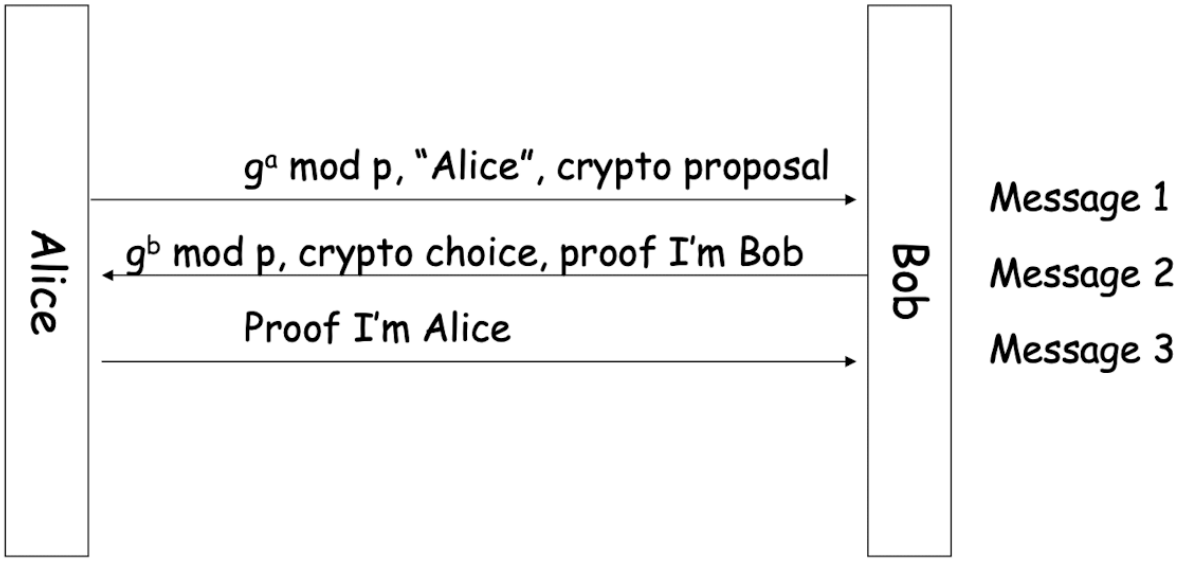
主模式

交换六个报文



野蛮模式

交换三个报文



两个阶段

IKEv1

- **第一阶段**，为建立IKE本身使用的安全信道而相互交换SA（采用ISAKMP）——**ISAKMP SA（双向）**
- **第二阶段**，利用第一阶段建立的安全信道交换IPSec通信中使用的SA——**IPSec SA（单向）**

IKEv2

- **初始交换阶段**：建立IKE本身使用的安全信道而相互交换SA——**IKE SA（双向）**
  和最初的CHILD_SA，包含两对消息：IKE_SA_INIT、IKE_AUTH
- **CREATE_CHILD_SA阶段**：更新IKE SA，或者更新和创建一个新的**CHILD_SA**，一对消息
- **INFORMATIONAL交换阶段**：用于删除SA，发送错误通知，检查IKE_SA，
  一对消息的存活性等。

Chap5:SSL/TLS

SSL协议族：一种在**TCP**之上为两个端实体之间提供安全通道的协议，包括SSLv2，SSLv3，TLS协议。在不提供IPSec安全保护的网络上，要实现安全的信息传输，只有依靠端到端的上层安全协议提供保护。

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**

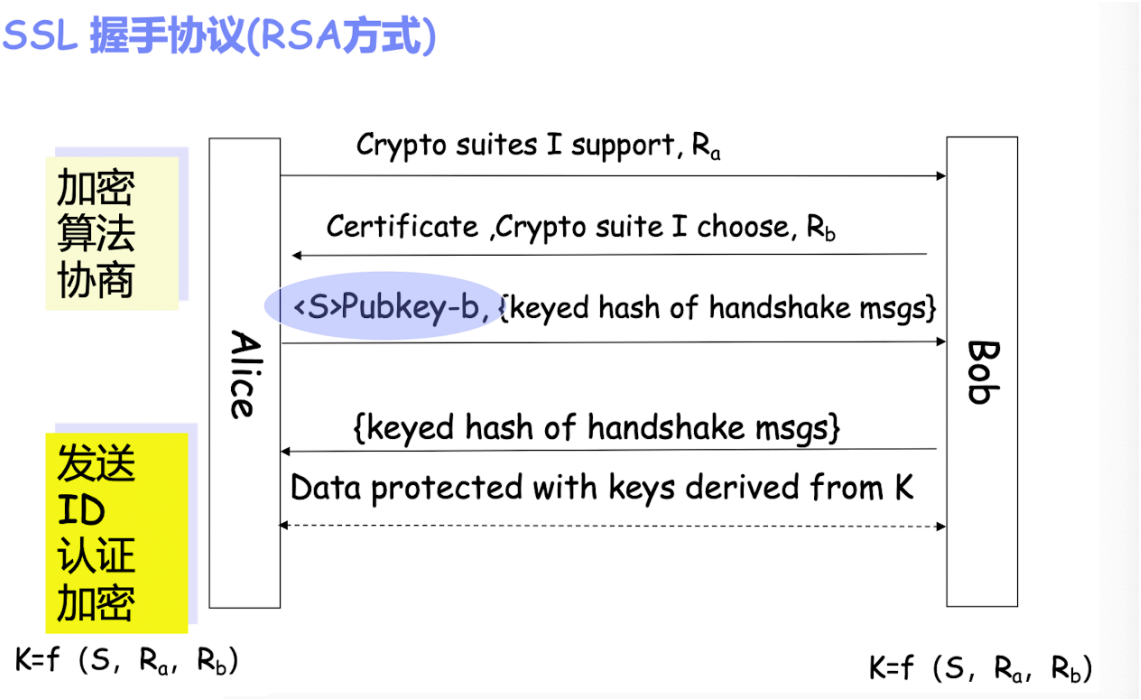
SSL提供的服务：

- 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...

SSL的基本层次结构

SSL协议分为两层

- 底层：**记录协议**
  - 建立在TCP之上
  - 用于上层协议封装
  - 安全性：提供**保密性（对称加密）和完整性（HMAC）**
- 上层：**握手协议、密码变更协议、告警协议、用户数据**
  - **握手协议：**安全连接之前交换安全信息（**对称密钥在这个地方协商好**）
    1. 客户和服务器相互认证
    2. 协商加密算法和密钥
    3. 安全性：身份认证，协商密钥等

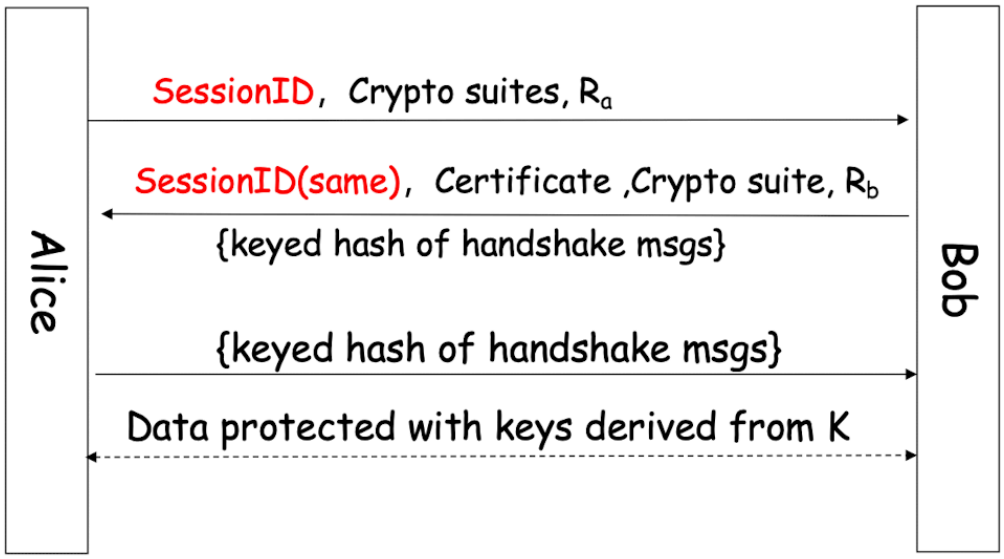


上图中的Pubkey-b是用Bob公钥加密的**pre-master key**。最终**主密钥**K = f(S, Ra, Rb)。对于每个连接，每个方向上各三个密钥，分别为**加密密钥**、**完整性保护密钥**、**IV**：gi（K，Ra，Rb），利用主密钥派生。**master_secret总是48字节长**，而**pre_master_secret长度不定**，取决于密钥交换算法。

会话重用

会话重用指的是在一次会话过程中，浏览器和服务器之间保持一个长时间的连接，而不是每次你点击一个链接都重新建立一个新的连接。比如你浏览商品、查看商品详情、加入购物车，这些操作都通过同一个连接完成，而不是每次点击都重新连接服务器。这就像你和朋友一直保持电话通话，不需要每次说一句话就挂断再拨打。

会话重用（进行重用的情况）

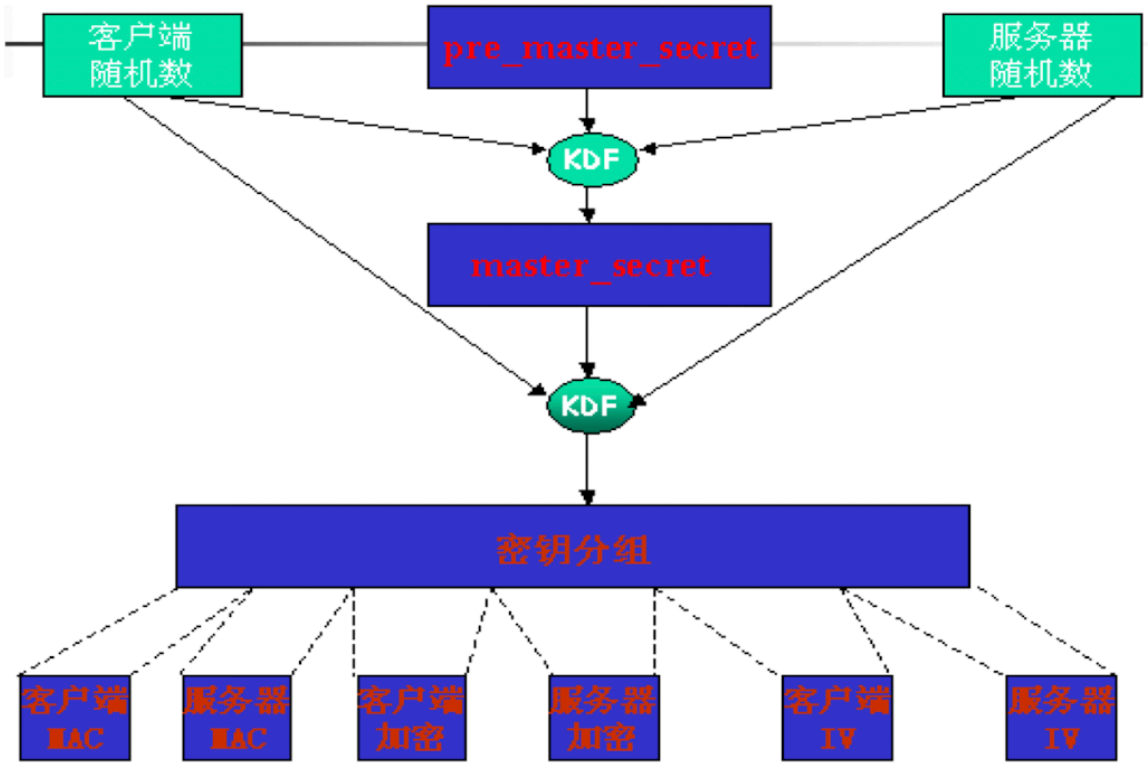


Bob返回相同的Session代表同意会话重用，返回不同的Session则和未进行重用的情况一样操作

简单来说，会话重用的原理就是：我把sessionID给你扔过去，你返回的是相同的sessionID，代表你同意会话重用，反之则不重用。

密钥生成（派生）

- 秘密值S：预备主密钥（Pre-mastersecret），由客户端生成
- 主密钥（Master secret）K：K = f（S，Ra，Rb）
- 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**：gi（K，Ra，Rb）



Chap6:Firewall & NAT

防火墙概念

防火墙：是位于两个(或多个)网络间，实施网间访问控制的一组组件的集合（软件+硬件+控制策略），它满足以下条件：

- 内部和外部之间的所有网络数据流必须经过防火墙；
- 只有符合安全政策的数据流才能通过防火墙；
- 防火墙自身能抗攻击；

防火墙 = 硬件 + 软件 + 控制策略

防火墙种类、功能

防火墙技术分类

- 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**

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

包过滤防火墙

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）

缺省策略

- 一切未被禁止的就是允许的
- 一切未被允许的就是禁止的

状态检测防火墙

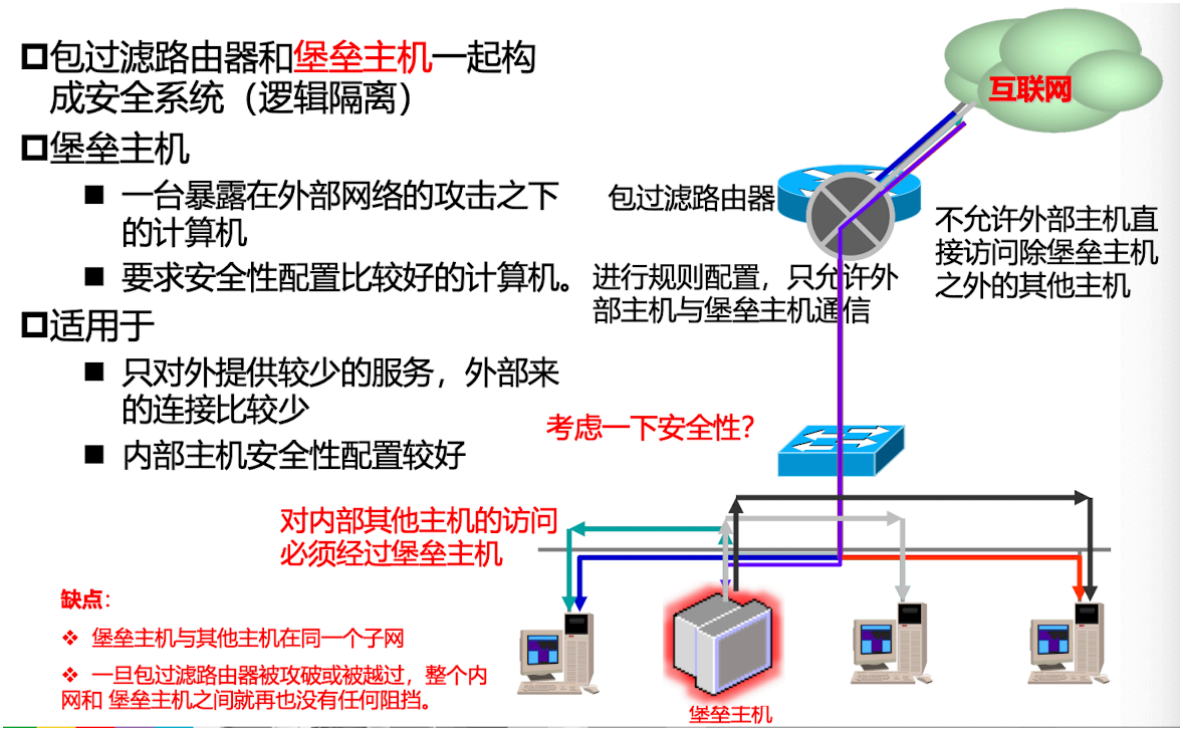
通过建立一个出网的TCP连接目录而加强TCP数据流的检测规则(**连接记录**)。即状态检测防火墙 = 包过滤防火墙 + 连接记录。报文过滤机制只允许那些和目录中某个连接匹配的数据流通过防火墙

复合型防火墙

单宿主主机

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

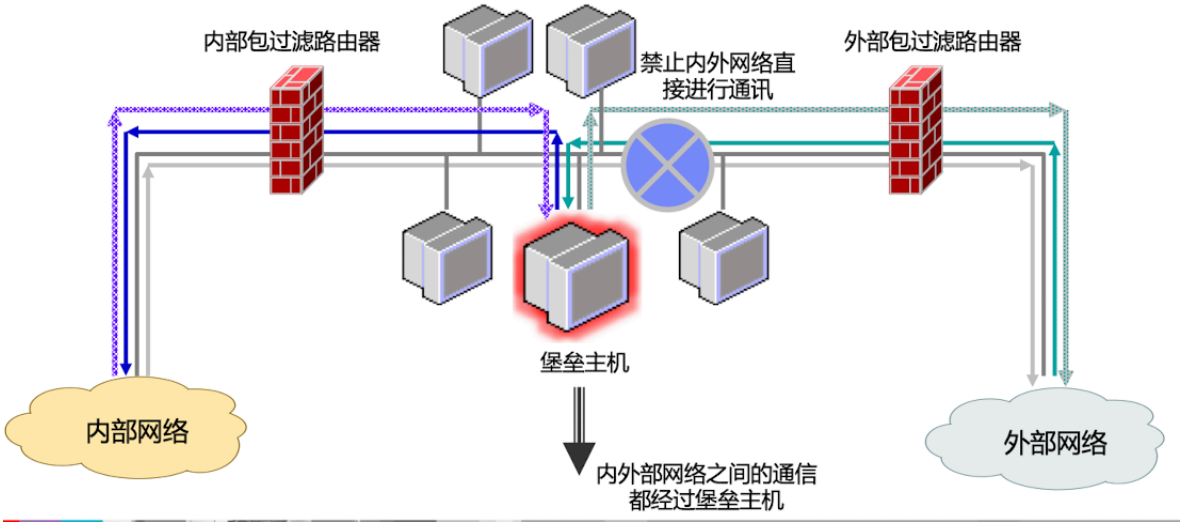
难点：如何保证双宿主主机安全

屏蔽子网结构

DMZ（Demilitarized Zone），非军事区或者停火区：

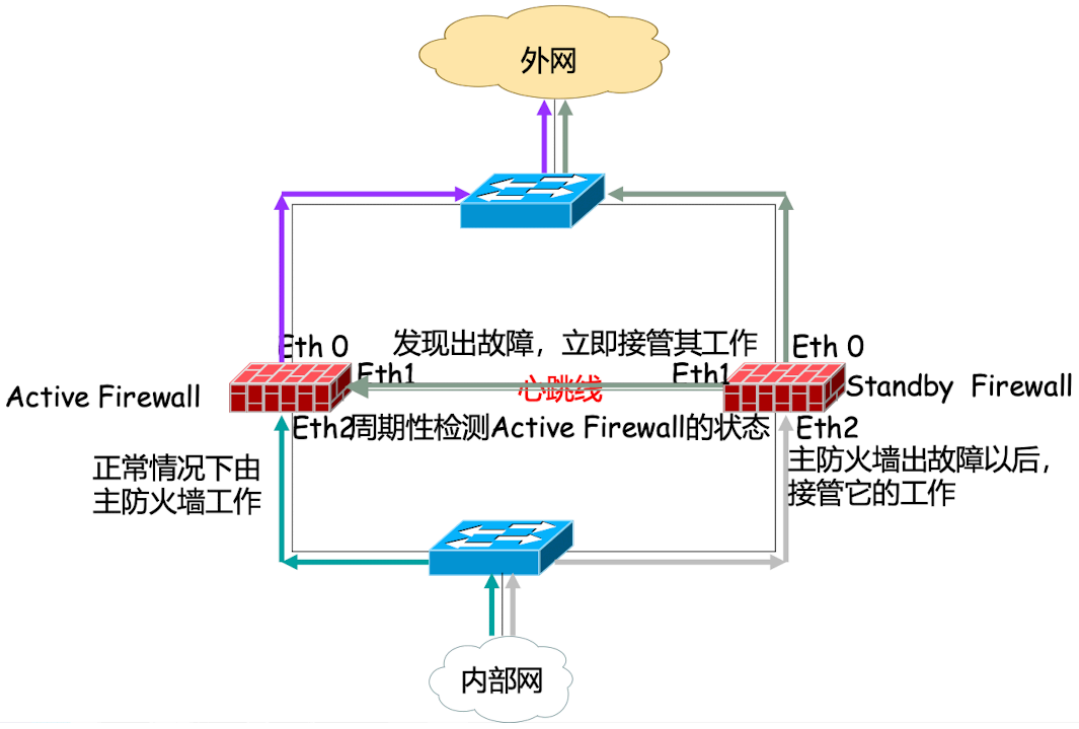
- 包含两个包过滤路由器
  - 外部路由器：只允许对DMZ的访问，拒绝所有以内部网络地址为目的地址的包进入内部网络。
  - 内部路由器：保护内部网络，防止来自Internet或DMZ的非法访问，拒绝外部发起的一切连接，**只允许内部对外的访问**，在特定需要前提下，可以允许从堡垒主机来的访问，从内部往外的访问也可以限制为必须通过堡垒主机。
- 在内部网络和外部网络之间创建了一个新的子网，可能只包含**堡垒主机**，也可能还包含一个或者多个**信息服务器**（所有对外服务在DMZ完成）

- 内外网通信必须经过堡垒主机



双热设备

目的：保证稳定性，一个防火墙完蛋了另一个马上顶上



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

NET基本原理、作用

NAT技术可以在路由器(边界)、防火墙上实现内外地址的翻译工作

NAT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（Source NAT，缩写为**SNAT**），即**IP伪装**（masquerade）
- 目的网络地址转换（Destination NAT，缩写为**DNAT**）。

实现方式(从地址转换的对应关系看):

- **静态NAT**（static NAT）-一一对应
- **动态NAT**（Dynamic NAT）-多对多
- **过载**（Overloading）-一对多 **NAT-PT**

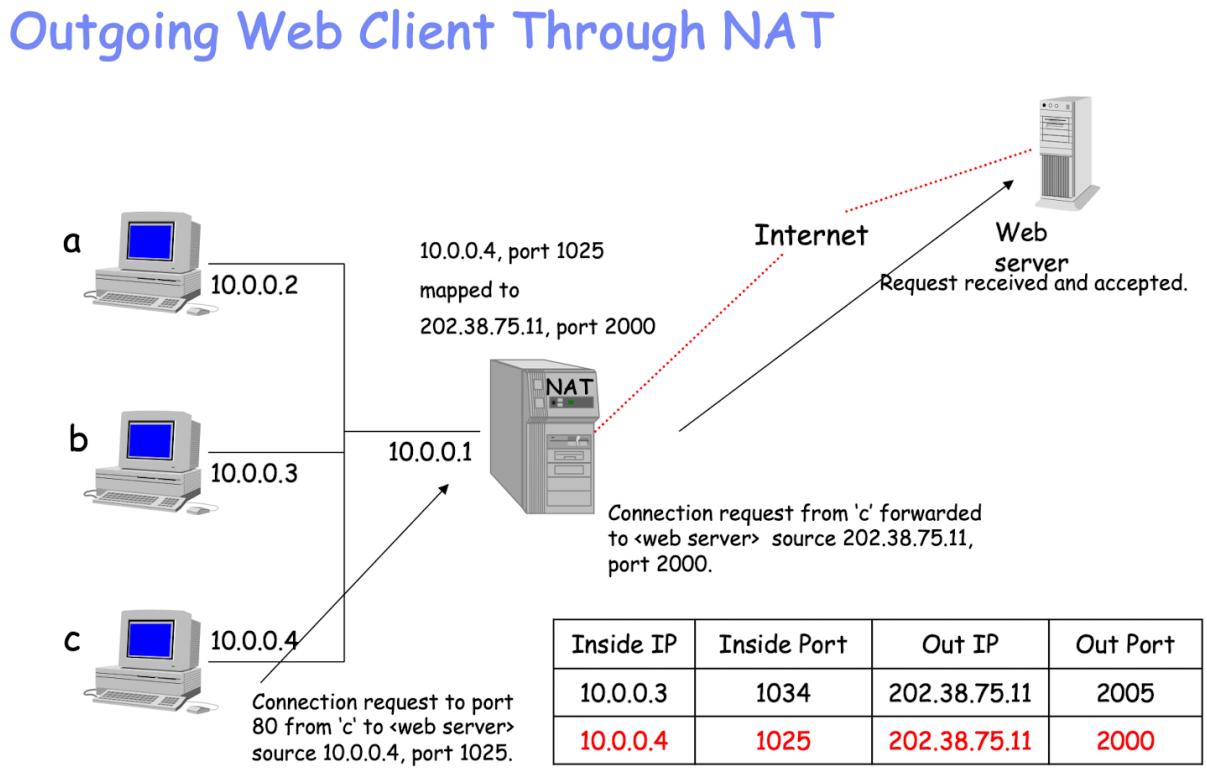
工作原理

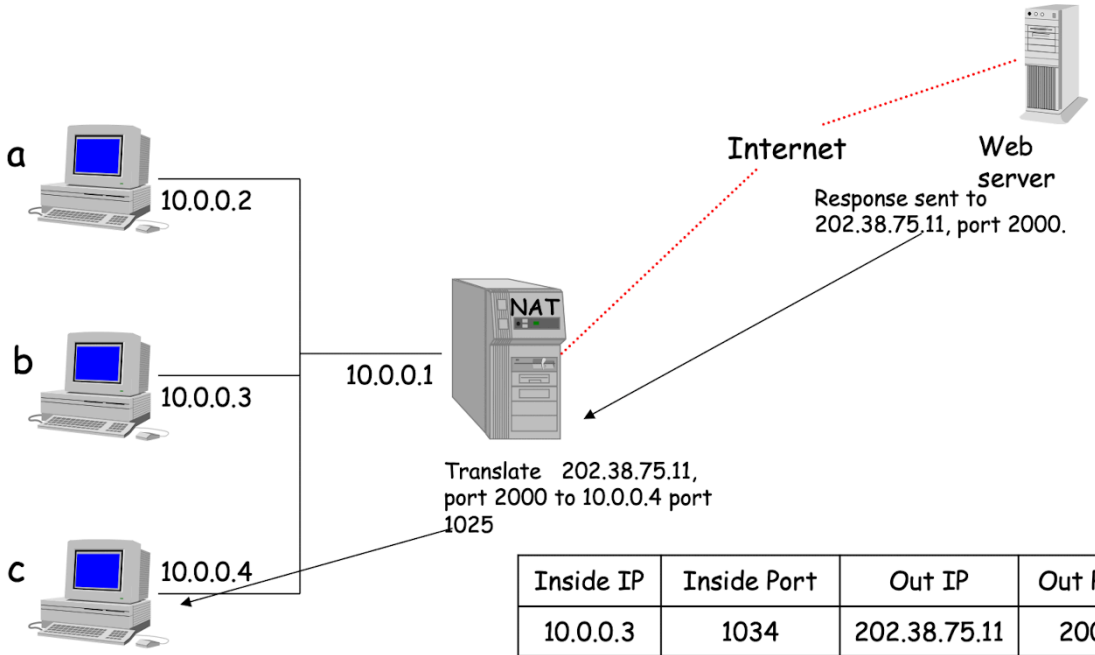
- 客户机将数据包发给运行NAT的计算机设备（NAT设备）
- NAT将数据包中的端口号和专用的IP地址换成它自己的某个端口号和公用的IP地址，然后将数据包发给外部网络的目的主机，同时会记录一个**跟踪信息**在映射表中，以便向客户机发送回答信息时的反映射。

- 外部网络发送回答信息给NAT设备
- NAT设备将所收到的数据包的端口号和公用IP地址转换为客户机的端口号和内部网络使用的专用IP地址并转发给客户机。

作用

- SNAT
  - **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
  - 在实现SNAT的环境下进行有效的服务访问
  - **流量均衡**





Inside IP	Inside Port	Out IP	Out Port
10.0.0.3	1034	202.38.75.11	2005
10.0.0.4	1025	202.38.75.11	2000

连接请求的过程：

- 计算机c（IP地址10.0.0.4）发起了一个到互联网某个Web服务器（外部服务器）的连接请求。请求的源端口是1025。
- NAT设备将该请求转换成公共IP地址202.38.75.11，使用端口2000发送到外部Web服务器。
- 外部Web服务器收到并接受了请求，响应返回给公共IP地址202.38.75.11端口2000。
- NAT设备收到响应后，将其转换回原始请求计算机c，IP地址10.0.0.4，端口1025。

iptables、netfilter

Linux系统中的两种主要工具，用于**管理网络流量**和**防火墙规则**。

netfilter

netfilter是一个内核模块框架，提供了以下功能：

- **数据包过滤**：允许或拒绝特定的数据包。
- **地址转换**：进行网络地址转换（NAT），包括源地址转换（SNAT）和目标地址转换（DNAT）。

- **数据包修改**：修改数据包的内容或头信息。
- **数据包记录**：记录通过的数据包信息，用于网络监控和日志记录。

netfilter在Linux内核中工作，位于网络栈的不同位置，提供钩子（hook）函数让iptables能够插入并执行规则。

iptables

iptables是一个用户空间的命令行工具，用于配置netfilter提供的规则。通过iptables，管理员可以定义各种防火墙规则来控制进出Linux系统的数据流。

Chap7:虚拟专用网技术VPN

VPN种类、功能（简单了解）

是什么：

- 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。

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

IPSec VPN（重点）

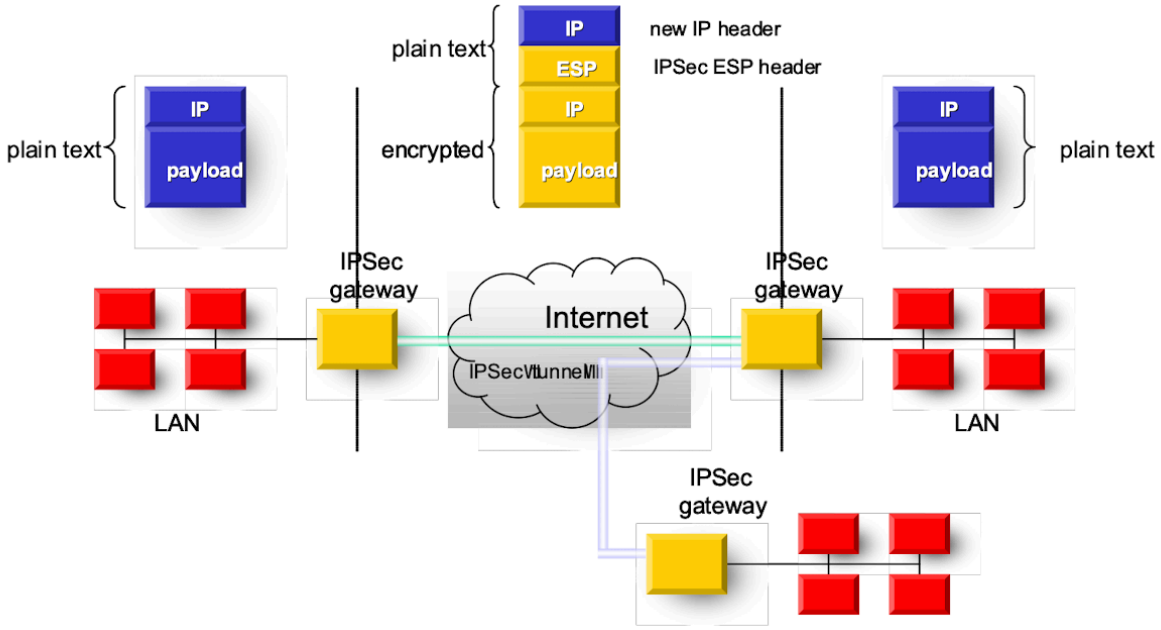
IPSec VPN

- 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）

IPSec VPN



Chap8：应用层安全协议

电子邮件发送时多个接收者时该怎么办?

发送者生成一个密钥，采用对称密码算法加密报文，即S{M} 再用接收方的公钥加密密钥S，并与加密的报文同时发送。假设接收者有A、B、C 三人，就分别生成三个加密密钥KA{S}，KB{S}， KC{S}，对报文进行认证

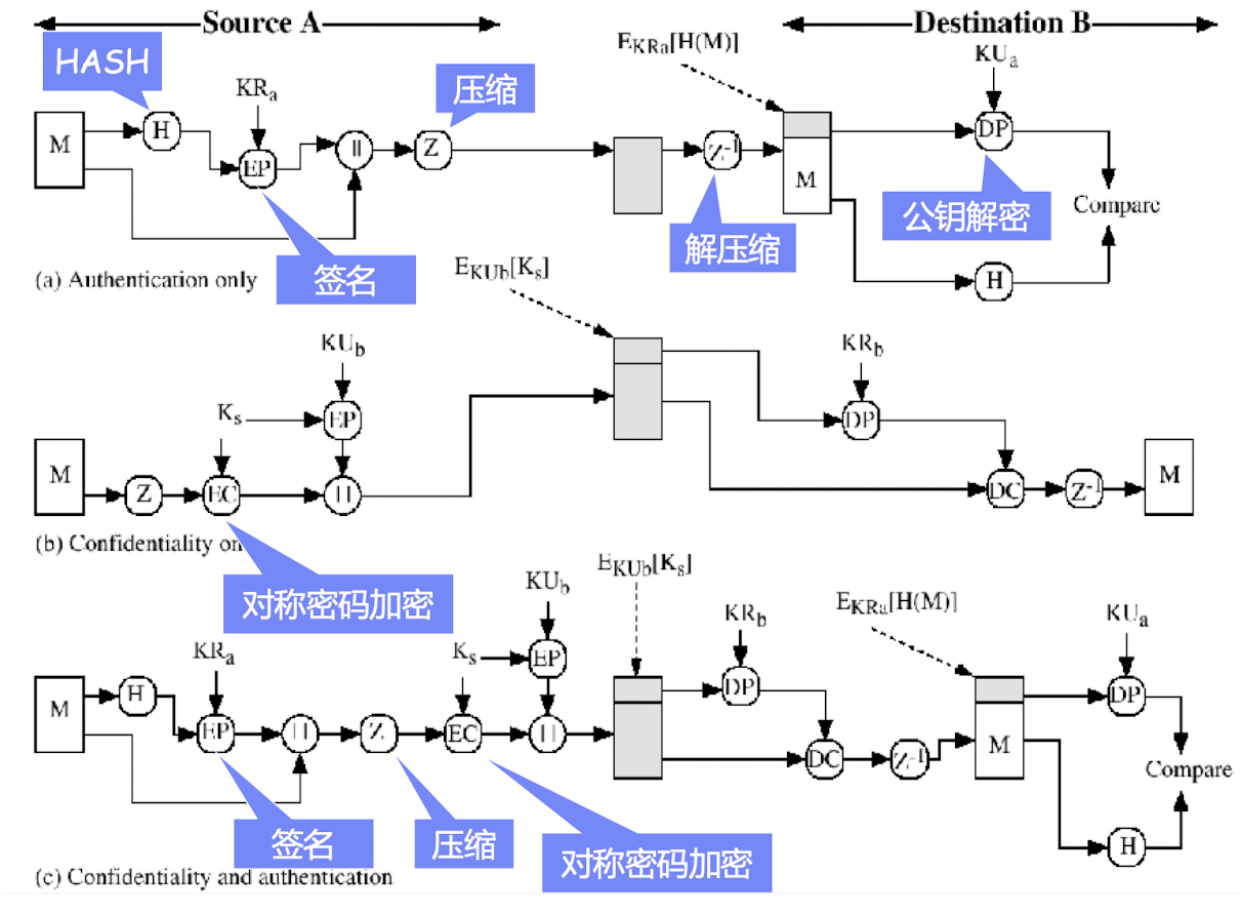
PGP

基本功能、安全服务、操作原理

PGP提供的安全业务：

- **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。**在压缩前签名，压缩后加密。**
- **兼容性：**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

操作原理

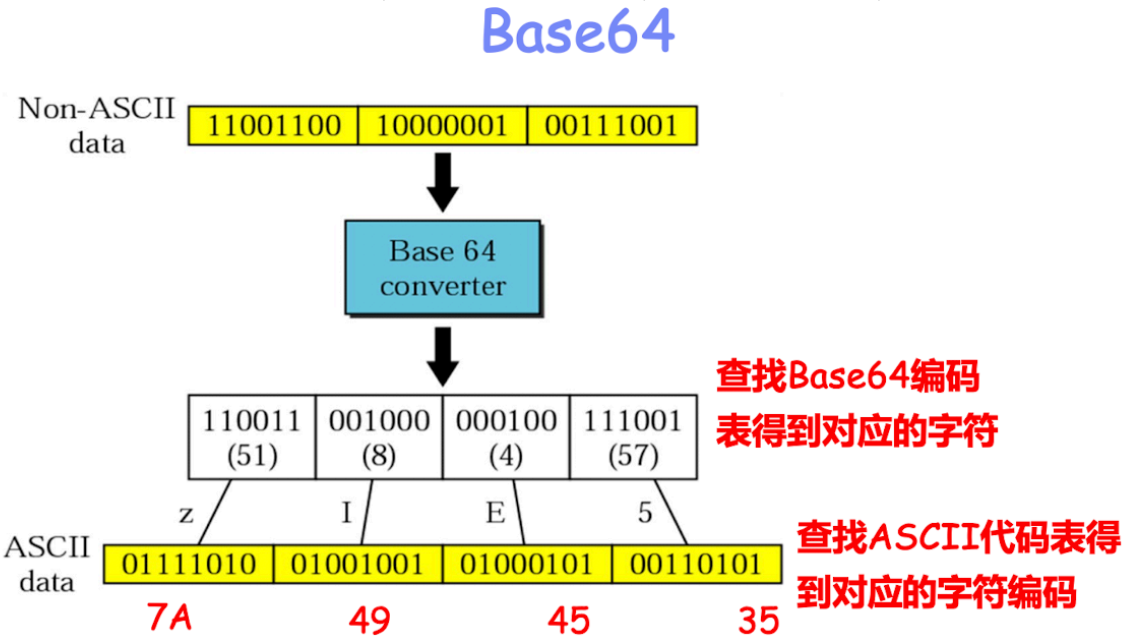


压缩

- **PGP 的压缩过程在报文的签名和加密之间，即先对报文签名，然后压缩，再是加密**
    - 签名后再压缩是为了方便保存未压缩的报文和签名，为了以后存储方便，如果签名是对压缩后报文进行 的，势必要保存一份压缩的文档与之对应，或者增加 部分计算。但相同的压缩算法可能产生略微不同的压 缩结果。
    - 压缩后加密可以节约传输文件的存储空间，加快加密速度，且因为压缩，减少了原文中的关联性，使密码 分析也更困难
- **压缩算法采用ZIP**

基64转换

基64转换方式的采用将原报文扩展了33%.
把3个8位字节转化为4个6位的字节，先**查对应的基-64表**，再**对应到ASCII表**，首位置0



若编码的数据不是3字节的整数倍，转换时不够6位的后面加0补成6位，如果数据长度对3余1，编码结果加2个"=="，余2，加1个"="

公钥环、私钥环

加密密钥

PGP使用**四种类型密钥**：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

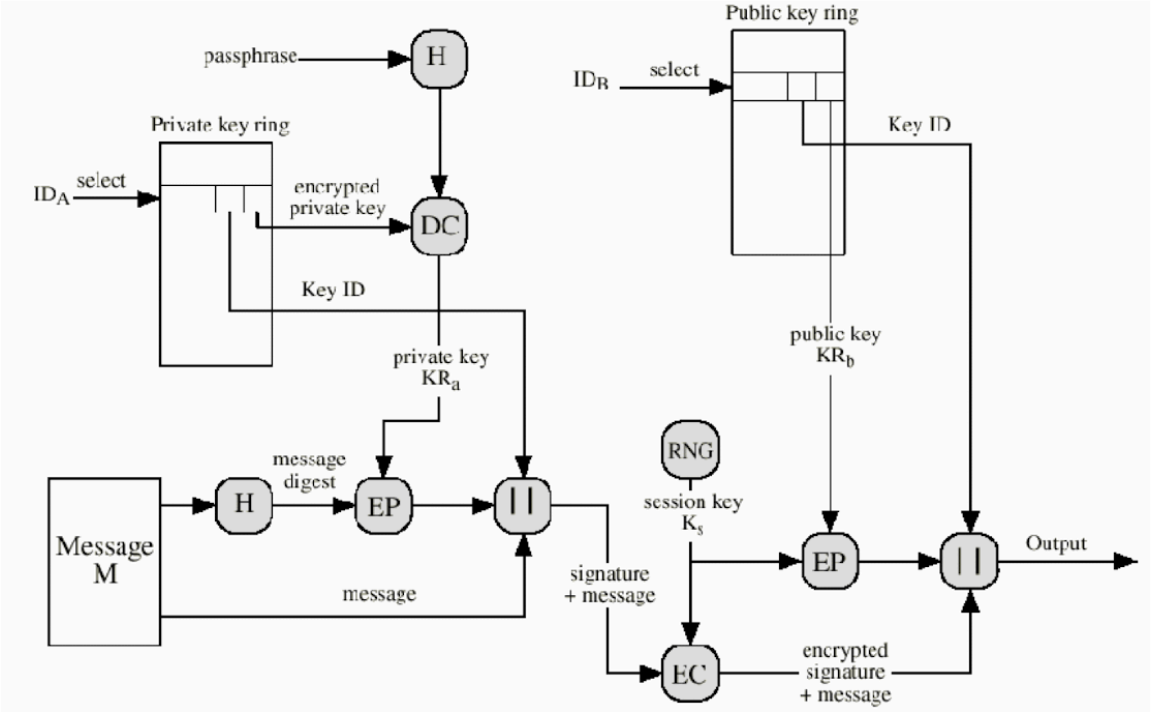
公钥管理

PGP虽然采用公钥密码体系，但不是证书。如何保证公钥是合法的?

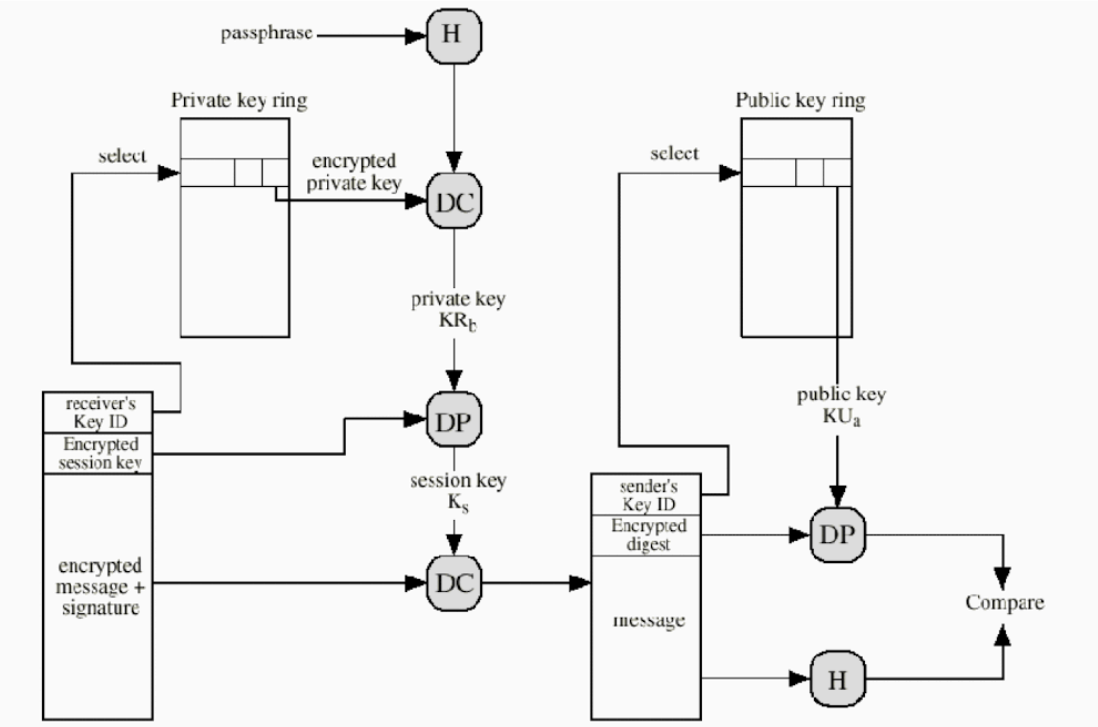
- 直接索取，其他方式确认
- 从可信任证书机构获得B的公钥
- **采用信任关系保护（从可信第三方）公钥**
    - **完全信任、部分信任、不信任**

PGP消息生成、接受操作流程

PGP message生成操作



PGP message 接收操作



私钥的保存

SET协议

基本概念

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。采用公钥密码体制，遵循X.509数字证书标准。

SET的系统组成

- **持卡人（Cardholder**:由发卡行所发行的支付卡的授权持有者
- **商家(Merchant)** :出售商品或服务的个人或机构，商家必须与收单行建立业务联系以接受支付卡这种付款方式
- **发卡行（Issuer**：为持卡人建立一个帐户，并发行支付卡的金融机构

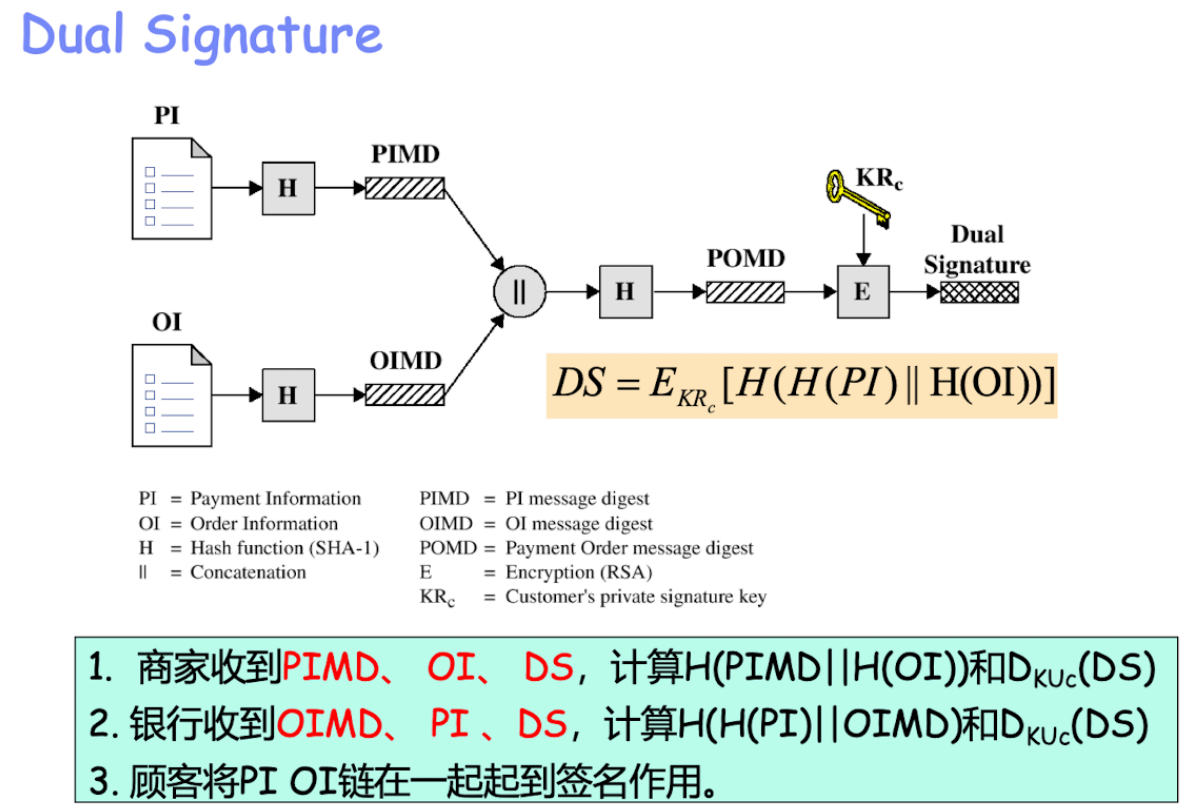
- **收单行（Aquirer**：为商家建立帐户并处理支付卡授权和支付的金融机构
- **支付网关（payment gateway**：由收单行操作的设备，实现对支付信息从Internet到银行内部网络的转换，并对商家和持卡人进行认证

数字信封

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

双重签名



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。

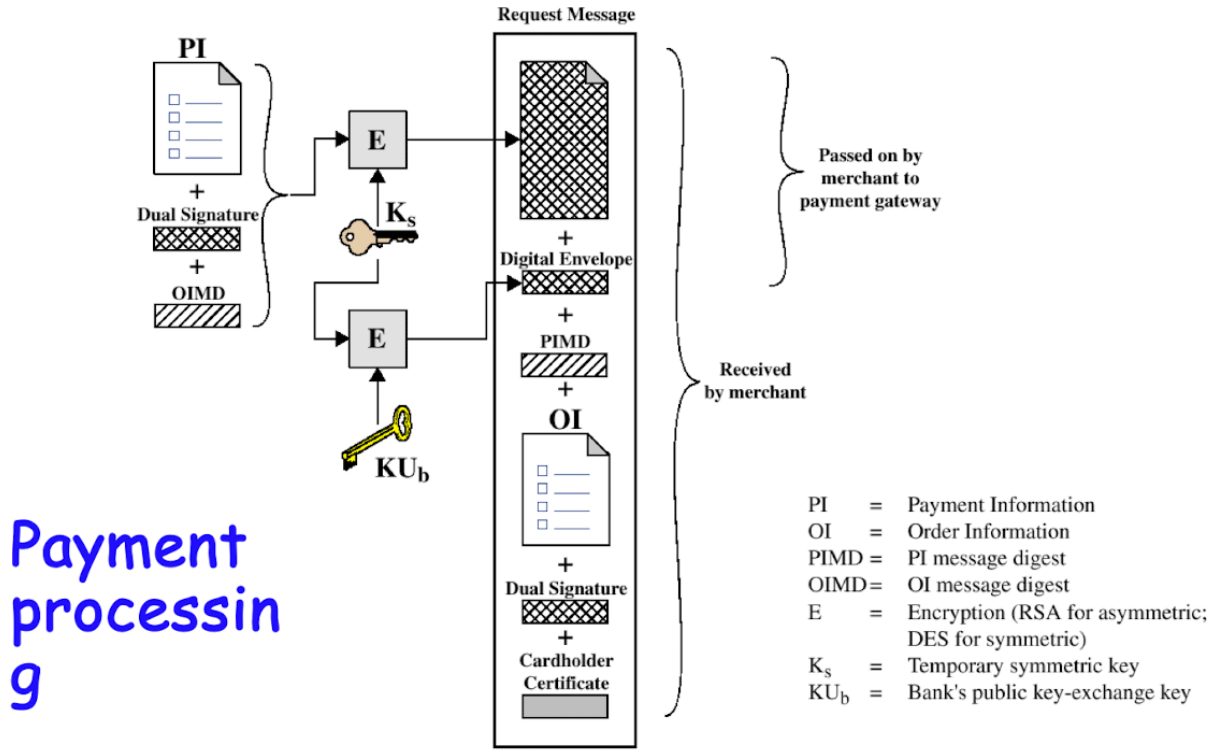
双重签名流程

持卡人发送购买请求

- **持卡人生成订单信息和支付指令**

    - **订单信息（Order Information, OI）**：包括商品描述、数量、价格等。
    - **支付指令（Payment Information, PI）**：包括信用卡号、有效期等。
- **计算订单信息的哈希值**
    - 持卡人对订单信息 OI 进行哈希运算，得到哈希值 $H(OI)$。
- **计算支付指令的哈希值**
    - 持卡人对支付指令 PI 进行哈希运算，得到哈希值 $H(PI)$。
- **连接哈希**
    - 将两个哈希值连接在一起，得到 $H(OI)||H(PI)$。
- **对连接的哈希值进行签名**
    - 持卡人使用自己的私钥对连接的哈希值 $H(OI)||H(PI)$ 进行数字签名，得到数字签名DS。
- **加密支付指令**
    - 持卡人使用商户的公钥对支付指令 PI进行加密，得到加密支付指令 $E(PI)$。
- **发送数据**
    - 持卡人将订单信息 OI、加密支付指令$E(PI)$、以及数字签名DS一起发送给商户。

持卡人发送购买请求（Purchase request）



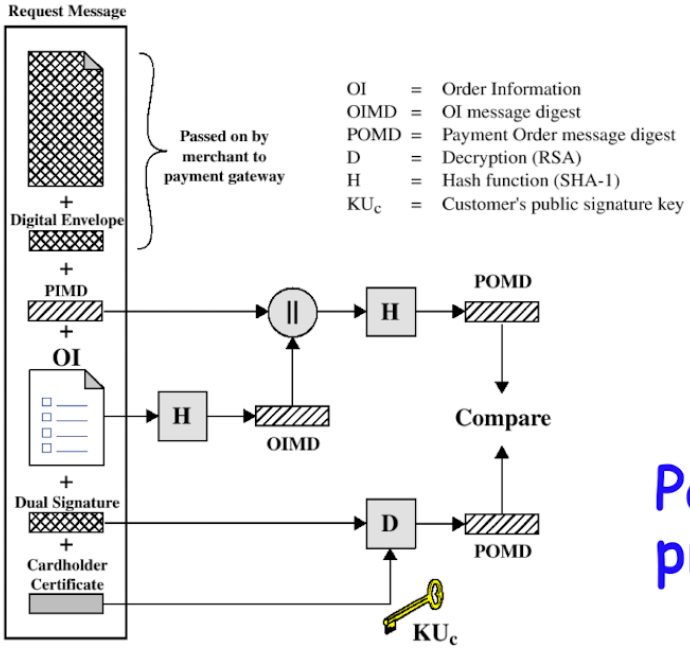
Payment processing

商家验证过程

商户处理过程

- **验证数字签名**
  - 商户使用持卡人的公钥对数字签名DS进行验证，确保DS是由持卡人生成的。
  - 商户计算订单信息OI的哈希值$H(OI)$。
  - 商户将$H(OI)$和发卡行返回的$H(PI)$连接起来，得到$H(OI)||H(PI)$，并与持卡人的签名结果进行比对，验证签名的正确性。
- **发送加密支付指令**
  - 商户将加密的支付指令$E(PI)$转发给支付网关

商家验证过程



Merchant Verifies Customer Purchase Request

Chap9：WLAN安全

WEP

WLAN的基本概念、安全需求

WLAN的安全需求

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

漫游认证、切换认证的区别，可能的方法

区别总结

1. **应用场景**：
   - **漫游认证**用于设备在不同AP之间移动时的认证，确保网络连接的连续性和安全性。
   - **参与认证**用于设备首次连接到网络时的身份验证，确保只有授权用户能够访问网络。
2. **认证频率**：

- **漫游认证**频率较高，因为设备在移动时可能频繁切换AP。
- **参与认证**通常只在设备初次连接网络或网络策略发生变化时进行。

3. **技术实现**：
   - **漫游认证**通常需要支持快速过渡协议（如802.11r）和缓存认证信息，以加快认证过程。
   - **参与认证**依赖于标准的认证协议和安全凭据，如WPA2-PSK或WPA2-Enterprise。

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

WPA 是对 WEP 的改进，提供了更强的加密和认证机制。WPA 引入了以下关键特性：

- **TKIP**：动态生成每个数据包的加密密钥，从而增强了加密的安全性。
- **MIC**：检查数据包的完整性，防止数据被篡改。
- **预共享密钥**：用于家庭和小型办公室网络，用户手动输入密钥。
- **802.1X 认证**：用于企业网络，通过认证服务器（如 RADIUS）进行用户认证。

WPA2

WPA2 是对 WPA 的进一步改进，成为 2004 年的强制标准。WPA2 主要引入了以下特性：

- **AES**：取代了 WPA 中的 TKIP，提供了更强的加密算法。
- **CCMP**：增强的数据完整性检查。
- 两种操作模式
  :
  - **WPA2-Personal**：使用预共享密钥（PSK）进行认证。
  - **WPA2-Enterprise**：使用 802.1X 认证和 RADIUS 服务器进行用户认证。

WAPI

WAPI是中国提出的一种无线局域网安全标准，旨在替代WPA和WPA2等国际标准，提供更高的安全性。WAPI由中国标准化管理委员会批准，是国家强制性标准GB 15629.11-2003。

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?

功能：实现主体身份和主体公钥之间的绑定关系

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

其他：证书序列号、版本，有效期等

生成证书：CA用自己私钥签名证书摘要附在证书之后

撤销原因：私钥泄漏、关系终止、CA私钥泄漏

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。

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

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

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。

方法：数字信封、D-H密钥交换

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

第二次小测

1.简单描述IPSec隧道模式和传输模式的区别?

传输模式：为IP载荷提供认证、完整性和机密性。
隧道模式：保护整个IP分组，提供认证、完整性和机密性。

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）

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。
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）

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?

字段：可变不可预测的，例如跳数
覆盖范围：ESP不包括IP首部

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?

32位对齐
加密算法要求分组为某字节的整数倍
某些字段要求为某字节的整数倍（例如段偏移）
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?

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：减少重新协商密钥产生的开销
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
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**

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?

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）

零碎知识点

DES：数据**分组长度为64位**，密文分组长度也是64位，使用的**密钥为64位**，**有效密钥长度为56位**，**有8位用于奇偶校验**

MD5（128bit），SHA-1（160bit），SHA-2（包括6种）

IPv4（32bit），IPv6（128bit）

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

ISAKMP协议：下层由UDP协议承载，端口号为500

IKE v1的主模式中：用公钥加密认证中存在的问题

- 采用了**四次公钥加/解密操作**，耗费计算资源，**与签名认证算法相比，多了两次加/解密**
- 修改方法
    - 采用修正的公钥加密认证