密码学

基本概念

密码学 = 密码编码学 + 密码分析学，编码学要点：

- 转换明文为密文的运算：置换和代换

  原则为可逆。代换变换的是**字母**, 而置换变换消息中各个字母的**位置**。
- 所用密钥数：对称密码和非对称密码
- 处理明文的方法：分组密码和流密码，一次一块 or 一字

古典密码

安全依赖于算法保密性。

- Caesar $c = (m + 3) \mod 26$
- 密钥词密码 单表代换，一个密钥词放在前面，其余按顺序
- Playfair 5*5 字母矩阵，i/j 用同一个编码
- Hill $C = KP \mod 26, P = K^{-1}C \mod 26$

  用于解密的 C 应当是取模之前的值。
- Vigenere 和 Verman

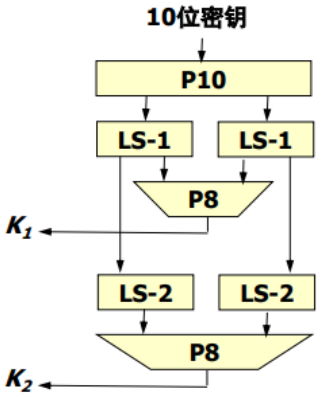
  都是流密码。
- Enigma

对称密码

安全性不在于算法保密性，在于密钥保密性；密钥以秘密信道分配给收发双方。

S-DES

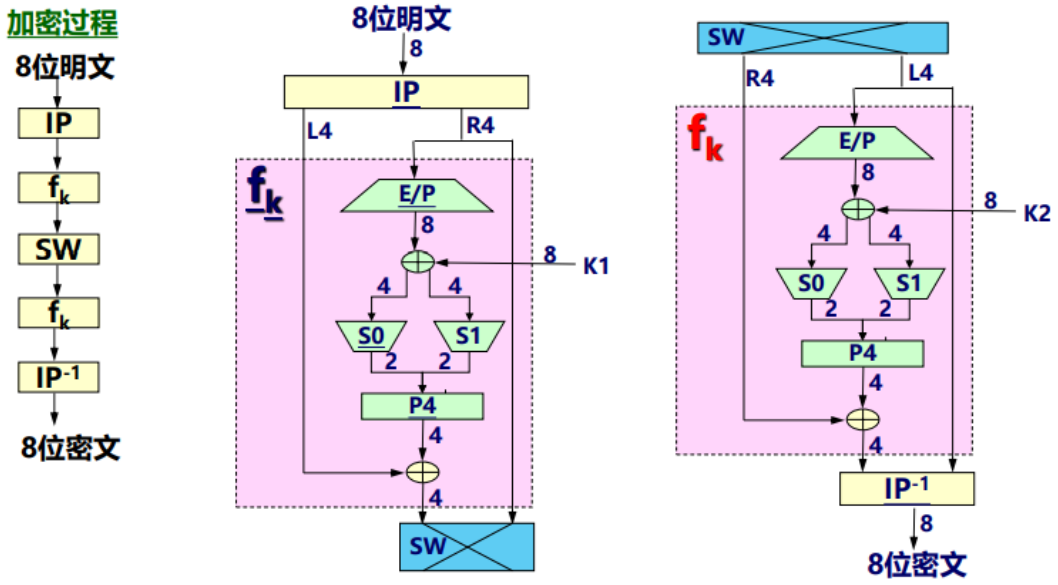
- 计算密钥 K1 K2



- 明文 -> IP -> fk1 -> SW -> fk2 -> IP^-1 -> 密文

  密文 -> IP -> fk2 -> SW -> fk1 -> IP^-1 -> 明文

  fk 特点：只变化左四位



Feistel 分组密码结构

- 扩散是指**使明文的统计特征不包含在密文中**，让每个明文数字尽可能地影响多个密文数字
- 混淆是尽可能地**使密文和密钥间的统计关系更复杂**

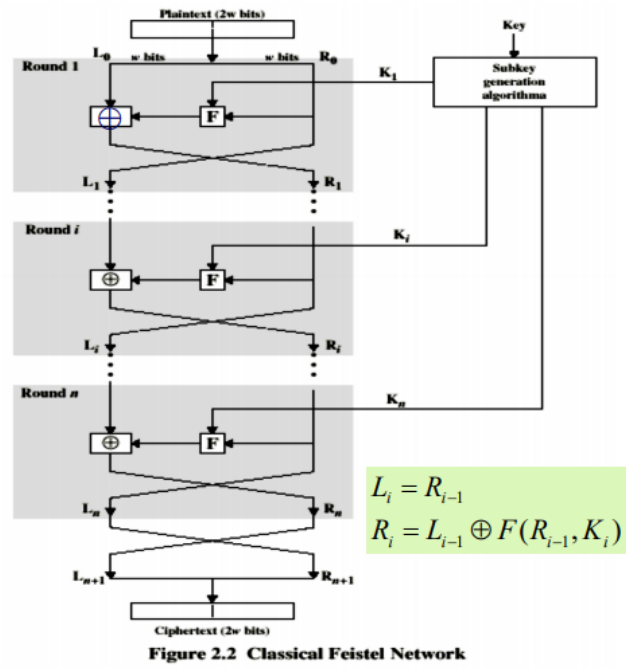


Figure 2.2 Classical Feistel Network

元素：分组长，密钥长，迭代轮数，Ki 产生算法，F 函数。

其它对称分组密码：

- DES/3-DES，RC5：基于 Feistel structure
- Bluefish，RC5：Modified Feistel
- AES：不基于 Feistel structure

非对称密码

基于数学函数而不是代换、置换。

错误说法：公钥密码比传统密码更安全、通用、分配更简单。实际上公钥算法只用于密钥交换和数字签名。

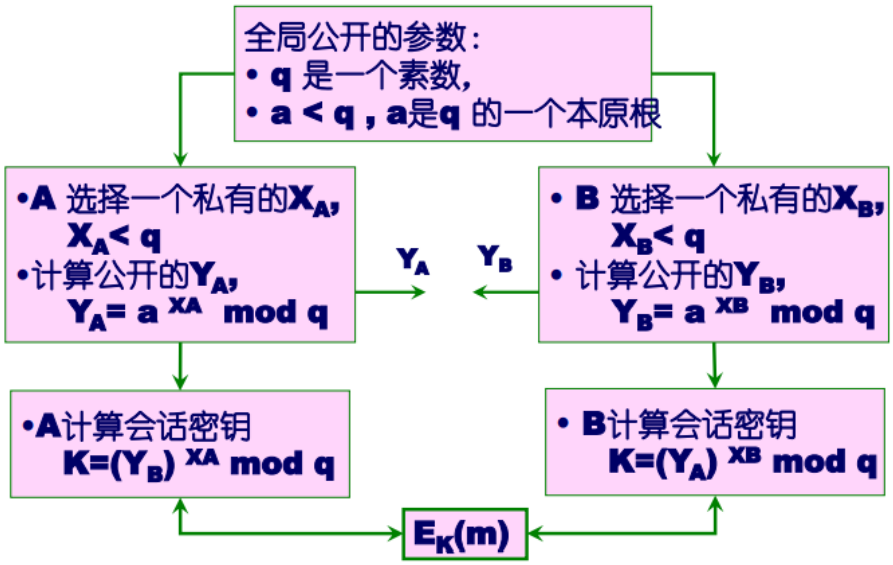
RSA

- 取素数 p, q 计算 $n = pq, \phi(n) = (p-1)(q-1)$
- 取与 $\phi(n)$ 互素的 e，再找 $d < \phi(n)$ 使得 $de = k\phi(n) + 1$
- 得到公钥 e, n, 私钥 d, n

加密 $C = M^e \mod n$ 解密 $M = C^d \mod n$

DH

只用于密钥交换。



密钥分配

- 对称密码密钥分配

  密钥分配中心 KDC 模式：

  1. A 向 KDC 请求一个会话密钥以保护与 B 的连接
  2. KDC 用 Ka 加密的消息应答，其中包括一次性会话密钥 Ks，和给 B 的内容，用 Kb 加密
  3. A 将加密内容发给 B，B 用 Kb 解密，s建立连接
- 公钥分配
- 用公钥分配对称密码密钥

认证技术

消息认证

消息认证是**验证所收到的消息确实来自真正的发送方且未被修改。**

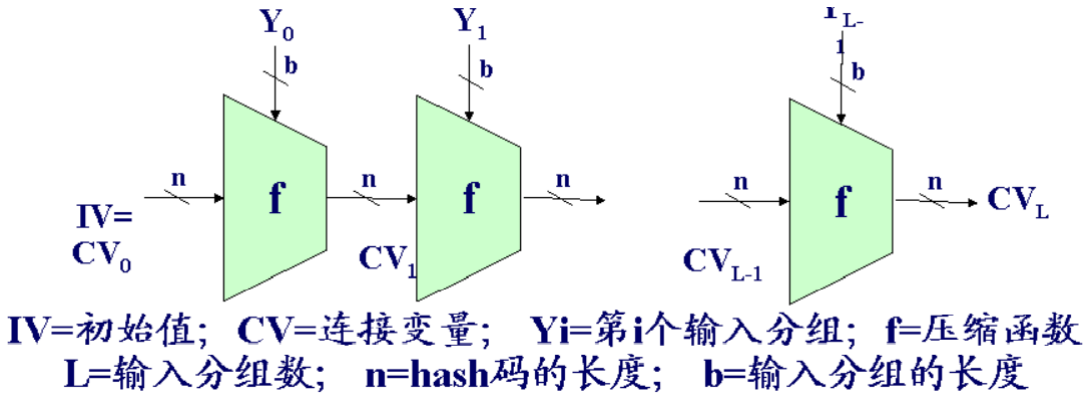
- 数字签名用于**抗击发送方否认**：接收方可以假称自己收到某消息，因此发送方也可以假称没有发送过某消息。

认证函数

- 消息加密、MAC、Hash
- MAC = Hash + 对称加密

加密形式	传输内容	认证	保密	数字签名
对称加密	$E_k[M\|\|H(M)]$ 或 $E_k[M]\|\|H(E_k[M])$	✅	✅	
对称加密	$M\|\|E_k[H(M)]$	✅		
发送方私钥	$M\|\|E_{KRa}[H(M)]$	✅		✅
发送方私钥+对称加密	$E_k[M\|\|E_{KRa}[H(M)]]$	✅	✅	✅
共享秘密值S	$M\|\|H(M\|\|S)$	✅		
共享秘密值S+对称加密	$E_k[M\|\|H(M\|\|S)]$	✅	✅	

安全 Hash 函数的一般结构



MD5，SHA1，RIPEMD-160 均在此框架下，基本步骤：

1. 添加填充位
2. 添加长度
3. 初始化 IV
4. 分组处理消息
5. 输出结果

身份认证

Basic 认证

每次 Http 请求，客户端都要向服务端发送账号和口令。

表单认证

- 解决 Basic 认证将账号、口令在客户端长期保存，每次都进行账号口令验证的问题。

流程类似 jwt.

仍然存在提交表单时，账号和口令被监听的风险。

改进：

- 对账号和口令加密
- 用挑战响应机制**避免重放攻击**：身份认证前，服务器向客户端返回随机生成的挑战码 M，
    - Basic认证中，客户端发送 $M||C_k(M)$ 用 MAC 进行认证。

- 表单认证中，客户端用口令 k 加密计算 $E_k(M||U)$, 并将账号 U 和 $E_k(M||U)$ 发送给服务端，服务端用存储的口令 k' 计算 $E_{k'}(M||U)$，比对，以完成用户身份验证。

访问控制技术：防火墙

设计目标：

- 所有从内到外或从外到内的通信，都必须经过防火墙
- 只有经过授权的通信才能通过防火墙，这些授权在本地安全策略中规定
- 不同类型的防火墙将实现不同的安全策略
- 防火墙本身必须免疫渗透，这意味着必须使用运行安全 OS 的可信系统

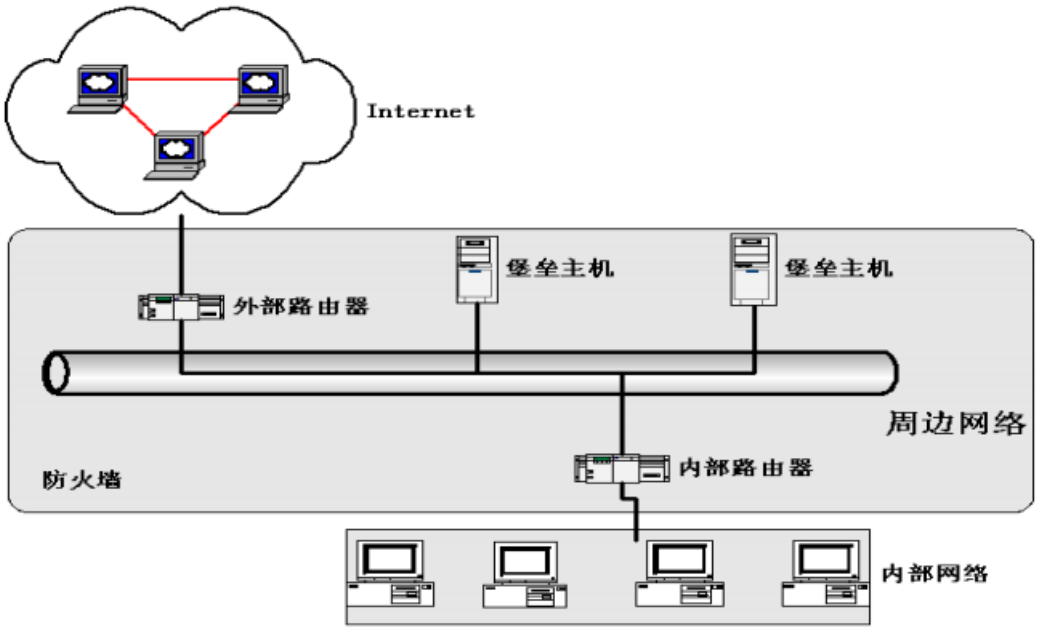
局限性：

- 需要用户定义访问控制规则，没有缺省配置
- 不能防止内部恶意的攻击者，不能替代内部网络系统的安全管理
- 无法控制没有经过它的连接
- 不能很好地防止病毒和信息扩散
- 防火墙无法防范全新的威胁和攻击

争议：

- 破坏了 Internet 端到端特性
- **防外不防内**
- 降低了人们的主机安全意识

屏蔽子网结构



- 不设防区 DMZ 放置在内部网络和外部网络之间。
- 外部路由器只允许互联网对 DMZ 的访问，拒绝所有目的地址为内部网络地址的包，拒绝所有不以内部网络为源地址的包进入互联网；
- 内部路由器防止互联网或DMZ访问内部。

互联网安全协议

安全目标 CIA

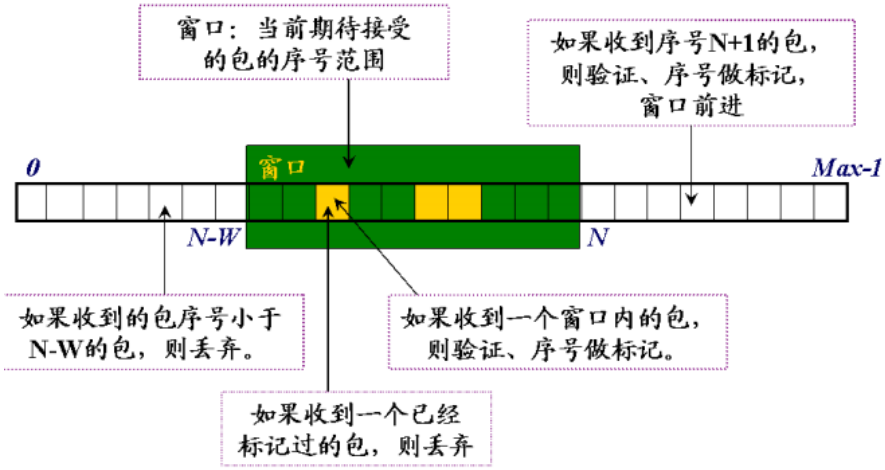
- confidentiality 机密性：防止信息泄露给未授权实体
- integrity 完整性：防止信息被篡改，或能检测篡改

- availability 可用性

IPsec

原理：在IP层加密/认证所有流量。

- IPSec 用**不可重复的序列号域** (Sequence Number)和**接收窗口**防范重放攻击。



安全关联

安全关联 SA，记录**一次 IPSec 连接的参数**，存储于 OS 维护的 SADB 中。

SA 是发送方到接收方的**单向**关系。包括：

- 安全参数索引 SPI
  - SPI = 0 被保留，在报文中出现表示 SA 不存在
  - 使得接收方能选择合适的SA处理接收包
- 目的 IP、安全协议：AH/ESP

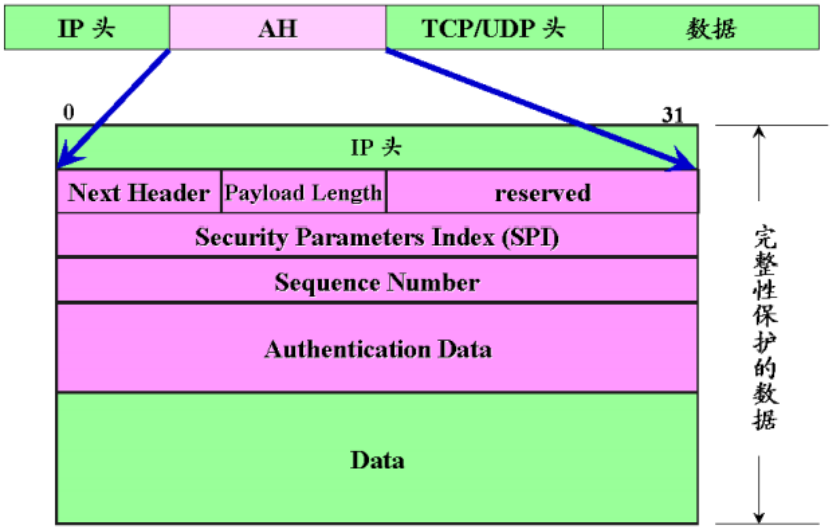
SPDB 入口，又称 SA 选择子，再输出 IP 包时选定 SA 进行处理。

安全服务

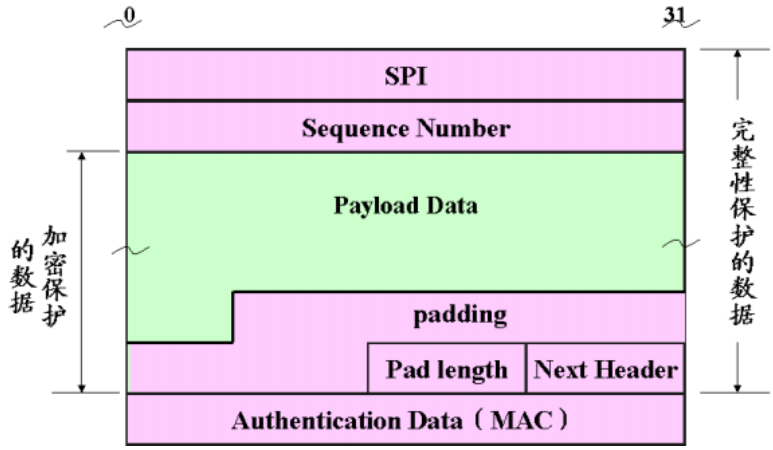
由 **AH (认证) 或 ESP (加密/加密+认证)** 提供。

认证基于 MAC，双方必须共享一个密钥。

- AH 认证 IP 载荷和 IP 头的固定/可预测部分

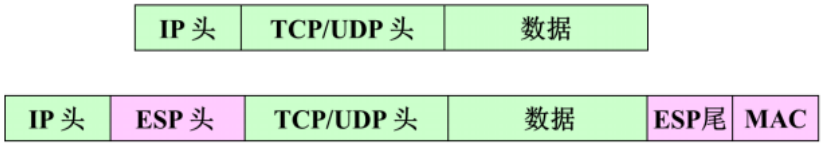


- ESP 加密和认证 (optional) IP 载荷



模式

- 传输模式，以 ESP 为例



- 隧道模式，以 AH 为例

安全关联组合

提供特定的 IPSec 服务集所需的 SA 序列。

- 传输邻接，只允许一级组合

  [IP1] [AH] [ESP] [upper]

- 隧道迭代，允许多层嵌套

  [IP2] [AH] [IP1] [ESP] [upper]，先加密后认证的例子

IKE

自动管理 IPsec SA 和 SADB.

- 核心技术是用 DH 算法交换密钥

两个阶段：

- 协商 IKE SA，有主模式和快速模式
  - 主模式提供了对通信双方的身份保护
  - 快速模式不提供身份保护，能减少信息传输的数量，也**适用于一方地址为动态的情况。**
- 协商 IPsec SA，只有快速模式
  - 一个 IKE SA 协商能为多个 IPSec SA 协商提供服务。

工作模式，可嵌套：

- 传输模式，端主机之间
- 隧道模式，安全网关之间

工作过程：

- IKE 守护进程运行于 OS 后台，当需要创建 SA 时，查询 SPDB 获得参数开始协商；协商成功则将得到的 SA 加入 SADB；
    - SPDB（Security Policy Database）决定 IP 包 与 SA 的联系。
- 不再使用某个 SA 时，IKE 守护进程将其从 SADB 删除，并通知远程的 IKE 守护进程。

SSL

传输层安全协议，为应用层提供保密性、完整性、身份认证。

体系结构：

- 会话：以握手协议建立，协商密码算法、主密钥等信息
- 连接：用会话的信息进行 TCP 通信，不支持 UDP.

SSL 握手协议

在传输应用数据前，协商密钥交换、加密、MAC 算法、主密钥，认证 Server 和 Client.

1. 建立安全能力
2. 服务器认证和密钥交换
3. 客户端认证和密钥交换
4. Finish

主密钥用于产生其他密钥.

SSL 记录协议

提供数据保密性和完整性。

- 分段，压缩（可选），**增加 MAC，加密**，增加首部

安全性分析

SSL 的安全性基于RSA等算法。

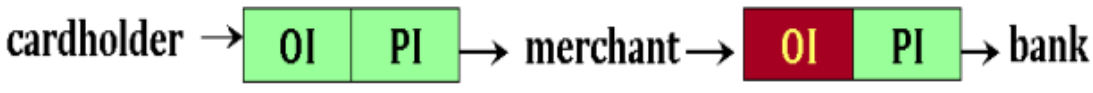
通过128位长的随机数“连接序号”，能防范重放攻击。

HTTPS = HTTP + SSL

依然无法避免ARP欺骗攻击，但由于加密传输，**不会泄露明文，攻击者无法篡改报文。**

SET

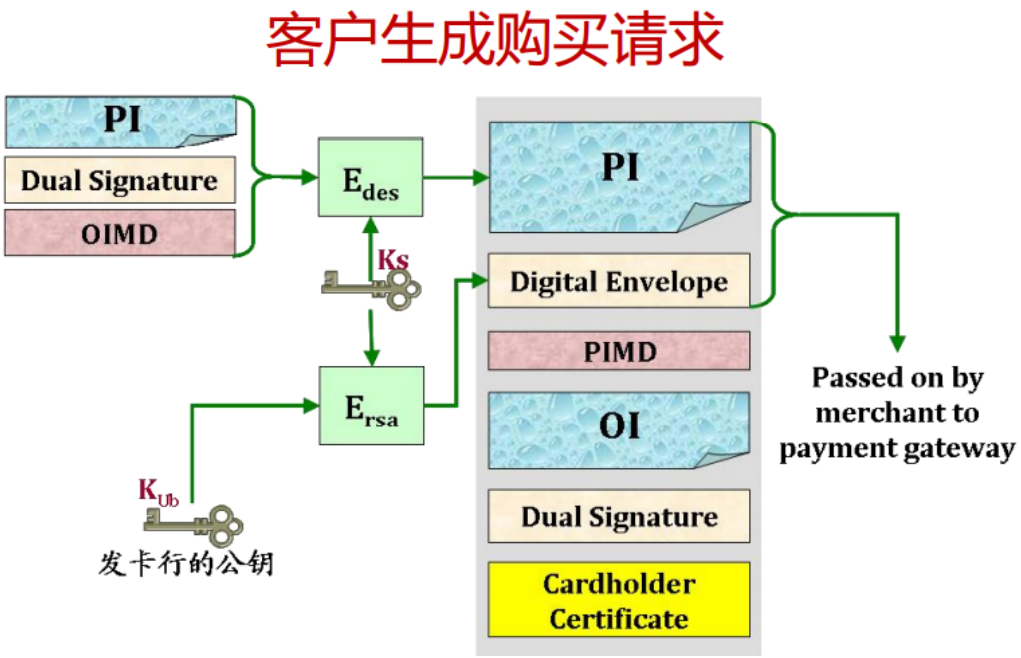
保证电子交易信息的私密性、保密性、完整性、抗抵赖。

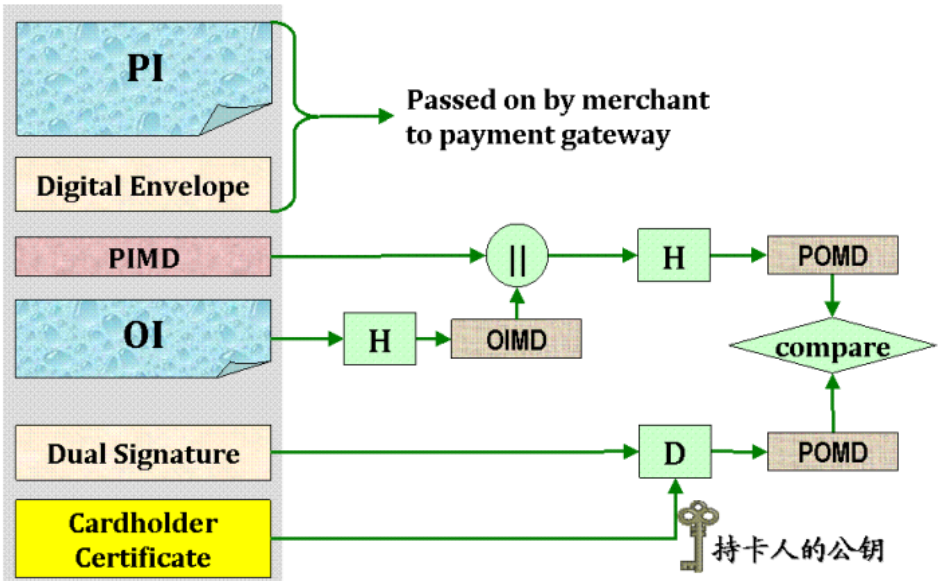


PI = Payment Information，OI = Order Information

OI 只暴露给商家，而 PI 只暴露给支付网关，为了防止 PI 泄露给商家或被商家篡改，需要**双签名。**

Dual Signature = $E_{kRc}[H(H(PI)||H(OI))]$，kRc 是用户私钥。





支付网关用其私钥解开数字信封 (Digital Envelope)，得到 Ks，解密 authorization block，验证双签名。

阶段：购买请求，支付授权，支付获取。

- 双签名主要用于前两个阶段

软件入侵技术

	概念	**需要宿主**	**自主传播**
陷门	程序的秘密入口，使访问者获得非法权限	是	否
逻辑炸弹	嵌在合法程序中，特定事件（通常为一个日期）出现时才会进行破坏的程序代码	是	否
Zombie	秘密地通过网络控制计算机，使其能发动攻击	否	是
特洛伊木马	**伪装**为有用的程序，但内部藏有隐蔽代码，留下后门	是	否
病毒	自我复制，感染其他程序和计算机。 **寄宿在宿主程序上**	是	是
蠕虫	利用网络系统漏洞将自己复制到其他计算机上，耗尽计算机资源	**否**	是