**出题依据：p162（双重签名）**

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)。

**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）

**可能用到的符号：**

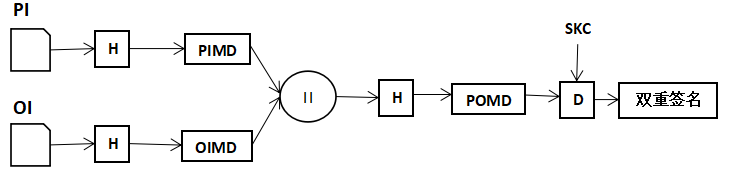
**DS：**双重签名 **OI：**订货信息 **PI：**支付信息 **H：**报文摘要算法

**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

**参考答案：**

**1.表达式：DS=Dskc（H（H（PI）|| H（OI）））**

**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H（PIMD|| H（OI））和Epkc（DS），在H（PIMD|| H（OI））=Epkc（DS）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H（OIMD|| H（OI））与Epkc（DS）是否相等，若H（OIMD|| H（OI））=Epkc（DS），确认双重签名，不相等则持卡人双重签名失败。**