**密钥分发的可能方式**

　　1、A选择一个密钥后以物理的方式传递给B

　　2、第三方选择密钥后物理地传给A和B

　　3、如果A和B先前或最近使用过一个密钥，则一方可以将 新密钥用旧密钥发送给另一方

　　4、如果A和B到第三方C有加密连接，则C可以在加密连接上发送密钥给A、B

**分析：**

　　1和2都需要人工交付，对链路加密（设备一对一连接）可行，对网络通信则不可行，因为网络通信涉及大量密钥

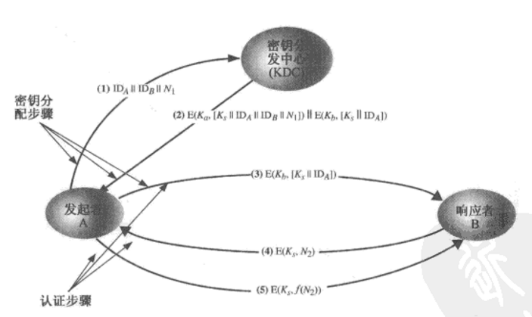
　　对于3，一旦攻击者获得一个密钥，则后序所有密钥便都不再安全。

　　4需要第三方即密钥分发中心，在网络通信中得到了广泛的应用。

**密钥分发方案**

**基本原理：**密钥分发中心KDC和每个终端用户都共享一对唯一的主密钥（用物理的方式传递，如U盾）。终端用户之间每次会话，都要向KDC申请唯一的会话密钥，会话密钥通过与KDC共享的主密钥加密来完成传递。

**典型方案描述**



　　　　1、A以明文形式向KDC发送会话密钥请求包。包括通话双方A、B的身份以及该次传输的唯一标识N1，称为临时交互号(nonce)。

　　　　　　临时交互号可以选择时间戳、随机数或者计数器等。KDC可根据临时交互号设计防重放机制。

　　　　2、KDC返回的信息包括两部分。

　　　　　　第一部分是A想获取的信息，用A的主密钥KA加密，包括通话密钥Ks和KDC收到的请求包内容用以验证消息到达KDC前是否被修改或者重放过。

　　　　　　第二部分是B想获取的信息，用B的主密钥KB加密，包括通话密钥Ks和A的身份。A收到后这部分消息便原样发给B。

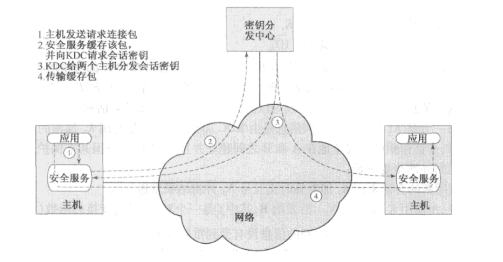
　　　　3、为保证A发给B的会话密钥信息未被重放攻击，A、B使用会话密钥进行最后的验证。

　　　　　　B使用新的会话密钥Ks加密临时交互号N2并发给A。A对N2进行一个函数变换后，用会话密钥发给B验证。

　　　　对于大型网络，可以建立KDC的层次体系来使得主密钥分发的开销最小化。

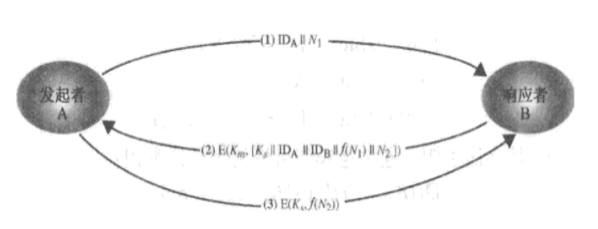
**透明的密钥控制方案**

　　　　其中心思想是通过设定专门的会话安全单元（SSM）来完成代表主机、获取会话密钥和加密会话消息的功能



**分布式的密钥控制方案**

　　　　该方案的核心思想是将每个终端都兼职干KDC的活。这显然大大增加了主密钥的数量（N(N-1)/2个），适合一些对KDC安全性要求高的中小系统。



　　　　Km是AB共享的主密钥。

**会话密钥生命周期**

　　　　对于面向对象的协议，在会话整个生命周期中使用同一个会话密钥，为每次新的会话使用新的会话密钥。若一个会话的生命周期很长，则周期性改变会话密钥。

　　　　对于无连接的协议如面向事务的协议，则可约定时间或者数量分配不同的会话密钥

**控制密钥的使用**

**目的：**

　　　　　　1、通过某种标识区分密钥的种类及使用范围

　　　　　　2、避免主密钥作为数据加密密钥带来的安全风险

**控制向量解决方案：**

　　　　　　1、KDC生成会话密钥Ks，同时使用一个控制向量CV，根据约定的规范描述会话密钥的用法和限制。然后用以下公式生成消息返回给用户。

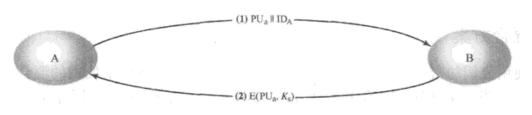
　　　　　　　　　　C = E([Km⊕h(CV)] , Ks) || CV　　　　　　　　h为Hash函数    Km是用户主密钥

　　　　　　2、用户可直接通过逆操作还原会话密钥　　Ks = D([Km⊕h(CV)] , E([Km⊕h(CV)] , Ks))

　　　　　　这样，通过将主密钥与CV异或避免了主密钥可能的暴露，同时也规范了会话密钥的使用。

由于公钥加密系统效率较低，几乎不会用于大数据块的直接加密，而是经常用在小数据块的加密上，其最重要的应用之一就是用于密钥分发，比如KDC的主密钥分发。

**简单的密钥分发方案**



　　1、A产生公私钥对{PUa,PRa}，然后将公钥和A的身份信息发给B。

　　2、B产生一个会话密钥，并用A的公钥加密发给A。由于只有A的私钥能解密，因此A能得到会话密钥。

　　缺陷：

　　这个方案很容易被中间人攻击。即有中间人同时扮演B和A的角色分别与A和B通信，从而获取会话密钥。根本原因就是这个方案缺乏认证。

**确保保密性和身份认证的密钥分发系统**

