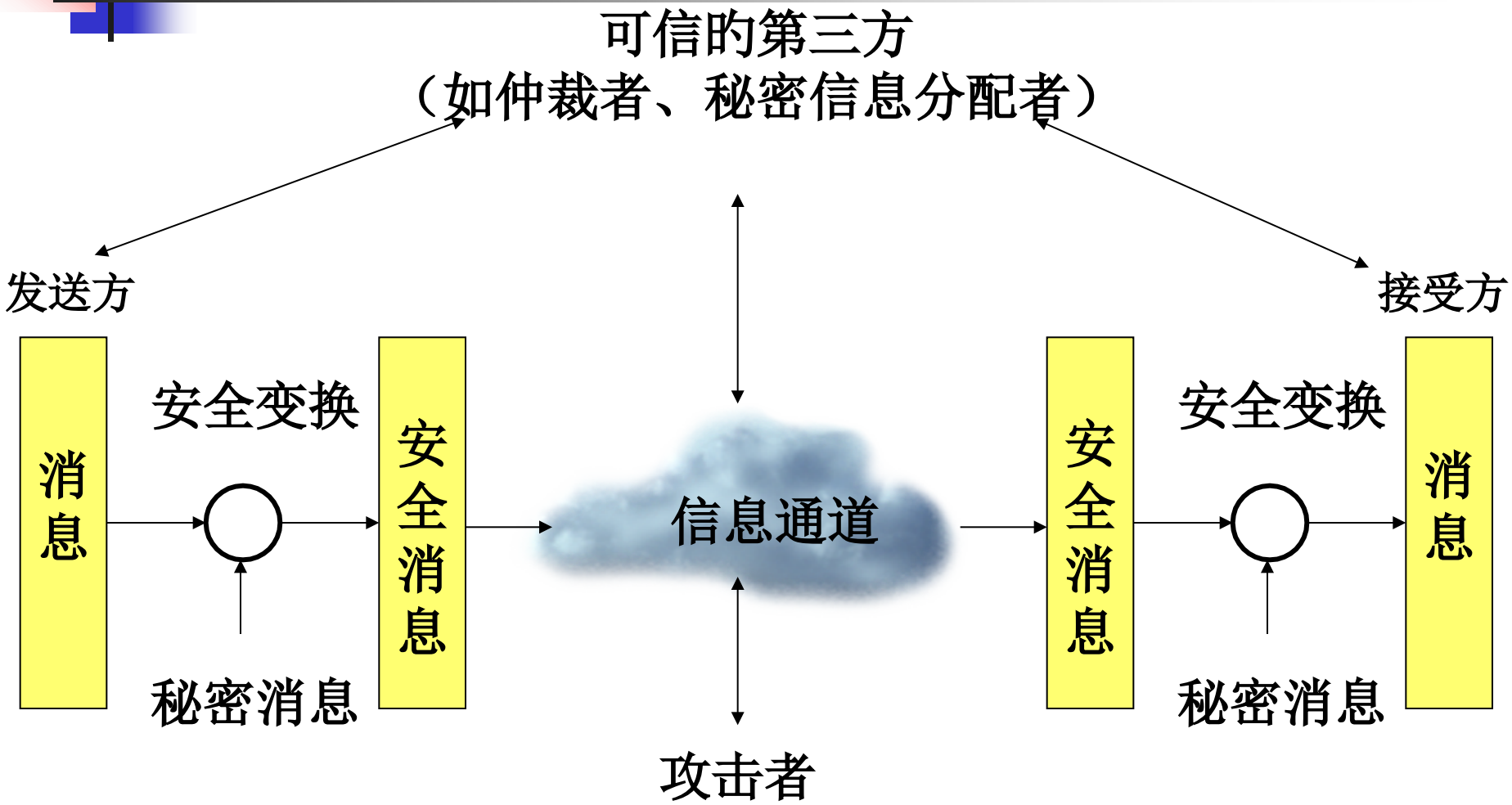
信息安全
密钥管理和PKI

网络安全模型


可信的第三方
（如仲裁者、秘密信息分配者）
发送方
接受方
消息
安全变换
安全消息
秘密消息
信息通道
攻击者
安全消息
安全变换
消息
秘密消息

设计安全服务需要涉及四个方面

- 设计执行安全有关的算法。该算法是攻击者无法攻破的。
- 产生算法使用的秘密信息
- 设计分配和共享秘密信息的措施
- 指明通信双方使用的协议，该协议利用安全算法和秘密信息实现安全服务

主要内容

- 密钥分配与管理
- PKI与PMI

密钥分配

- 全部的密码技术都依赖于密钥。
- 网络安全中，密钥的地位举足轻重。怎样安全可靠、迅速高效地分配密钥，怎样管理密钥一直是密码学领域的主要问题。
- 密钥管理措施因所使用的密码体制不同而不同。

密钥分配

- 全部的密码技术都依赖于密钥。
- 网络安全中，密钥的地位举足轻重。怎样安全可靠、迅速高效地分配密钥，怎样管理密钥一直是密码学领域的主要问题。
- 密钥管理措施因所使用的密码体制不同而不同。

密钥分配

- 密钥的生存周期：授权使用该密钥的周期
  - 拥有大量的密文有利于密码分析；一种密钥使用得太多了，会给攻击者增大搜集密文的机会；
  - 在单一密钥受到威胁时，限制信息的暴露
  - 限制一技术使用到它估计的使用期
  - 限制计算密集型密码分析攻击的有效时间

密钥分配

- 密钥经历的阶段
  - 产生
  - 分配
  - 使用
  - 更新
  - 撤消
  - 销毁

密钥分配

- 密钥类型
  - 基本密钥（Base Key），又称初始密钥（Primary Key)，顾客密钥(User key)，是由顾客选定或由系统分配给顾客的，可在较长时间（相对于会话密钥）内由一对顾客所专用的密钥。
  - 会话密钥（Session Key），即两个通信方在一次通话或互换数据时使用的密钥。
  - 密钥加密密钥（Key Encrypting Key），用于对会话密钥进行加密时采用的密钥。又称辅助（二级）密钥(Secondary Key)或密钥传送密钥(key Transport key)。通信网中的每个节点都分配有一种此类密钥。
  - 主机主密钥（Host Master Key），对密钥加密密钥进行加密的密钥。

密钥分配

- 密钥类型
  - 公钥体制下，还有公开密钥、秘密密钥、署名密钥之分。
  - 安装使用期限分长久密钥（涉及主密钥、密钥加密密钥和用于完毕密钥协定的密钥）和短期密钥（数据密钥和用于一次会话的会话密钥）。

密钥分配

- 对于通信双方A和B，密钥的分配能够有下列措施
  - 密钥由A选定，经过物理的措施安全地传递给B
  - 密钥由可信第三方C选定，经过物理的措施传递给A和B
  - 若A和B都有一种到可信第三方C的加密连接，则C能够经过加密连接将密钥安全的传递给A和B
  - 若A和B都在可信第三方公布自己的公开密钥，在他们都能够用彼此的公钥进行加密通信

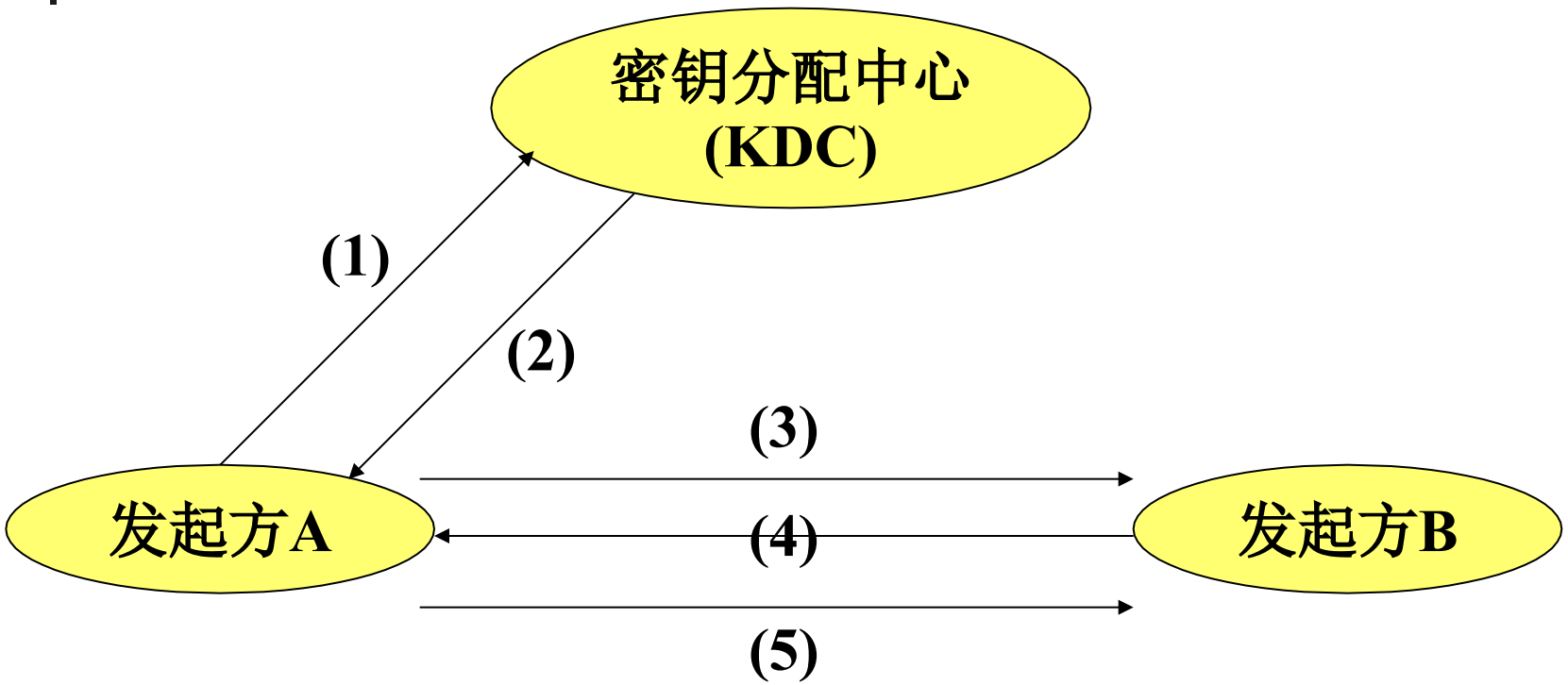
对称加密密钥分配

- 集中式密钥分配方案
  - 由一种中心节点负责密钥的产生并分配给通信各方，或由一组节点构成层次构造负责密钥的产生并分配给通信的各方。
  - 顾客不需要保存大量的会话密钥，只需要保存同中心节点的加密密钥，用于安全传送由中心节点产生的会话密钥。
  - 缺陷：通信量大，需要很好的鉴别功能以认证中心节点和通信方
  - 密钥分配中心KDC技术

集中式密钥分配方案

- 密钥分配中心KDC技术中，假定每个通信方与KDC之间都共享一种唯一的主密钥，且这个主密钥是经过其他安全途径传递的。
  - (1) A→KDC: $ID_a||ID_b||N_1$
  - (2) KDC → A : EKa[Ks||IDa||ID_b||N_1||Ekb[Ks||IDa]]
  - (3) A → B: E_{Kb}[Ks||IDa]
  - (4) B → A: $E_{Ks}[N_2]$
  - (5) A → B: $E_{Ks}[f(N_2)]$
  - IDa和IDb标识通信双方；N_1和N_2是一种目前量(nonce)用来标识目前交互；Ks是分配的会话密钥

集中式密钥分配方案

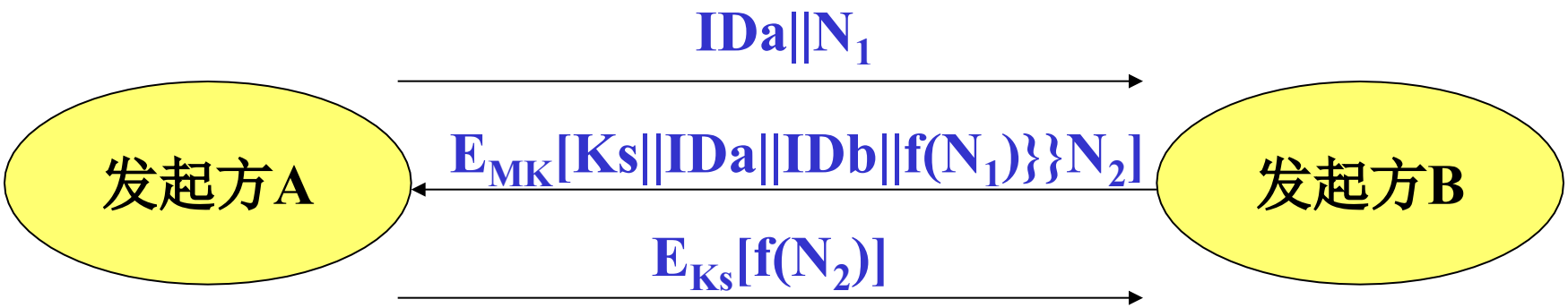


集中式密钥分配方案

- 单个密钥分配中心KDC无法支持大型的通信网络。
  - 每两个可能要进行安全通信的终端都必须同某个KDC共享密钥
- 当通信的终端数量很大，会出现下列问题
  - 每个终端都要同许多密钥分配中心共享密钥，增长了终端的成本和人工分发密钥分配中心和终端共享的主密钥的成本
  - 需要几种尤其大的密钥分配中心，每个密钥分配中心都同几乎全部终端共享主密钥，然而各个单位往往都希望自己来选择或建立自己的KDC

分散式密钥分配方案

- 要求n个通信方保存多达(n(n-1))/2个主密钥，适合于小型网络或一种大型网络的局部范围

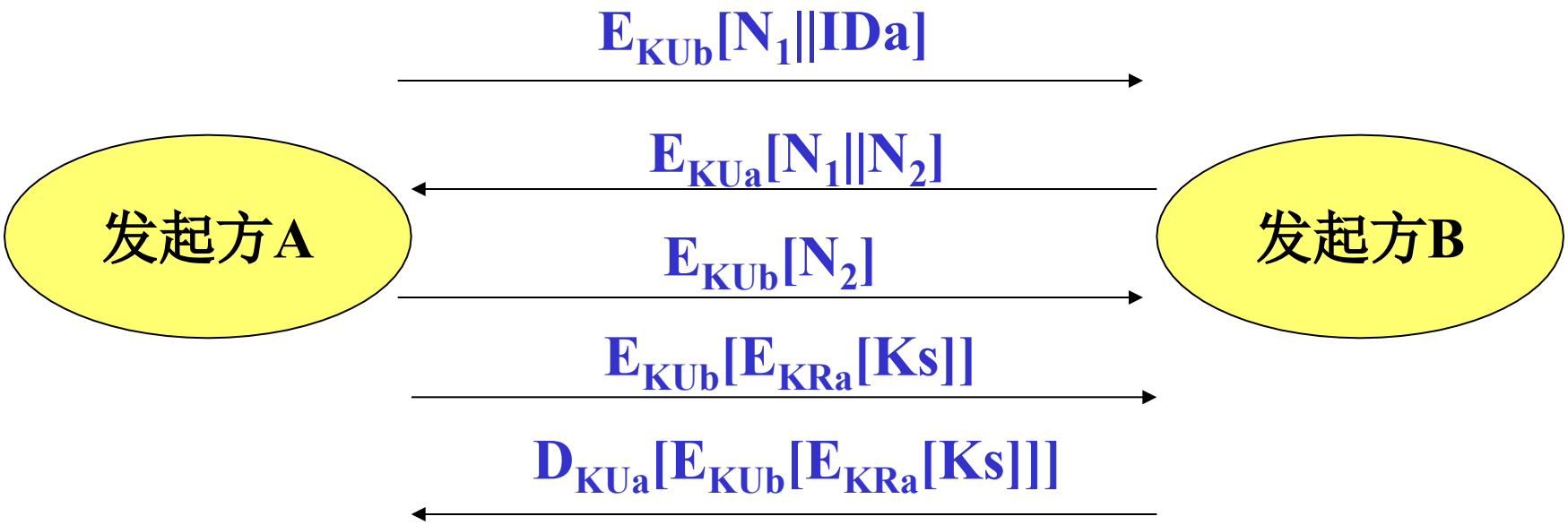


公钥的密钥分配

- 获取通信方的公钥的多种途径
  - 公钥的公开宣告
  - 公开可用目录
  - 公钥管理机构
  - 公钥证书

利用公钥进行对称加密密钥的分配

- 假定通信方A和B已经经过某种措施得到对方的公钥，需要进行对称密钥的分配
- 1-3步进行身份认证，4-5步由A产生密钥Ks，分配于B，并与B共享



密钥的管理

- 密钥的生成
  - 密钥的生成与所使用的密钥生成算法有关，假如生成的密钥强度不一致，则称该算法构成的密钥空间是非线性密钥空间，不然是线性密钥空间。
  - 大部分密钥生成算法采用随机过程或伪随机过程生成密钥。

密钥的管理

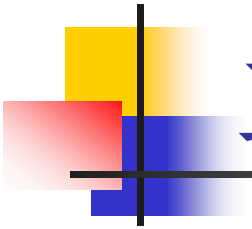
- 密钥的使用
  - 使用时注意保密，并及时更新
  - 确保打算用于一种目的的密钥不能和用于另一种目的的密钥交替使用。将密钥值和密钥的正当使用范围绑定在一起。
- 密钥的存储
  - 将公钥存储在专用媒体（软盘、芯片等）一次性发放给各顾客，顾客在本机中就能够取得对方的公钥，协议非常简朴，又很安全。这种形式只有在KDC等集中式方式下才干实现。
  - 用对方的公钥建立密钥环各自分散保存（如PGP）。
  - 将各顾客的公钥存储在公用媒体中。

密钥的管理

- 密钥的备份与恢复
  - 假如备份的密钥拷贝是可读的，它们应该以两个或两个以上的密钥分量形式存储。当恢复密钥时，必须懂得该密钥的全部分量。
  - 每个密钥分量应该涉及足够大的检验和，是的校验的错误率较低。
  - 密钥的恢复应在多重控制下进行

密钥的管理

- 密钥的销毁
  - 密钥必须定时更换，更换密钥后，原来的密钥必须销毁。
  - 当密钥不再使用，该密钥的全部拷贝都被删除，重新生成或重新构造该密钥的所需信息也被全部删除时，该密钥中断它的生命期。



主要内容

- 密钥分配与管理
- PKI与PMI

PKI技术

- 公钥基础设施（PKI）
  - 利用公钥理论和技术建立的提供信息安全服务的基础设施
  - PKI是一种原则的密钥管理平台，它能够为全部网络应用透明地提供采用加密和数据署名等密码服务所必须的密钥和证书管理。
- 认证技术
  - 数字署名
  - 身份辨认
  - 信息的完整性验证

PKI技术

- **PKI的功能**
  - 证书、密钥的自动更新
  - 交叉认证
  - 加密密钥和署名密钥的分隔
  - 支持对数字署名的不可抵赖
  - 密钥历史的管理