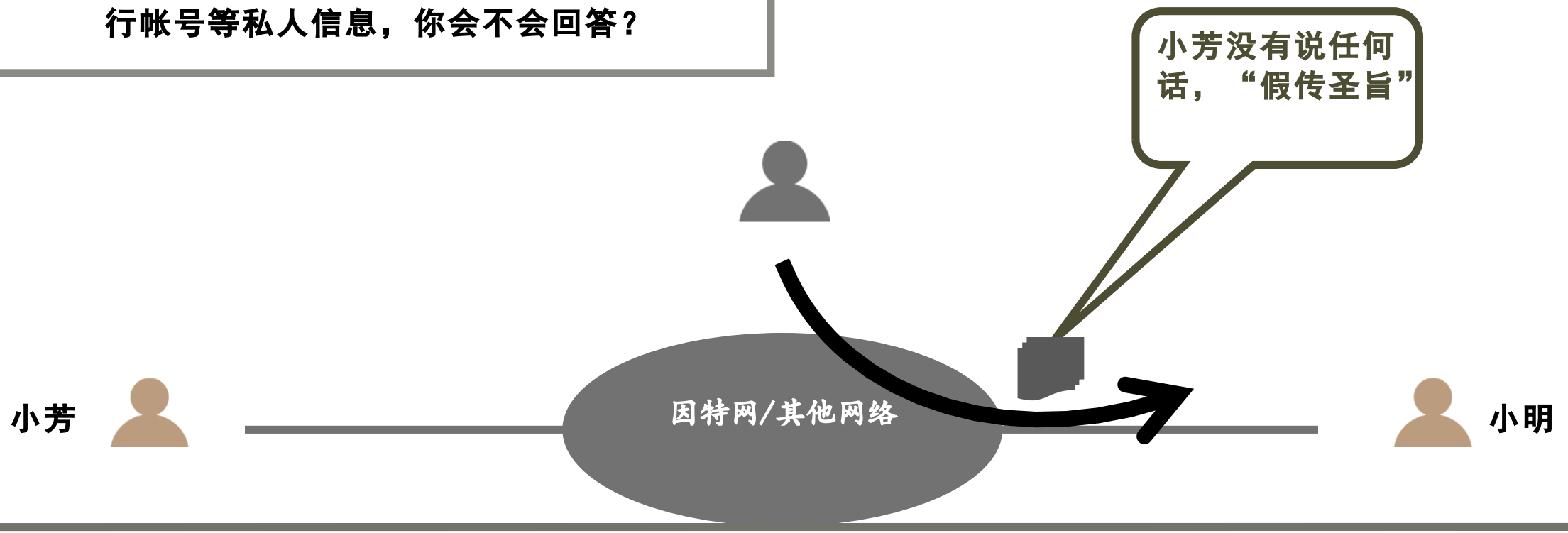
用户认证

如何抵御伪造的信息

认证的目的

- 收到的邮件是来自你认为的那个朋友？
- 有人打电话声称是银行职员，询问银行帐号等私人信息，你会不会回答？

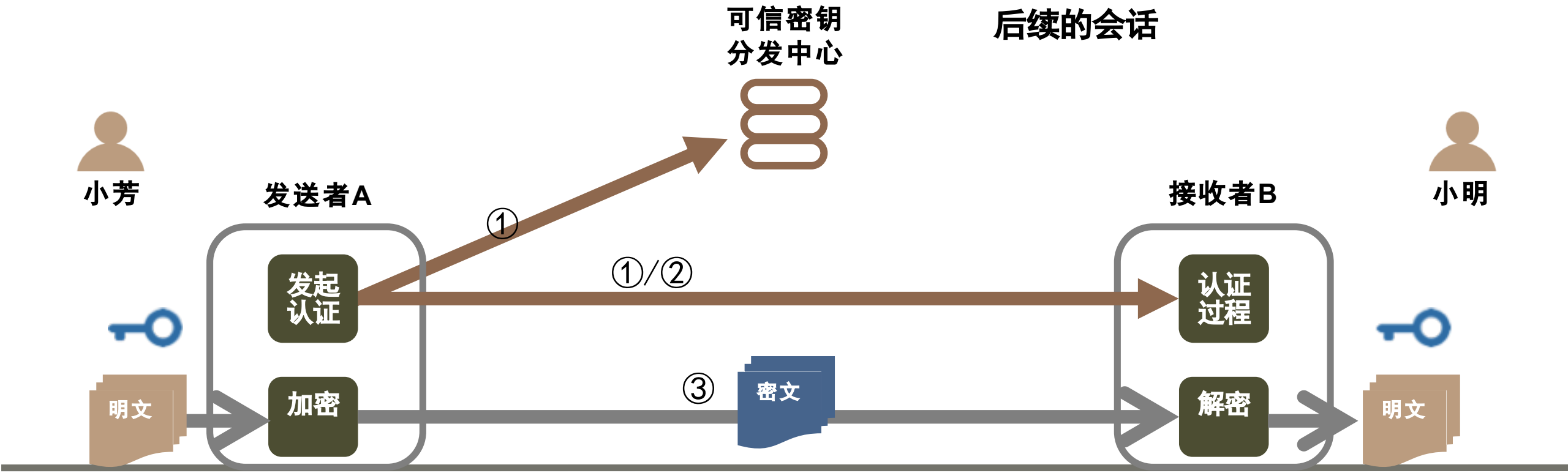
伪造：攻击者伪造信息发送给接收者



认证及其通用模型

认证（Authentication）：一个进程用来验证它的通信对方是否是所期望的实体而不是假冒者的技术。

① 小芳主动发起认证（密钥中心/小明）
② 执行一个认证过程
③ 小芳和小明用秘密的会话密钥加密后续的会话



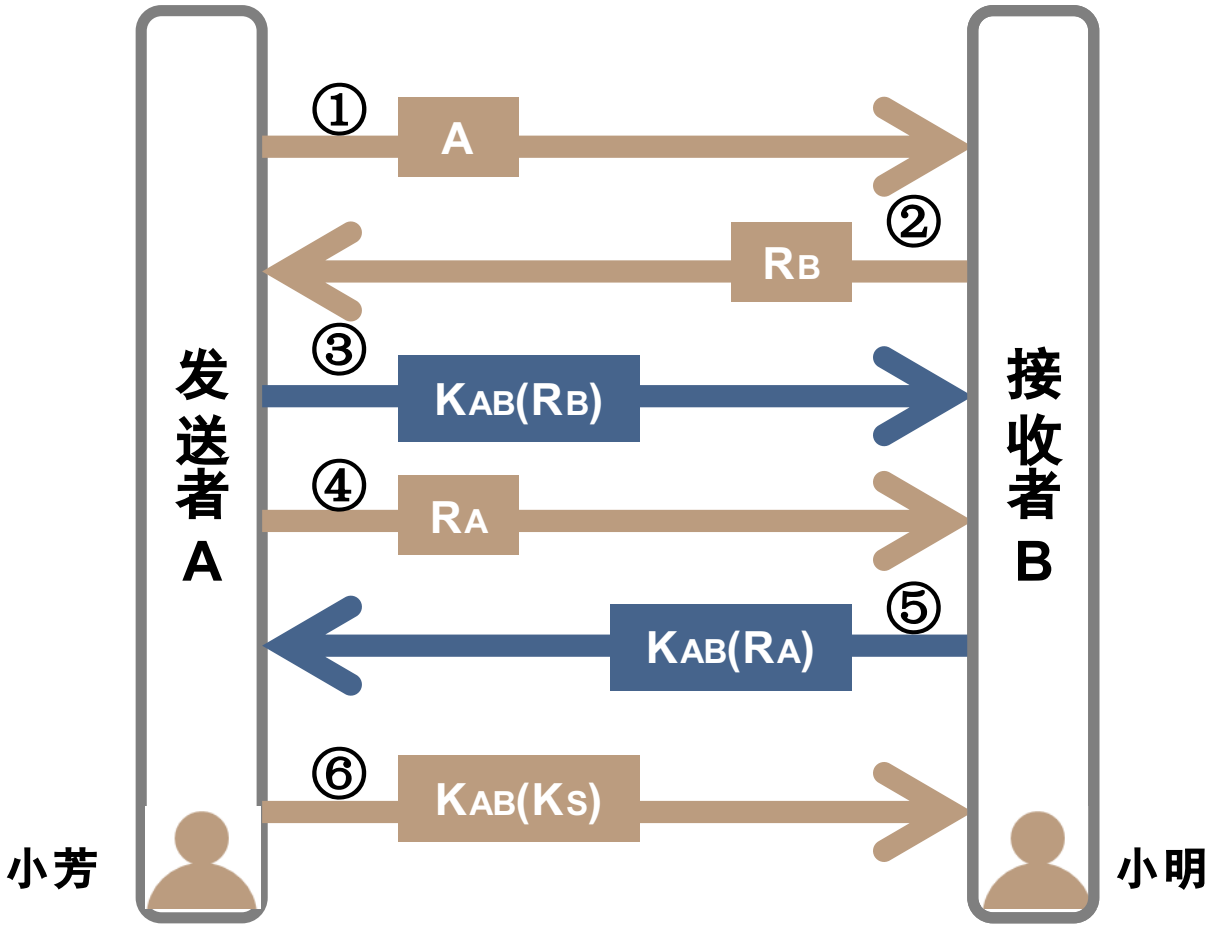
会话密钥

基于共享密钥的认证

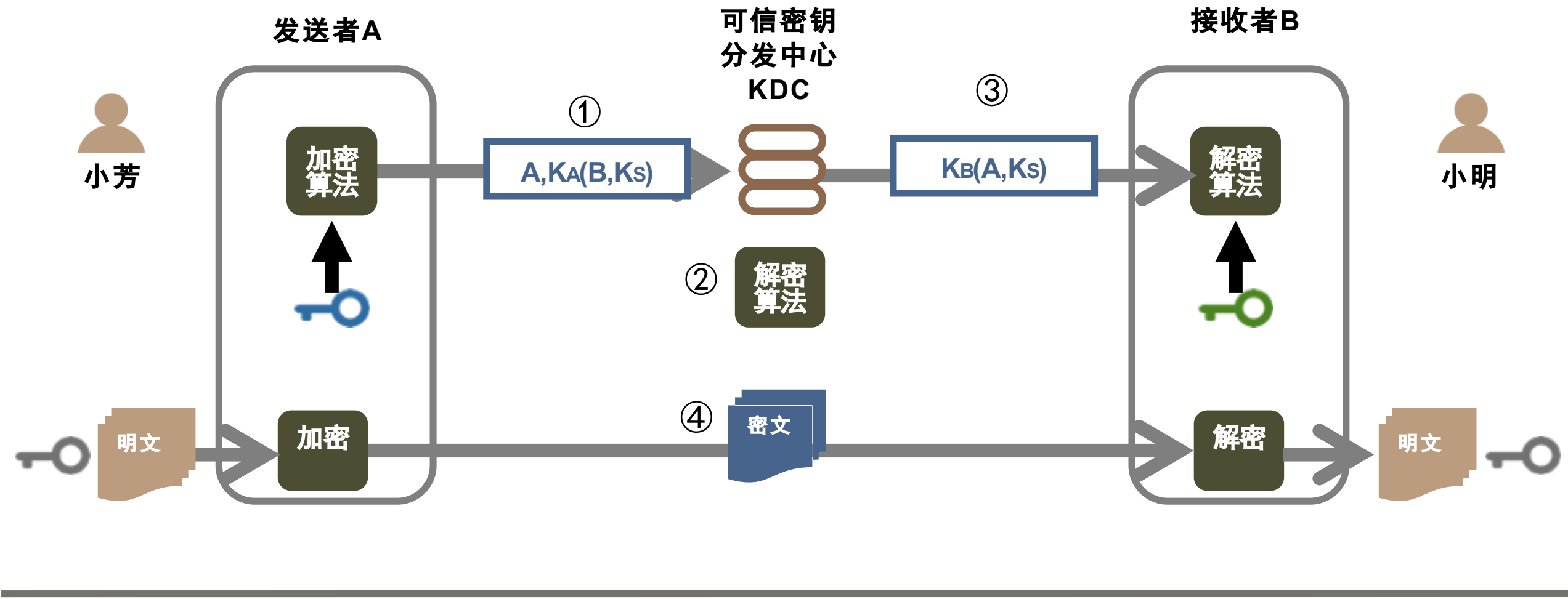
挑战 - 应答（challenge-response）：一方给另一方发送一个随机数，后者将这个随机数做一个特殊的替代，再把结果返回给前者。

- Ri是挑战，i指明了发起挑战的一方
- Ki是密钥，这里i代表密钥的所有者
- Ks是会话密钥

假设：双方已经共享了一个密钥K_{AB}



基于密钥分发中心的认证

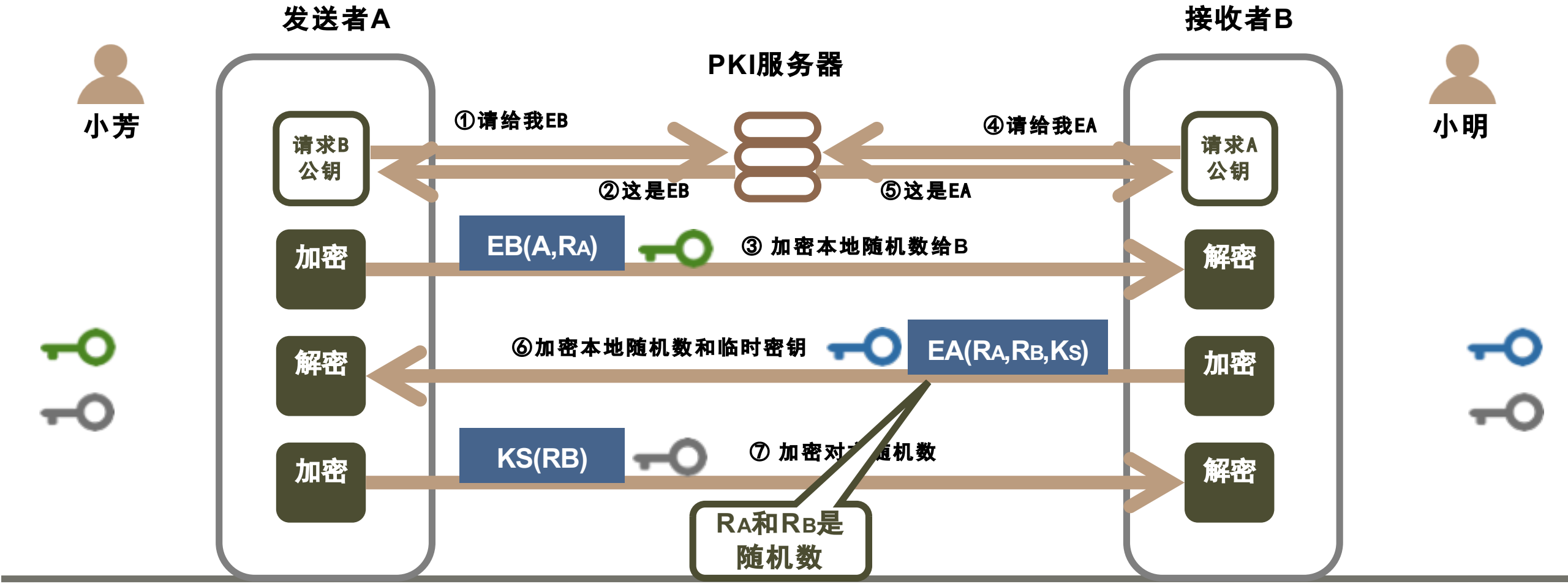


北京大学

KDC与A的密钥　KDC与B的密钥　会话密钥Ks

基于公开密钥的认证

PKI目录服务器：提供公钥证书的查询服务。



A的公钥　B的公钥　会话密钥Ks