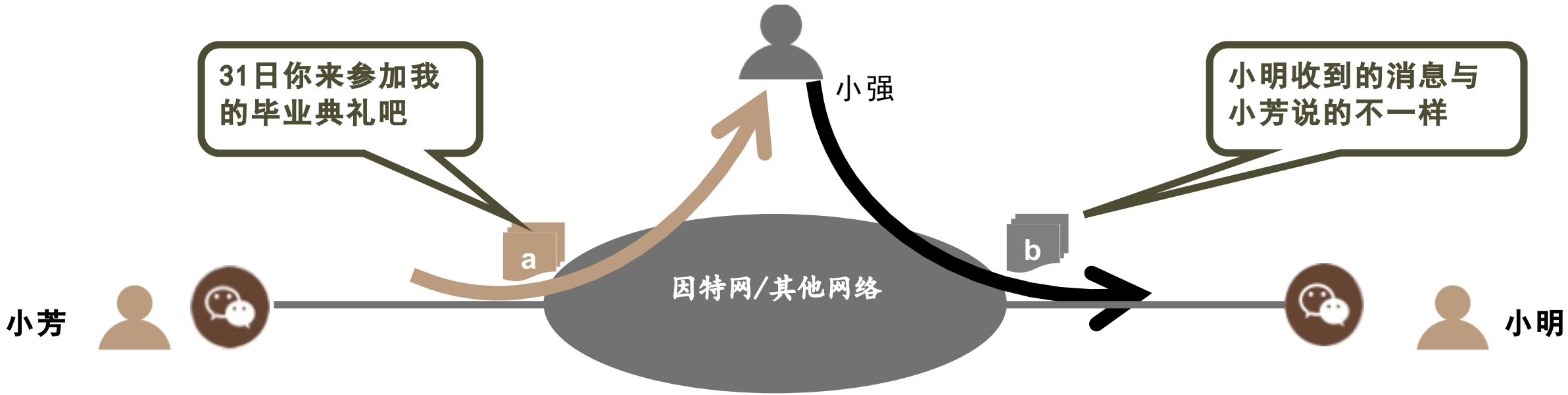
数字摘要概述

消息的完整性

完整性：发送者和接收者必须确信他们的通信内容在过程中没有被恶意或者偶然修改。

完整性要求

确保消息没有在传输途中被篡改。



数字摘要基本思想

数字摘要（message digest）：以单向散列函数思想为基础，功能是只认证消息但不保密。

单向散列函数：接受一个任意长度的明文作为输入，根据此明文计算出一个固定长度的位串。

消息摘要特性

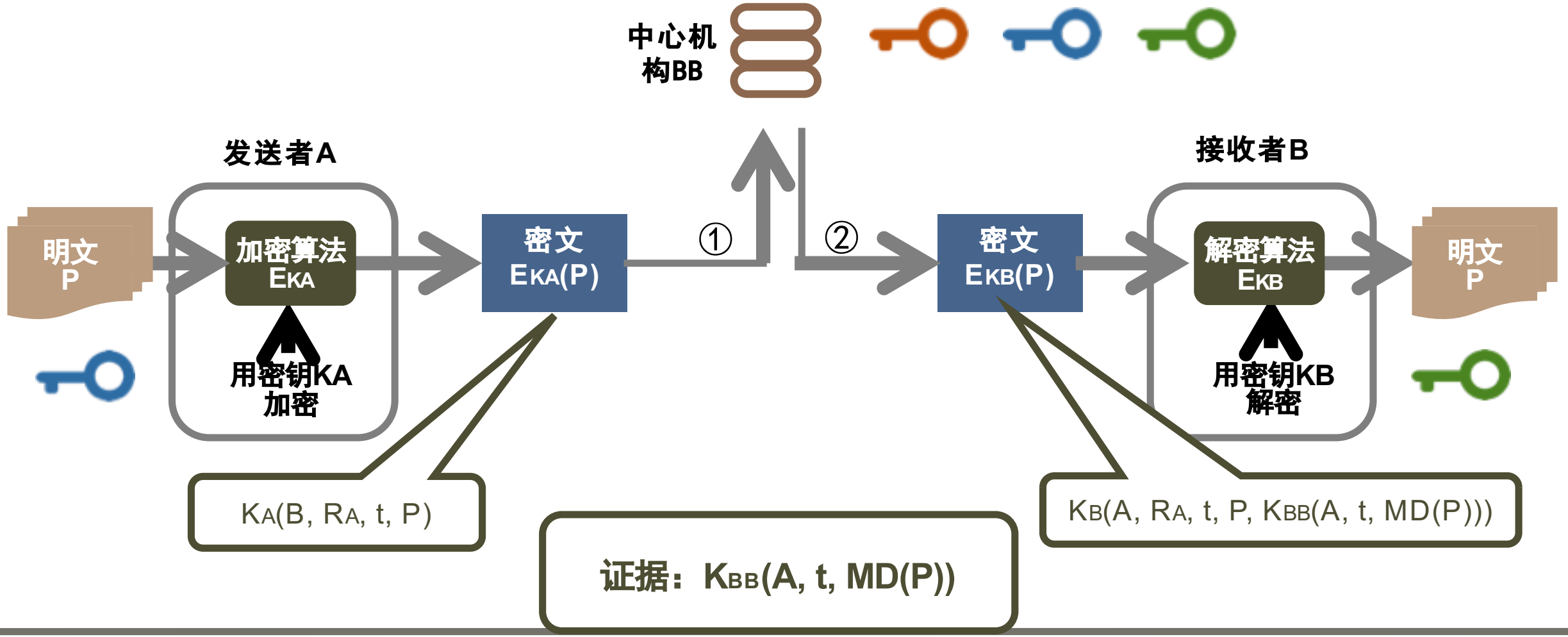
- 给定P，很容易计算MD(P)
- 给定MD（P），想有效找到P是不可能的
- 给定P，无法找到满足MD (P') = MD(P)的P'
- 输入明文即使只有1位变化，也会导致完全不同的输出

- 用消息摘要来验证消息的完整性
- 用消息摘要来验证消息的数字签名

从一段明文计算出一个消息摘要比用公开密钥算法来加密这段明文快得多

MD： message digest

数字摘要在对称密钥数字签字中的应用



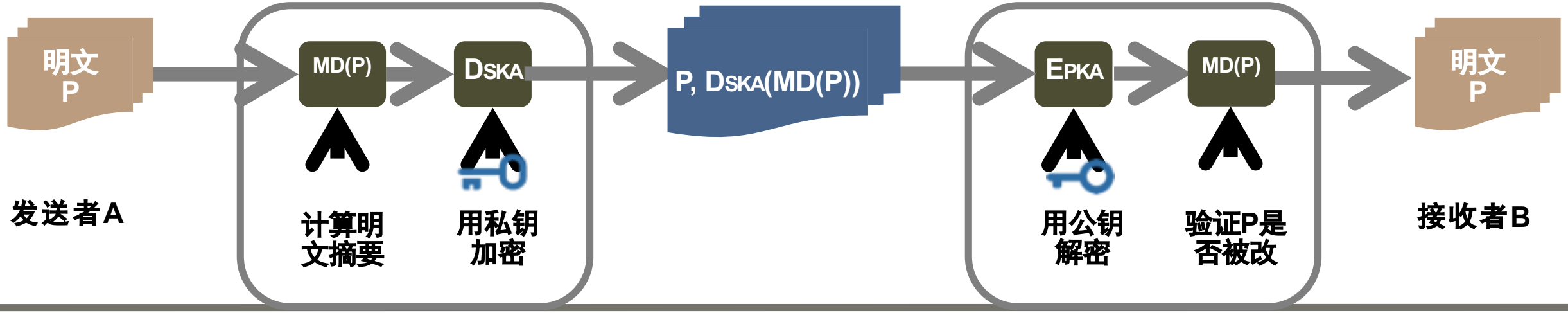
BB的密钥K_{BB}　B的密钥K_B　A的密钥K_A

数字摘要在公开密钥数字签名中的应用

如果有人篡改了P，收到明文为P'，那么

$$MD(P') != MD(P)$$

- 发送者计算明文P的消息摘要MD(P)
- 发送者用私钥加密消息摘要
- 接收者用公钥获得消息摘要
- 对收到的明文P计算消息摘要，比较上述解密的摘要以此验证P是否被篡改过



A公钥PKA　A私钥SKA　B公钥PKB　B私钥SKB