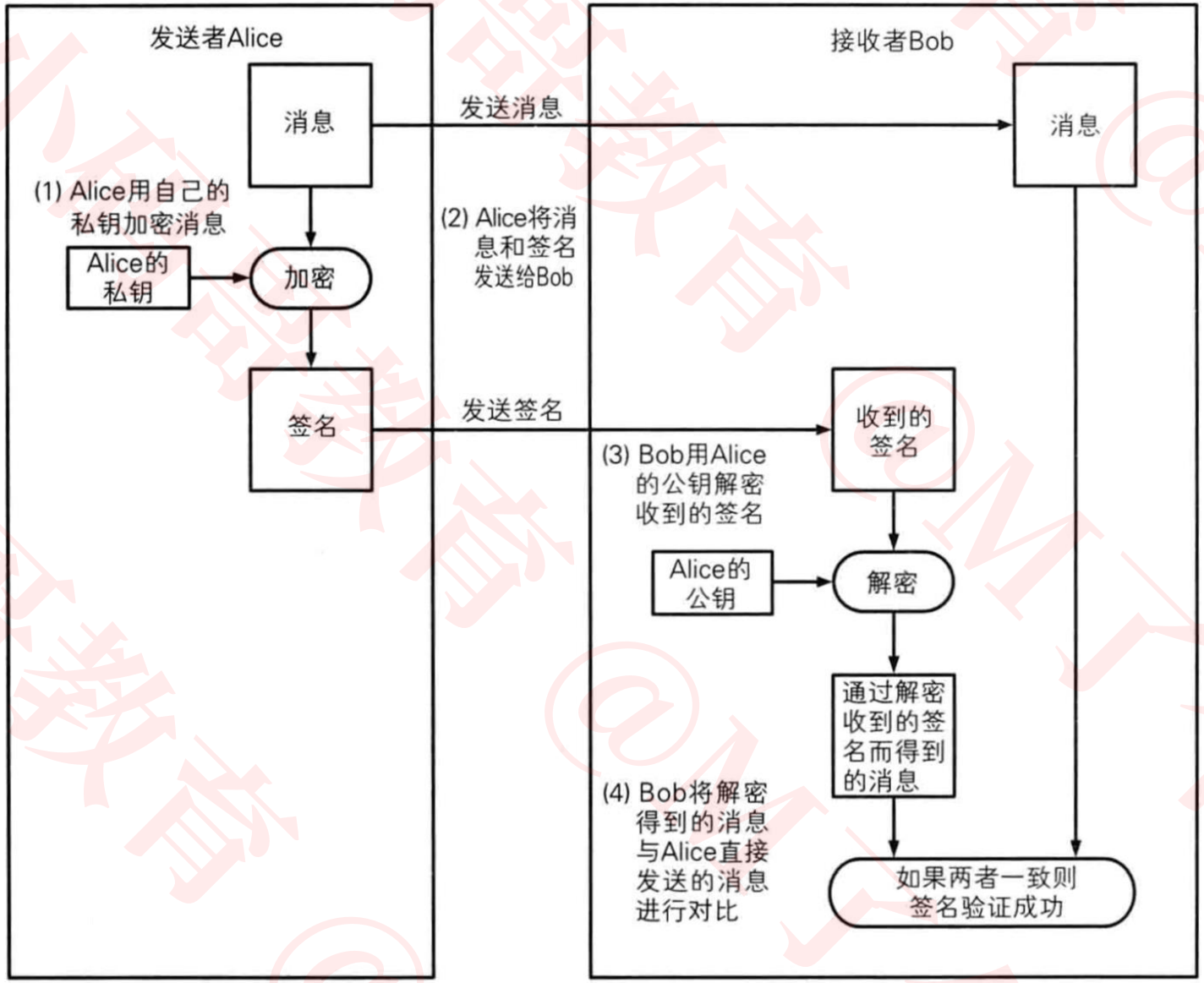
想象以下场景

- Alice发的内容有可能是被篡改的，或者有人伪装成Alice发消息，或者就是Alice发的，但她可以否认
- 问题来了：Bob如何确定这段消息的真实性？如何识别篡改、伪装、否认？
- 解决方案
  - 数字签名

数字签名

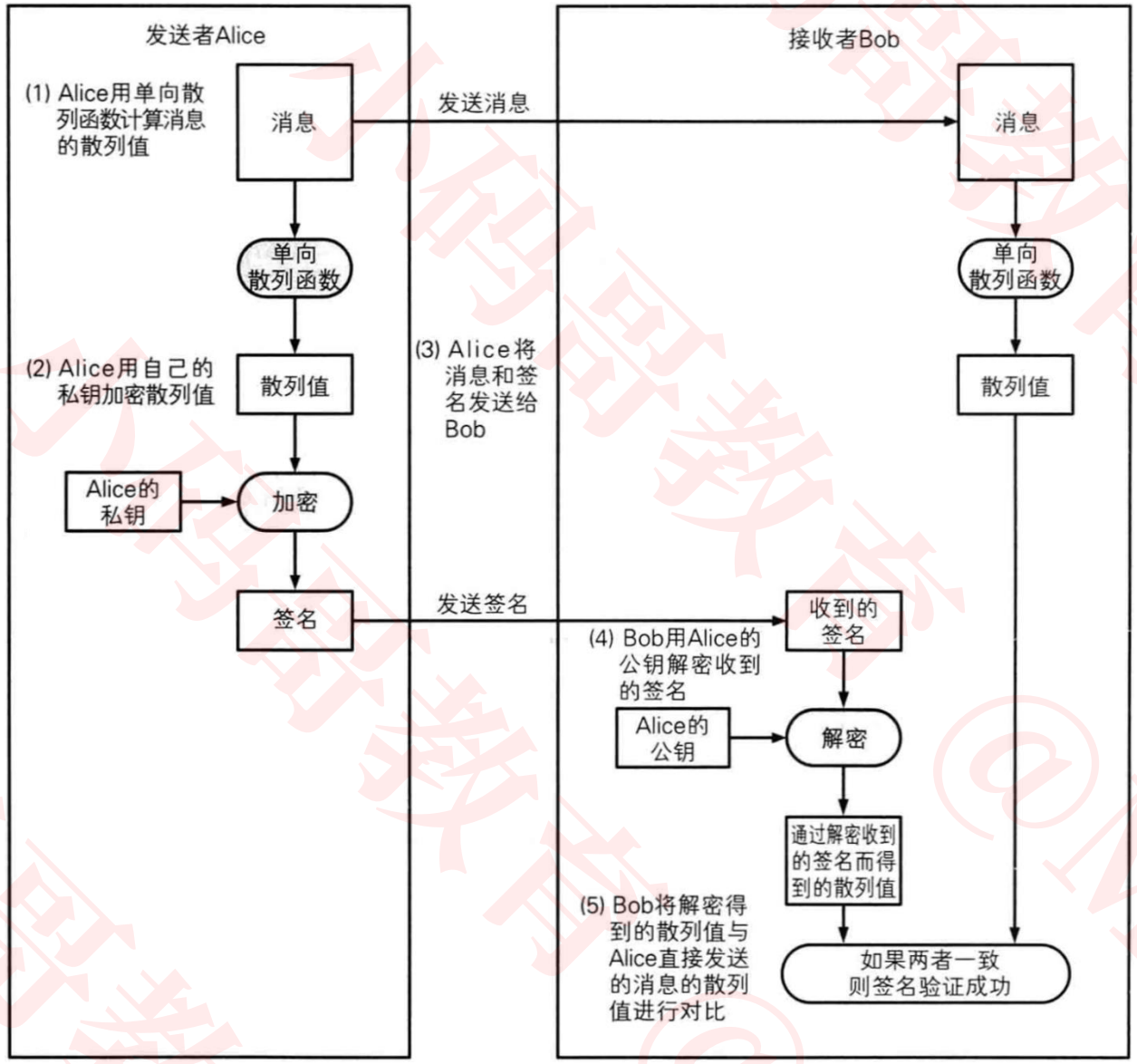
- 在数字签名技术中，有以下2种行为
  - 生成签名
    - ✓ 由消息的发送者完成，通过“签名密钥”生成
  - 验证签名
    - ✓ 由消息的接收者完成，通过“验证密钥”验证
- 如何能保证这个签名是消息发送者自己签的?
  - 用消息发送者的私钥进行签名

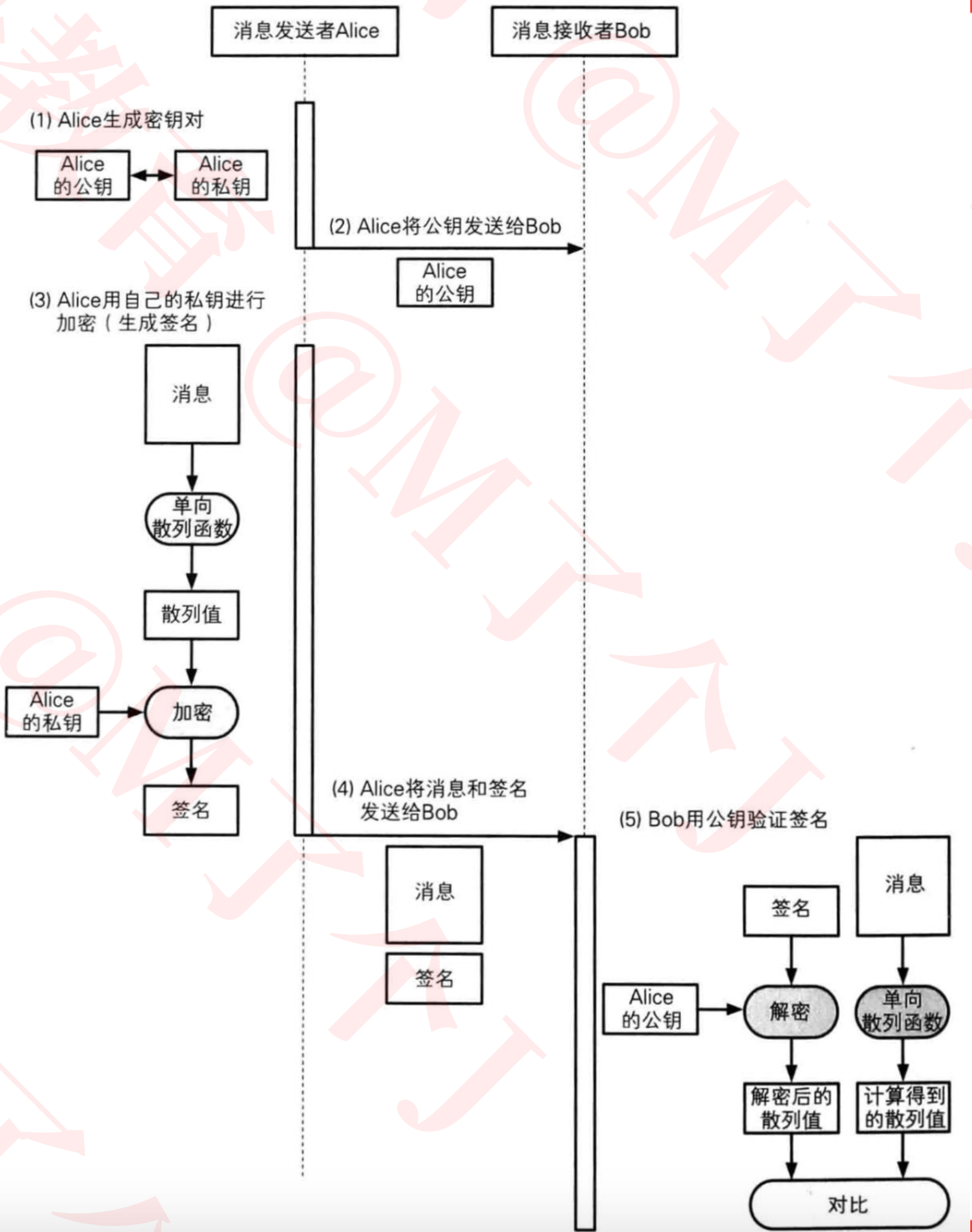
数字签名 – 过程


发送者Alice
消息
(1) Alice用自己的私钥加密消息
Alice的私钥
加密
签名
发送消息
(2) Alice将消息和签名发送给Bob
发送签名
接收者Bob
消息
收到的签名
(3) Bob用Alice的公钥解密收到的签名
Alice的公钥
解密
通过解密收到的签名而得到的消息
(4) Bob将解密得到的消息与Alice直接发送的消息进行对比
如果两者一致则签名验证成功

小码哥教育 SEEMYGO

数字签名 - 过程改进





数字签名 – 疑惑

- 如果有人篡改了消息内容或签名内容，会是什么结果?
  - 签名验证失败，证明内容被篡改了

- 数字签名不能保证机密性?
  - 数字签名的作用不是为了保证机密性，仅仅是为了能够识别内容有没有被篡改

- 数字签名的作用
  - 确认消息的完整性
  - 识别消息是否被篡改
  - 防止消息发送人否认