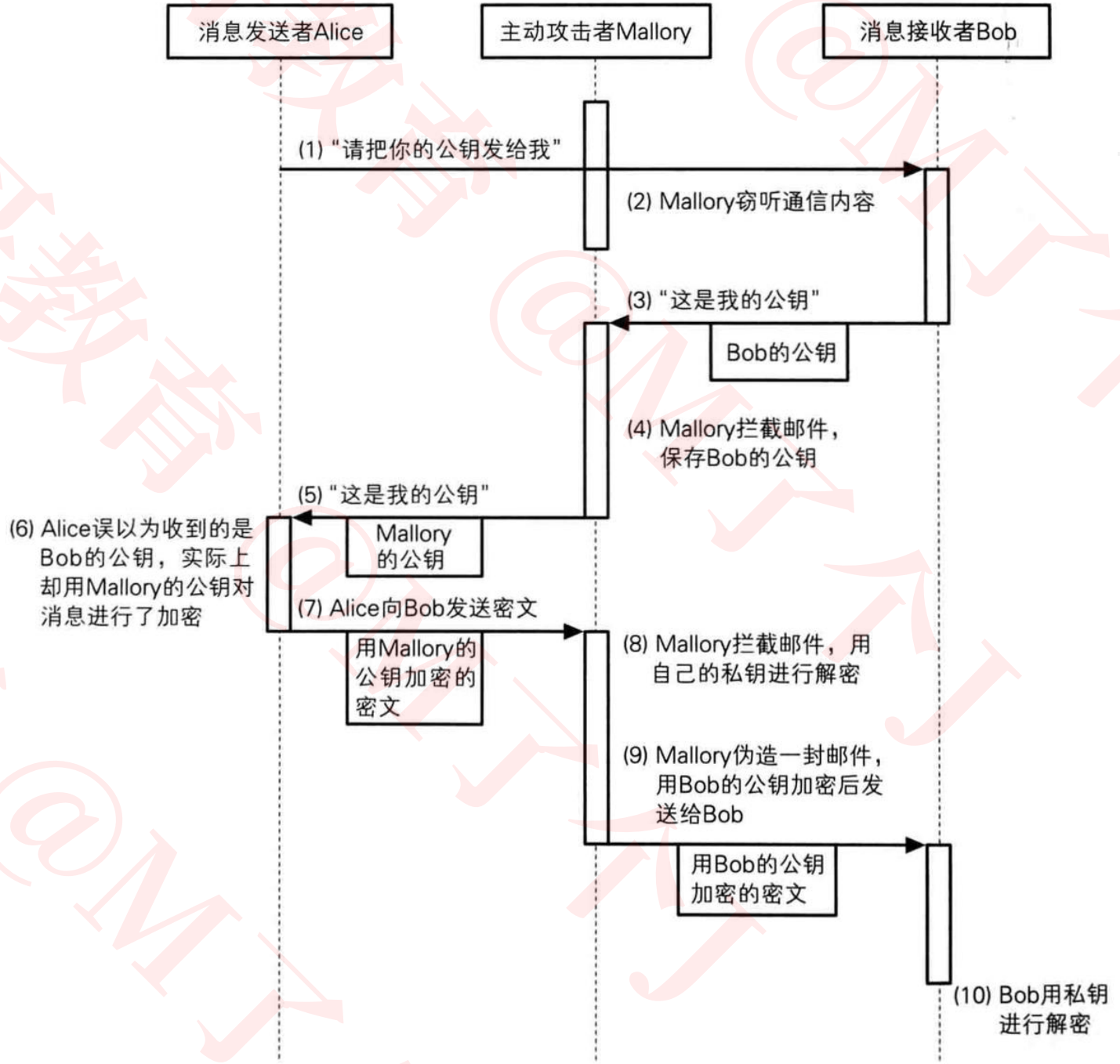
公钥的合法性

- 如果遭遇了中间人攻击，那么
  - 公钥将可能是伪造的

- 如何验证公钥的合法性?
  - 证书



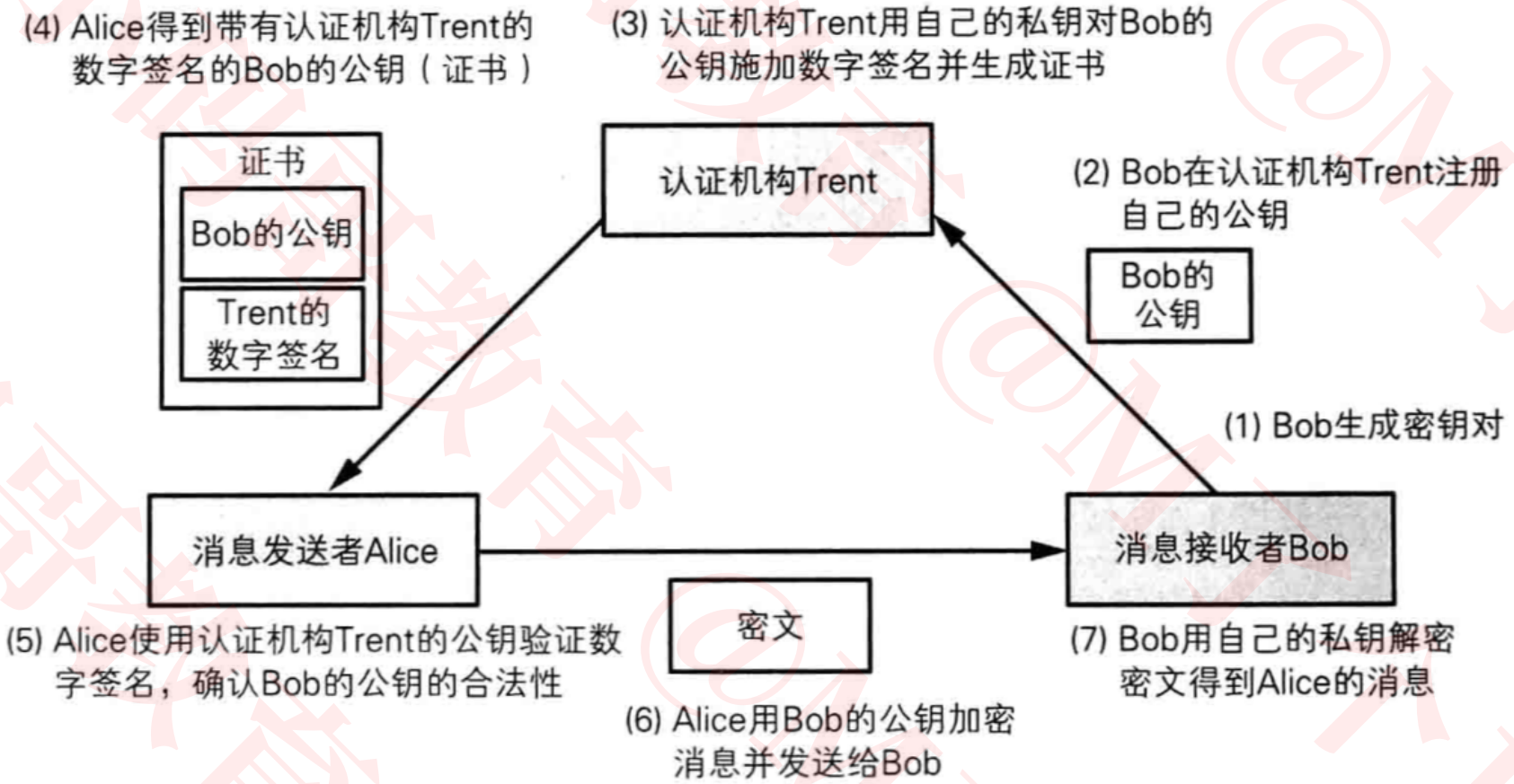
证书（Certificate）

- 说到证书
  - 首先联想到的是驾驶证、毕业证、英语四六级证等等，都是由权威机构认证的

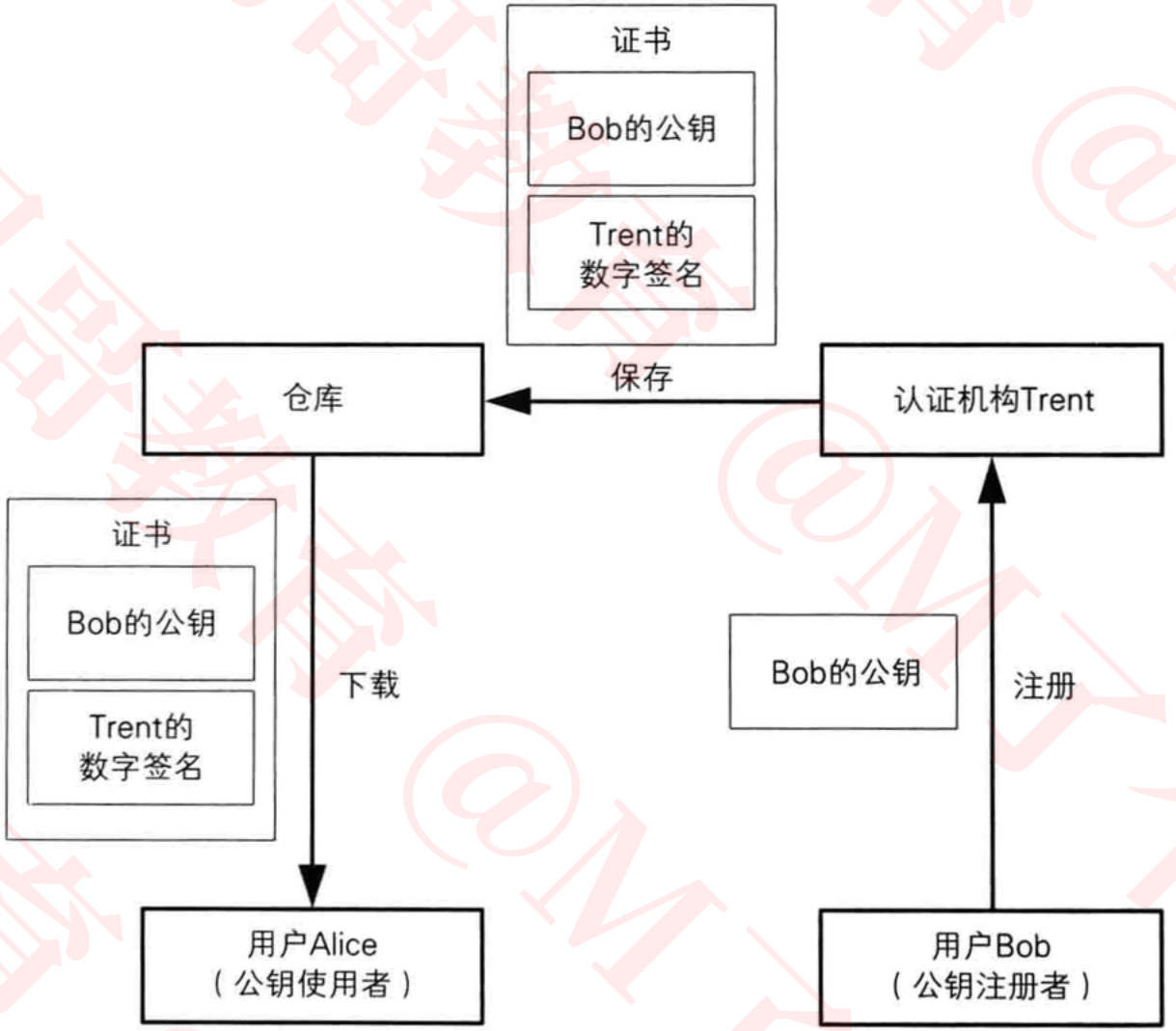
- 密码学中的证书，全称叫**公钥证书**（Public-key Certificate，PKC），跟驾驶证类似
  - 里面有姓名、邮箱等个人信息，以及此人的公钥
  - 并由认证机构（Certificate Authority，CA）施加数字签名

- CA就是能够认定“公钥确实属于此人”并能够生成数字签名的个人或者组织
  - 有国际性组织、政府设立的组织
  - 有通过提供认证服务来盈利的企业
  - 个人也可以成立认证机构

证书 – 使用


(4) Alice得到带有认证机构Trent的数字签名的Bob的公钥（证书）
(3) 认证机构Trent用自己的私钥对Bob的公钥施加数字签名并生成证书
证书
Bob的公钥
Trent的数字签名
认证机构Trent
(2) Bob在认证机构Trent注册自己的公钥
Bob的公钥
(1) Bob生成密钥对
消息发送者Alice
消息接收者Bob
密文
(5) Alice使用认证机构Trent的公钥验证数字签名，确认Bob的公钥的合法性
(6) Alice用Bob的公钥加密消息并发送给Bob
(7) Bob用自己的私钥解密密文得到Alice的消息

证书 – 注册和下载


证书
Bob的公钥
Trent的
数字签名
仓库
保存
认证机构Trent
证书
Bob的公钥
Trent的
数字签名
下载
Bob的公钥
注册
用户Alice
（公钥使用者）
用户Bob
（公钥注册者）

证书 – 查看Windows已经信任的证书

① Windows键 + R >>> 输入**mmc**

② 文件 >>> 添加/删除管理单元

③ 证书 >>> 添加 >>> 我的用户账户 >>> 完成 >>> 确定