## HTTPS

购买数字证书, 存储在服务器上

Client

验证数字证书真实性

验证通过, 取出公匙

本地生成随机数

用公匙加密随机数

生成会话私匙

请求数字证书(包含公匙)

返回数字证书(包含公匙)

不怕窃取,因为中间 人没有解密私匙,读 不出会话私匙(随机 数)

会话私匙回传服务器

服务器与客户端建立连接

未来通信用会话私匙加密

Server

拿到会话私匙

用CA处购买的私匙解 密会话私匙

非对称加密连接建立完 成

安全隐患-中间人攻击

请求数字证书时被拦截 攻击者向Client传回自己的假证书 欺骗用户信任了这个证书 客户端验证通过假证书

虚拟中间人通信成立,存在安全隐患

解决方法:客户端直接绑定公匙,公匙存储在客户端本地

客户端收到公匙以后与存储在本地的公匙进行校验,防虚假证书