

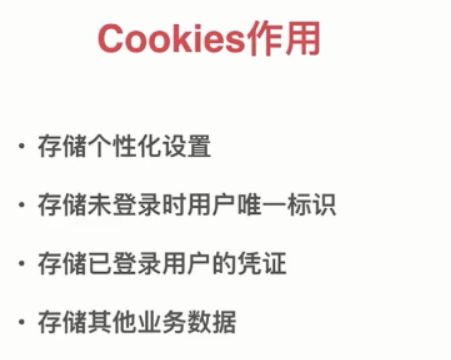
Cookies 存储在前端，后端可以通过http头来设置cookie, js也可以取得cookie,设置cookie

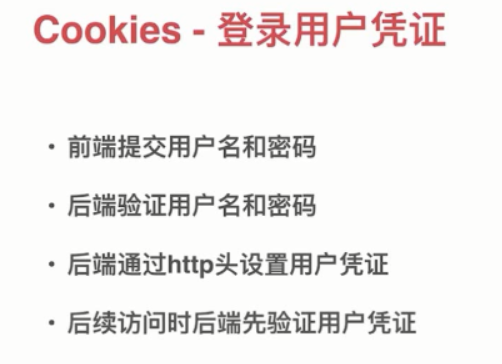
在站内都会带上cookie, 也有可能是在缓存中拿的

用户登录成功后后，会带上cookie



Cookie 没有删除方法，也是通过设置，失效时间为过去时间；





直接用用户id会有巨大的隐患，，可能是别人的id

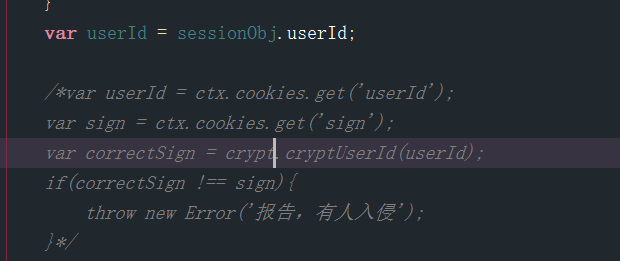




这个签名只能自己算出来，可以用node de crypto



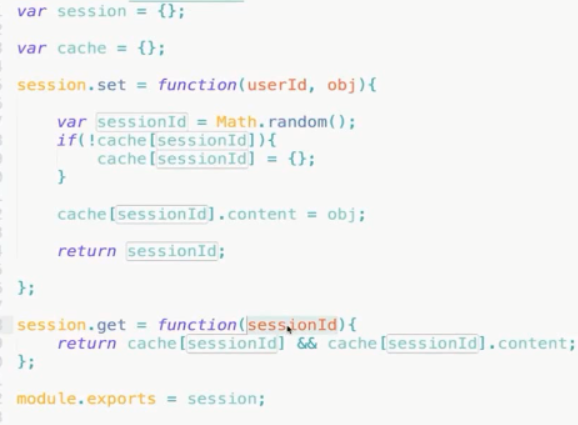
签名是不可逆的， userId +签名， 要把用户Id 暴露到后端，在计算一下，进行比较；



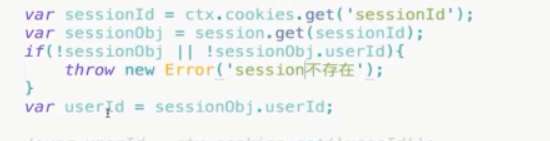
由后台提供私钥，别人不知道的

Cookie 中是没有真实信息的， 不存用户数据

可以用sessionId（随机数）, 登陆成功派发一个sessionID,这个和验证码原理相同







Session是放在内存中的，改变要重启，后端重启时，session会丢失，

生产环境一般不放在内存中， session 一般放在外村中，这样一方面是放在内存中，多台服务器的session 不同步，用户会感觉有点调，一会登陆，一会不登陆，而在外存中可以保证是同步，同时当访问量大时，session放在内存中，扛不住。