第15讲讲HTTPS协议：点外卖的过程原来这么复杂

对称加密，加密和解密的秘钥是相同的。

非对称加密一个是公开的公钥，另外一个是自己私有的私钥，公钥加密的信息，只有私钥才能解密。私钥加密的信息，只有公钥才能解密。

对称加密比非对称加密效率高，但是还是有被截取的风险

非对称加密需要通过证书和权威机构来验证公钥的合法性

HTTPS是综合了对称加密和非对称加密算法的HTTP协议，既保证了传输安全，也保证了传输效率。

权威机构是CA(Certificate Authority)，证书内容包括证书所有者，公钥，发布机构，有效期。

Ssl里面，会发送加密方式，压缩方式，解密方式，hash信息，一个随机数。

因此对网址的连接得到的是一个证书，通过拿到CA的公钥解密外卖网站的签名，hash也正确，就没有问题。