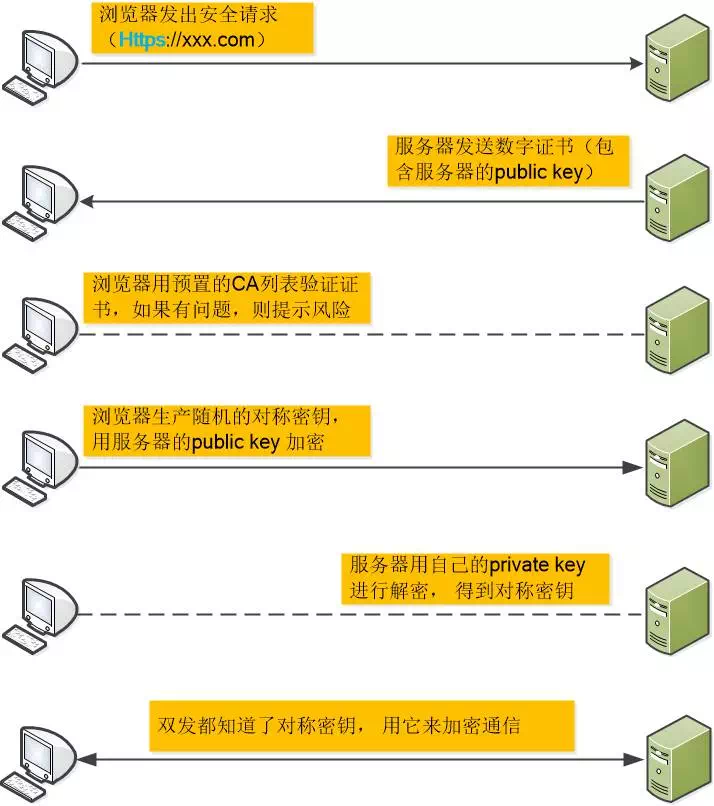
————————————————https————————————————————



https的ssl与tls的安全层协议位于应用层与传输层之间。

服务器有有两个私钥，ca的私钥和自己的私钥。

第二步中，服务器传输公钥会根据ca证书的私钥进行加密生成签名和自己的公钥一起传输给浏览器，浏览器根据内置的顶层ca证书做校验。