HTTPS协议详解

# 文档总述

也算接触了一些有关于https方面的项目，一直想抽个时间把这块的内容记录一下，希望赶紧梳理一下。

以下所有内容都仅仅只是个人见解。

想要比较全面了解https，需要从下面3个方面来了解：

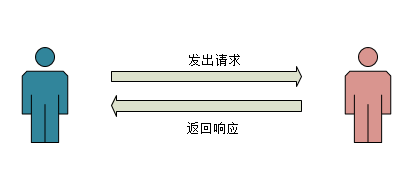
* https出现的背景、https在网络层的位置、https最终通过什么样的方案解决了什么样的难题。
* http详解，包括https整个调用过程，以及涉及的所有知识点的了解，特别是证书相关的。
* https实战：了解得再多，我们还得知道，应该怎么使用呀。如何使用已有的框架发布以及调用https服务，其中包括发布单向或者双向认证的服务，调用单向或者双向的服务或者跳过证书认证。

以下解释的过程中，大致出个3个人物，小胖---客户端，璐璐---服务器，小三---恶意攻击者。小胖如何与小三斗智斗勇与璐璐交流。

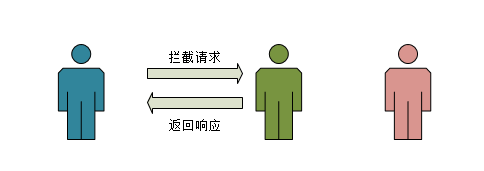
# 基本背景

## 通信被拦截

有一天，小胖想给璐璐发一条消息，正常的过程如下图所示：

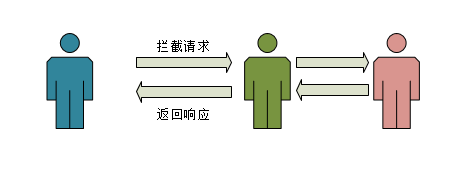


可是不知道来了一个小三，把我发出的请求给拦截了，并且以璐璐的口吻给我做出了响应，把我臭骂了一顿，害我伤心难过好几天，后来才知道被别人给篡改了，如下图所示：



是的，小三是绿色的。。。

当然，还有另外一种情况，他既然能拦截请求，也可以看到我的消息，那么他以我的口吻再说一些坏话发给璐璐，即篡改我的信息，显然璐璐看到后肯定会大发雷霆，我吃不到好果子，如下图：



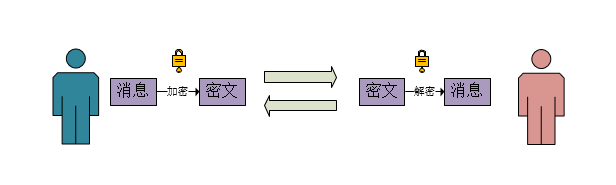
所以，这里面有两个问题：

* 我发出去的消息，不想被别人看到。
* 正在和我通话的人，必须是璐璐，不能是别人，而且我也可以确认这一点。

## 问题怎么解决

### 先加个密吧

先说第一个问题，最简单的方式就是对称加密，密钥只有一个，既可以使用密钥对消息进行加密，也能够使用密钥对密文进行解密，如下图所示



那么问题又来了，密钥怎么给璐璐？肯定不能在网络上传输呀，密钥万一被盗取了，那岂不是完蛋了。那我只能见面的时候，偷偷地给璐璐了，这样可保我们后续所有的通话都安全进行。

这样进行了一段时间，没想到又有新的问题了。

### 我太花心了

也不能老是和一个女生聊天呀，不得同时撩很多妹纸呀，但是这个密钥传递的话，好像不是特别方便呀，我不能每个人去见个面偷偷给一次密钥呀，这样我也没有时间啊。

然后出现了一种叫做非对称加密（RSA）的方式，每一个人都有两把钥匙，一个叫做私钥，一个叫做公钥，两个对应起来。私钥加密的密文，只有公钥才能解。同理，公钥加密的密文，只有私钥才能解开。但是私钥是自己的，不能给任何人看，公钥是公开的，大家都可以使用，如下图所示：

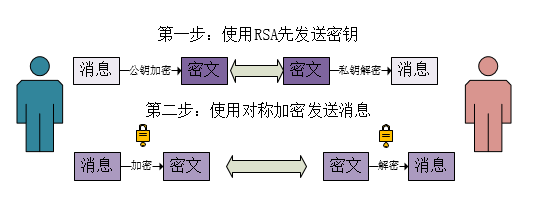


这样我就可以拿着妹纸的公钥给妹纸发消息了，反正只有她才能解。

那为啥不是我拿着自己的私钥发消息呢？我作为请求者，如果用我的私钥加密，那么任何可以拦截我消息的人都可以用我的公钥进行解密。

那么RSA真的这么好用吗？虽然它很强大，私钥加密的，仅仅只有这个私钥对应的公钥才能解。但是它的缺点也特别明显，就是加密解密实在太慢了，让人受不了。

对了，我们为什么抛弃了对称加密？就是因为加密的密钥传递太麻烦了，必须见面亲自给而不能网络传输，那现在不是可以使用RSA吗？那我们就先使用RSA来传递我们的密钥，之后我们就一直用密钥来交流，这样岂不是既安全又快，美滋滋呀。如下图所示：



难道这样就完美了吗？似乎还不行。

### 璐璐到底是谁

我用璐璐的公钥去加密，那这个公钥一定就是璐璐的吗？璐璐是怎么发给我的，肯定是在网络上的啊，只要在网络上面发，那肯定有可能被篡改。万一璐璐在发的过程中，被小三拦截了，小三把他自己的公钥给我了，我还是以为是璐璐的。结果用小三的公钥给璐璐发消息，被小三拦截，小三再用自己的私钥解密，篡改，再使用璐璐的公钥加密，璐璐收到消息后就可以用自己的私钥解密，看到信件内容了。这样我们之间的通信也被小三给看见了。也就是说还得有一种办法来证明我拿到的公钥是我以为的公钥，即证明她是她。

这个例子在生活中太多了，比如办个什么事情，一般都要出具“我是我”、“我妈是我妈”的证明，我们也没有办法，必须在一些权威机构或者公证处，出具一些我的个人证件等等，让他们认可我，然后再开具证明。

公钥也是一样，我得给公证处出具一些信息来证明我的身份，这样他们认可以后，给我盖个章，说明一下这个公钥就是谁的公钥，开个证明即可。