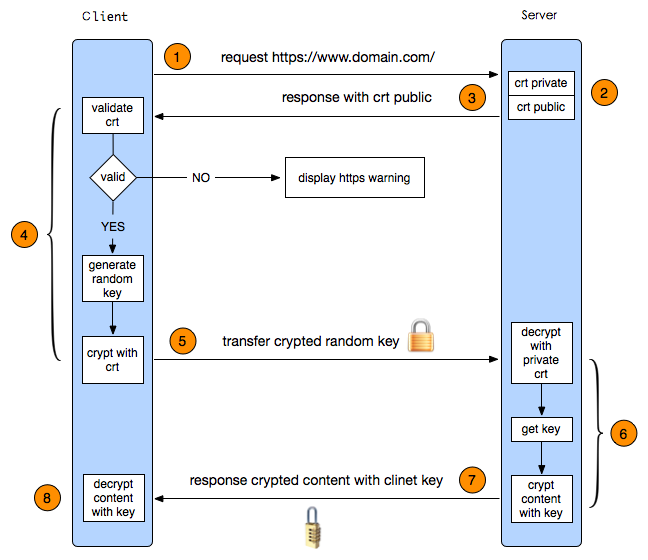
<https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html>

# [图解HTTPS](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html)

我们都知道HTTPS能够加密信息，以免敏感信息被第三方获取。所以很多银行网站或电子邮箱等等安全级别较高的服务都会采用HTTPS协议。

### HTTPS简介

HTTPS其实是有两部分组成：HTTP + SSL / TLS，也就是在HTTP上又加了一层处理加密信息的模块。服务端和客户端的信息传输都会通过TLS进行加密，所以传输的数据都是加密后的数据。具体是如何进行加密，解密，验证的，且看下图。



### 1. 客户端发起HTTPS请求

这个没什么好说的，就是用户在浏览器里输入一个https网址，然后连接到server的443端口。

### 2. 服务端的配置

采用HTTPS协议的服务器必须要有一套数字证书，可以自己制作，也可以向组织申请。区别就是自己颁发的证书需要客户端验证通过，才可以继续访问，而使用受信任的公司申请的证书则不会弹出提示页面(startssl就是个不错的选择，有1年的免费服务)。这套证书其实就是一对公钥和私钥。如果对公钥和私钥不太理解，可以想象成一把钥匙和一个锁头，只是全世界只有你一个人有这把钥匙，你可以把锁头给别人，别人可以用这个锁把重要的东西锁起来，然后发给你，因为只有你一个人有这把钥匙，所以只有你才能看到被这把锁锁起来的东西。

### 3. 传送证书

这个证书其实就是公钥，只是包含了很多信息，如证书的颁发机构，过期时间等等。

### 4. 客户端解析证书

这部分工作是有客户端的TLS来完成的，首先会验证公钥是否有效，比如颁发机构，过期时间等等，如果发现异常，则会弹出一个警告框，提示证书存在问题。如果证书没有问题，那么就生成一个随即值。然后用证书对该随机值进行加密。就好像上面说的，把随机值用锁头锁起来，这样除非有钥匙，不然看不到被锁住的内容。

### 5. 传送加密信息

这部分传送的是用证书加密后的随机值，目的就是让服务端得到这个随机值，以后客户端和服务端的通信就可以通过这个随机值来进行加密解密了。

### 6. 服务段解密信息

服务端用私钥解密后，得到了客户端传过来的随机值(私钥)，然后把内容通过该值进行对称加密。所谓对称加密就是，将信息和私钥通过某种算法混合在一起，这样除非知道私钥，不然无法获取内容，而正好客户端和服务端都知道这个私钥，所以只要加密算法够彪悍，私钥够复杂，数据就够安全。

### 7. 传输加密后的信息

这部分信息是服务段用私钥加密后的信息，可以在客户端被还原

### 8. 客户端解密信息

客户端用之前生成的私钥解密服务段传过来的信息，于是获取了解密后的内容。整个过程第三方即使监听到了数据，也束手无策。

（全文完）

[#1楼](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html#2566483) 2012-11-29 18:24 [五子登科](https://www.cnblogs.com/minzhuhu/) 

请教楼主，如果客户端要发送内容给服务端是怎么加密的，也是通过第5步中的随机值进行加密的？

[支持(0)反对(0)](javascript:void(0);)

[#2楼](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html#2567738) 2012-11-30 23:52 [lovebanyi](https://www.cnblogs.com/lovebanyi/) 

监听到确实是没有问题，但是如果处在路由端可以修改数据的就有风险了，  
  
这个风险在于验证证书的有效性哪边。 根证书的哪些人就可以搞定这个了。还有一些网站证书本身就是非法的，网站必弹哪个。在客户端请求证书的时候发一个假的证书给它，然后自己向服务端请求证书。 把自己当成代理就行了。

[支持(3)反对(0)](javascript:void(0);)

[#3楼](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html#2927545) 2014-04-29 10:11 [twlkyao](https://www.cnblogs.com/twlkyao/) 

[@](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html#2567738) lovebanyi  
代理的话也许要有证书，并且可以得到客户端的认证，就像Fiddler一样。

[支持(0)反对(0)](javascript:void(0);)

[#4楼](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html#2927755) 2014-04-29 14:04 [echozhao](http://home.cnblogs.com/u/406904/) 

请问博主这个图用什么工具绘制的？

[支持(0)反对(0)](javascript:void(0);)

[#5楼](https://www.cnblogs.com/zhuqil/archive/2012/07/23/2604572.html#3249517) 2015-08-18 10:12 [生命潦草](https://www.cnblogs.com/cyc_aspx/) 

443 解密之后是不是要转发到80端口？