**HTTPS和HTTP的区别主要如下：**

**1、https协议需要到ca申请证书，一般免费证书较少，因而需要一定费用。**

**2、http是超文本传输协议，信息是明文传输，https则是具有安全性的ssl加密传输协议。**

**3、http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。**

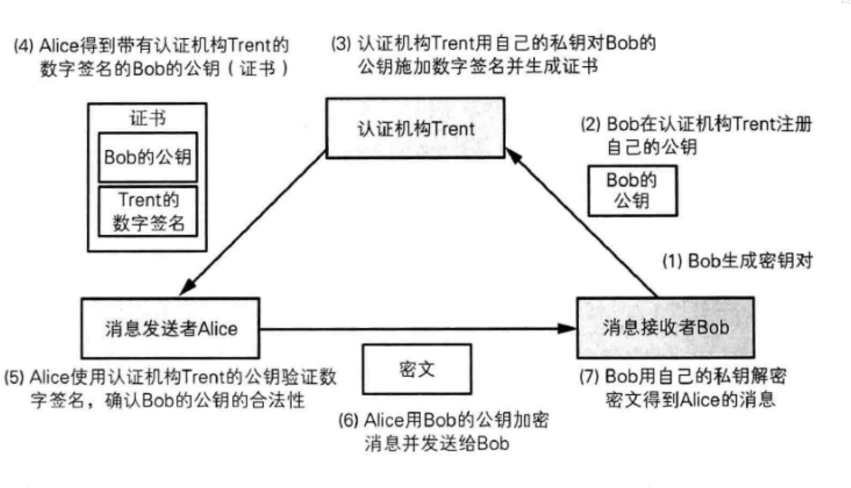
**4、http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全。**

**加密方法：**

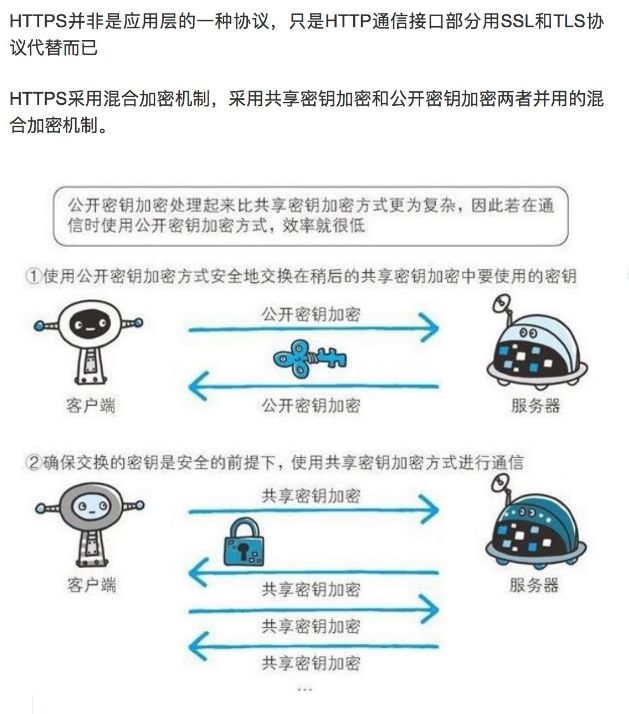
* **对称加密：加密解密用的是同样的“钥匙”**
* **非对称加密：加密解密用的是不同的“钥匙”**

**Https：http over ssl（secure socket layer）采用非对称加密，等于在http和tcp之间嵌入了ssl层**

**优势：相对安全、搜索排名高**

**缺点：**

* **HTTPS协议握手阶段比较费时，会使页面的加载时间延长近50%，增加10%到20%的耗电；**
* **HTTPS连接缓存不如HTTP高效，会增加数据开销和功耗，甚至已有的安全措施也会因此而受到影响；**
* **SSL证书需要钱，功能越强大的证书费用越高，个人网站、小网站没有必要一般不会用。**
* **SSL证书通常需要绑定IP，不能在同一IP上绑定多个域名，IPv4资源不可能支撑这个消耗。**
* **HTTPS协议的加密范围也比较有限，在黑客攻击、拒绝服务攻击、服务器劫持等方面几乎起不到什么作用。最关键的，SSL证书的信用链体系并不安全，特别是在某些国家可以控制CA根证书的情况下，中间人攻击一样可行**

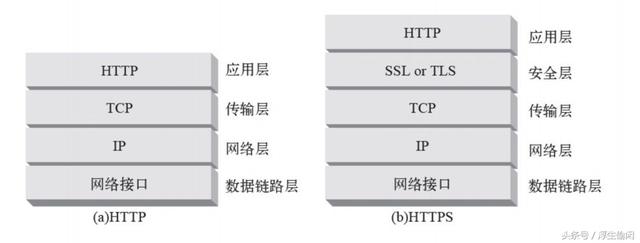


https其实就是建构在SSL/TLS之上的 http协议，所以https比http要占用更多的资源 http使用TCP 三次握手建立连接，客户端和服务器需要交换3个包，https除了 TCP 的三个包，还要加上 ssl握手需要的9个包，所以一共是12个包。HTTPS就是在安全的传输层上发送的HTTP。浏览器收到公钥后会对公钥进行一系列的验证，如：颁发机构，过期时间等等。认证失败会有警告，比如上面说的我们自己生成的证书，不是授信组织办法。成功的话，会生成一个随机值作为对称加密的密钥稍后还会提及到。

https其实就是建构在SSL/TLS之上的 http协议，所以https比http要占用更多的资源

http使用TCP 三次握手建立连接，客户端和服务器需要交换3个包，https除了 TCP 的三个包，还要加上 ssl握手需要的9个包，所以一共是12个包。

HTTPS就是在安全的传输层上发送的HTTP。HTTPS没有将未加密的HTTP报文发送给TCP它在将HTTP报文发送给TCP之前，先将其发送给了一个安全层，对其进行加密如图：



过程简述

* 1.客户端发起HTTPS请求
* 2.服务器将公钥返回给客户端
* 3.浏览器接收到服务器公钥

浏览器收到公钥后会对公钥进行一系列的验证，如：颁发机构，过期时间等等。认证失败会有警告，比如上面说的我们自己生成的证书，不是授信组织办法。成功的话，会生成一个随机值作为对称加密的密钥稍后还会提及到。用服务器返回的公钥对这个随机值进行加密

* 4.加密后的随机值发送到服务器
* 5.客户端与服务器进行加密通信

客户端和服务器端信息数据通信，就是秘钥为随机值的，对称加密了

|  |
| --- |
| 图解 HTTPS 通信过程 |
|  |
|  |
| 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。  http://cdn.liqwei.com/upload/www/201211/20121130144420002.png  **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。，把自身支持的一系列Cipher Suite（密钥算法套件，简称Cipher）发送给服务端  **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。**  **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，那么就生成一个随机值。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随机值(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。 |

非对称加密算法：RSA，DSA/DSS     在客户端与服务端相互验证的过程中用的是非对称加密   
对称加密算法：AES，RC4，3DES     客户端与服务端相互验证通过后，以随机数作为密钥时，就是对称加密  
HASH算法：MD5，SHA1，SHA256  在确认握手消息没有被篡改时