https://www.cnblogs.com/f-ck-need-u/p/6089523.html

HTTP是应用层协议，基于TCP/IP

HTTPS即Secure HTTP， HTTP安全版本。实现是在HTTP和TCP之间加了一层加密层: TLS/SSL

**何为TLS/SSL ？**

SSL是个加密套件，负责对HTTP的数据进行加密。TLS是SSL的升级版。现在提到HTTPS，加密套件基本指的是TLS。

**传输加密的流程**

原先是应用层将数据直接给到TCP进行传输，现在改成应用层将数据给到TLS/SSL，将数据加密后，再给到TCP进行传输。

常见加密方式：

对称加密：加密解密的钥匙都是一样的。也就是说，两两通信的双方都需要一把钥匙，那n个人通信，需求量巨大问题。但是加密解密效率高些。

非对称加密：用公钥加密，用私钥解密 。（其实只要是一对公钥，私钥，无论用公还是用私加密，都可以用另一把解密。根绝需要。）

举个例子：

小明要访问某大型同性社交网站，将自己的隐私提交，浏览器通过网站的公钥加密，发送数据到这个网站，这样加密了数据，安全。

网站收到后，用自己的私钥，解密，得到数据。

看起来安全，但是如果拿网站的公钥这个公钥过程被黑了，拿到伪造的公钥，怎么办？

解决：

如果公钥在一个一定公正合法的地方拿，就安全了。

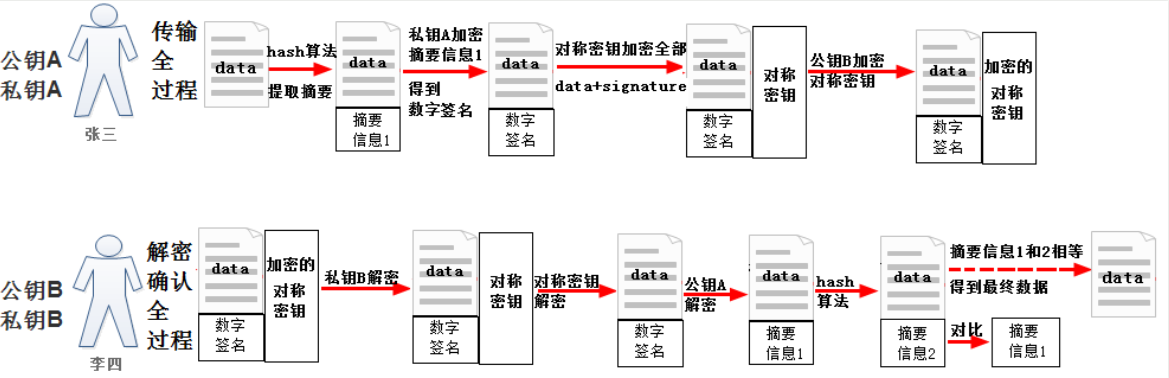
所以，需要一个公认的安全合法的中介：CA，信任中心，意思是公钥都在这拿，但是要来拿，你就要拿这个浏览器在我这注册过的证书，这个证书OK，我才给你。

CA最基本的条件就是：信任，必须默认允许CA是公平公开合法的，大家都放心的，不然CA都不让人放心，非对称就没有什么意义了，变成对称，互相持有对方公钥。

公钥是正确的，加密后安全，发送后仅浏览器能解密，安全。HTTPS安全。

**下面是https使用ssl加密机制的握手通信过程**。

https://www.cnblogs.com/f-ck-need-u/p/6089523.html



TLC/SSL 便是基于非对称加密，更多详细而深入的密码学知识，请参考度娘。