https协议实际上就是包裹了ssl的http，有一个公式 http+加密+认证+完整性保护 = https

https是采用 非对称加密+对称加密相结合的方式 来进行加密，过程如下：

（1）服务器拥有一个公钥A，一个私钥B

（2）浏览器向服务器发起请求，服务器就把公钥A明文传输给浏览器

（3）浏览器拿到公钥A后，随机生成一密钥X，然后用公钥A进行加密传输给服务器

（4）服务器拿到后，用私钥B进行解密得到密钥X

（5）这时候浏览器和服务器手头上都有密钥X，之后就会用这个密钥X来进行对称性加解密