超文本传输协议HTTP协议被用于在Web浏览器和网站服务器之间传递信息，HTTP协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了Web浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此，HTTP协议不适合传输一些敏感信息，比如：信用卡号、密码等支付信息。

为了解决HTTP协议的这一缺陷，需要使用另一种协议：安全套接字层超文本传输协议HTTPS，为了数据传输的安全，HTTPS在HTTP的基础上加入了SSL/TLS协议，SSL/TLS依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

HTTPS协议是由SSL/TLS+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全

HTTPS协议的主要作用可以分为两种：一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。

第一层：HTTPS本质上是为了实现加密通信，理论上，加密通信就是双方都持有一个对称加密的秘钥，然后就可以安全通信了

但是，无论这个最初的秘钥是由客户端传给服务端，还是服务端传给客户端，都是明文传输，中间人都可以知道。那就让这个过程变成密文就好了呗，而且还得是中间人解不开的密文。

第二层：使用非对称加密 加密客户端与服务端协商生成对称秘钥之前各种盐值、种子。

但是，在使用非对称加密秘钥之前，比如由服务端生成非对称秘钥，它需要将生成的公钥给到客户端，这个时候公钥就会在网络中明文传输，任何人都可以更改，会有中间人攻击的问题。因此，只能引入公信机构CA，使我们传输自己的公钥时可以保证不会被篡改！