HTTP和HTTPS

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不适合传输一些敏感的信息，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协议，SSL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。

HTTP：是互联网上应用最为广泛的一种网络协议，是一个客户端和服务器端请求和应答的标准，用于从www服务器传输超文本到本地浏览器的传输协议，它可以使浏览器更加高效，使网络传输减少。

HTTPS：是以安全为目标的HTTP通道，简单讲是HTTP的安全版，即HTTP下加入SSL层，HTTP的安全基础是SSL，因此加密的详细内容就需要SSL。

HTTPS协议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。另一种是确认网站的真实性。

简单来说，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，要比HTTP协议安全。

HTTPS和HTTP的区别主要如下：

1.https协议需要得到ca申请证书，一般证书免费的较少。

2.http是超文本协议，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。

HTTPS工作流程（也是保证数据安全的机制）：（一定记住，攻击者只能从中间截取信息，不能从源上获得信息）

1.客户端发起HTTPS请求：用户在浏览器中输入一个https网址，然后连接到服务器的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。

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：这部分工作是由客户端的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，用随机值用钥匙锁起来，服务端用钥匙去解锁，看到被锁住的内容。

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.服务端解密信息：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：这部分信息是服务端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端传过来的信息，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，也没有办法。

HTTPS的好处：

1.使用https协议可认证用户和服务器，确保数据发送到正确的客户机和服务器。

2.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，要比http协议安全，可防止数据在传输过程中不被窃取、改变、确保数据的完整性。

3.https是现行架构下最安全的解决方案，虽然不是绝对安全，但它大幅增加了中间人攻击的成本。

https的缺点：

1.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。

2.https连接缓存不如http高效，大流量网站如非必要也不会采用，流量成本太高。

3.https连接服务器端资源占用很多，支持访客稍多的网站需要投入更大的成本。

4.https协议握手阶段比较费时，对网站的响应速度有负面影响，如没必要，没有理由牺牲用户体验。

HTTPS的加密方式：

1.对称加密：对称密钥加密又称专用密钥加密，即发送和接收数据的双方必使用相同的密钥对明文进行加密和解密。

2.非对称加密：非对称加密算法需要两个密钥：公开密钥