https协议：超文本传输安全协议

（英语：Hypertext Transfer Protocol Secure，缩写：HTTPS，常称为HTTP over TLS，HTTP over SSL或HTTP Secure）

是一种通过计算机网络进行安全通信的传输协议。HTTPS经由HTTP进行通信，但利用SSL/TLS来加密数据包。HTTPS开发的主要目的，是提供对网站服务器的身份认证，保护交换数据的隐私与完整性。这个协议由网景公司（Netscape）在1994年首次提出，随后扩展到互联网上。

简单来说，HTTPS 是 HTTP 的安全版，是使用 SSL/TLS 加密的 HTTP 协议。通过 TLS/SSL 协议的的身份验证、信息加密和完整性校验的功能，从而避免信息窃听、信息篡改和信息劫持的风险。

HTTPS 提供了加密 (Encryption)、认证 (Verification)、鉴定 (Identification) 三种功能。如下的解释中，假设是张三和李四在通讯。

私密性(Confidentiality/Privacy):

也就是提供信息加密，保证数据传输的安全；保证信息只有张三和李四知道，而不会被窃听。

可信性(Authentication):

身份验证，主要是服务器端的，确认网站的真实性，有些银行也会对客户端进行认证；用来证明李四就是李四。

完整性(Message Integrity):

保证信息传输过程中的完整性，防止被修改；李四接收到的消息就是张三发送的。

HTTPS就是在应用层和传输层中间加了一道验证的门槛以保证数据安全

SSL/TLS 协议

SSL(Secure Socket Layer) 安全套接层

TLS(Transport Layer Security) 传输层安全

1996年 NetScape 公司发布 SSL v3.0；

1999年互联网标准化组织ISOC接替NetScape公司，发布了SSL的升级版TLS 1.0版。

2006年和2008年，TLS进行了两次升级，分别为TLS 1.1版和TLS 1.2版。

SSL 及其继任者 TLS 是为网络通信提供安全及数据完整性的一种安全协议。

TLS与SSL在传输层对网络连接进行加密。

SSL协议主要服务

1）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）加密数据以防止数据中途被窃取

3）维护数据的完整性，确保数据在传输过程中不被改变。

基本的运行过程

SSL/TLS协议的基本思路是采用公钥加密法，也就是说，客户端先向服务器端索要公钥，然后用公钥加密信息，服务器收到密文后，用自己的私钥解密。

（1）如何保证公钥不被篡改？

解决方法：将公钥放在数字证书中。只要证书是可信的，公钥就是可信的。

（2）公钥加密计算量太大，如何减少耗用的时间？

解决方法：每一次对话（session），客户端和服务器端都生成一个"对话密钥"（session key），用它来加密信息。由于"对话密钥"是对称加密，所以运算速度非常快，而服务器公钥只用于加密"对话密钥"本身，这样就减少了加密运算的消耗时间。

SSL/TLS协议的基本过程是这样的：

（1） 客户端向服务器端索要并验证公钥。

（2） 双方协商生成"对话密钥"。

（3） 双方采用"对话密钥"进行加密通信。

