SSL协议让网络上的数据传输更安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022_SSL_E5_8D_8F_E8_AE_AE_E8_c101_181881.htm SSL是一种安全传输协议，其全称是Securesocketlayer（安全套接层）。该协议最初由Netscape企业发展而来，现已成为网络上用来鉴别网站和网页浏览者身份，以及在浏览器使用者及网页服务器之间进行加密通讯的全球化标准。由于SSL技术已建立到了所有主要的浏览器和WEB服务器程序中，因此，仅需安装数字证书，或服务器证书就可以激活服务器功能了。 SSL的工作原理 SSL协议分为两部分：Handshake Protocol和RecordProtocol。其中Handshake Protocol用来协商密钥，协议的大部分内容就是通信双方如何利用它来安全的协商出一份密钥。RecordProtocol则定义了传输的格式。 SSL是一个介于HTTP协议与TCP之间的一个可选层，如果利用SSL协议来访问网页，其步骤如下： 1、用户： 在浏览器的地址栏里输入https://www.sslserver.com 2、HTTP层：将用户需求翻译成HTTP请求，如： GET/index.htmHTTP/1.1 Host http://www.sslserver.com 3、SSL层：借助下层协议的的信道，安全的协商出一份加密密钥，并用此密钥来加密HTTP请求。 4、TCP层：与服务器的443端口建立连接，传递SSL处理后的数据。 5、接收端（即服务器）与此过程相反。 SSL在TCP之上建立了一个加密通道，通过这一层的数据经过了加密，因此达到保密的效果。 如果上面你看得不太懂的话，我们来看一个更形象的比喻，我们假设A与B通信，A是SSL客户端，B是SSL服务器端，加密后的消息放在方括号[]里，以突出和明

文消息的区别。双方的处理动作的说明用圆括号（）括起。A：我想和你安全的通话，我这里的对称加密算法有DES，RC5，密钥交换算法有RSA和DH，摘要算法有MD5和SHA。 B：我们用DES－RSA－SHA这对组合好了。这是我的证书，里面有我的名字和公钥，你拿去验证一下我的身份（把证书发给A）。目前没有别的可说的了。 A：（查看证书上B的名字是否无误，并通过手头早已有的CA的证书验证了B的证书的真实性，如果其中一项有误，发出警告并断开连接，这一步保证了B的公钥的真实性）（产生一份秘密消息，这份秘密消息处理后将用作加密密钥，加密初始化向量和hmac的密钥。将这份秘密消息-协议中称为per_mas ter_secret-用B的公钥加密，封装成称作ClientKeyExchange的消息。由于用了B的公钥，保证了第三方无法窃听） 我生成了一份秘密消息，并用你的公钥加密了，给你（把ClientKeyExchange发给B） 注意，下面我就要用加密的办法给你发消息了！（将秘密消息进行处理，生成加密密钥，加密初始化向量和hmac的密钥） [我说完了] B：（用自己的私钥将C lientKeyExchange中的秘密消息解密出来，然后将秘密消息进行处理，生成加密密钥，加密初始化向量和hmac的密钥，这时双方已经安全的协商出一套加密办法了）。 注意，我也要开始用加密的办法给你发消息了！ [我说完了] A：[我的秘密是……] B：[其它人不会听到的……] SSL可以应用在哪些场合 通过原理的介绍，我们可以知道，利用SSL协议可以有效加强我们的信息传输保密性。利用这一点，我们就可以将其应用到WEB服务器的安全访问上，邮件的安全传输上等。如尚易网站的企业邮箱（https://mail.corpease.net/cgi-bin/domainadmin）就采用了这种

访问方式。 识别一个网站是否启用了SSL安全协议最简单最直接的办法就是看它的网址信息，通常的我们看到的都是以http://开头的网址，而采用了该安全协议后，网址的开头是：https://，多了一个S。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com