# SSL协议讲解

**一、作用**

不使用SSL/TLS的HTTP通信，就是不加密的通信。所有信息明文传播，带来了三大风险。

（1） **窃听风险**（eavesdropping）：第三方可以获知通信内容。

（2） **篡改风险**（tampering）：第三方可以修改通信内容。

（3） **冒充风险**（pretending）：第三方可以冒充他人身份参与通信。

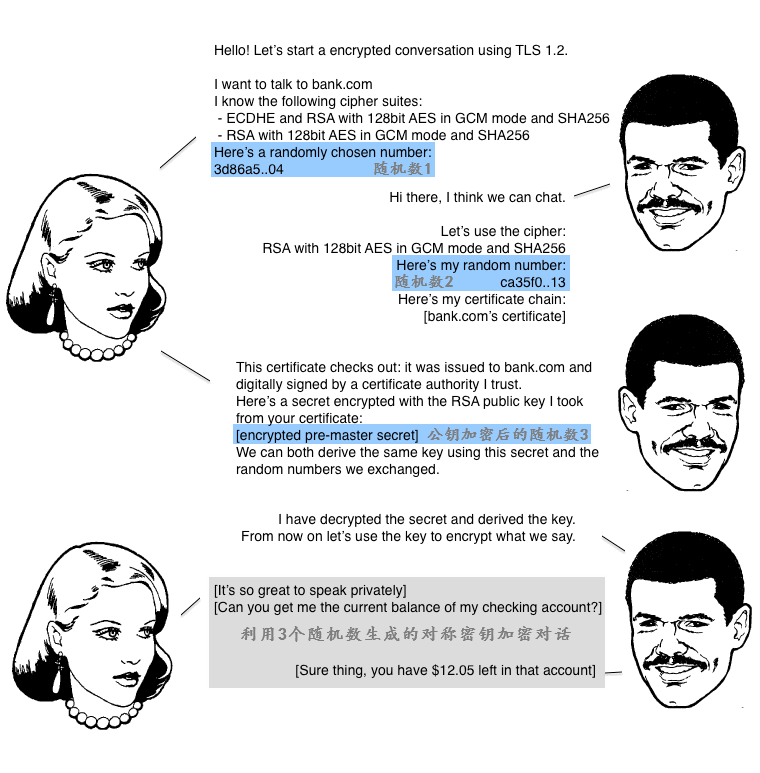
SSL/TLS协议是为了解决这三大风险而设计的，希望达到：

（1） 所有信息都是**加密传播**，第三方无法窃听。

（2） 具有**校验机制**，一旦被篡改，通信双方会立刻发现。

（3） 配备**身份证书**，防止身份被冒充。

**二、握手阶段的详细过程**



第一步，爱丽丝给出支持的协议版本、支持的压缩方法、支持的加密方法，比如RSA公钥加密、一个客户端生成的随机数1（Client random）。

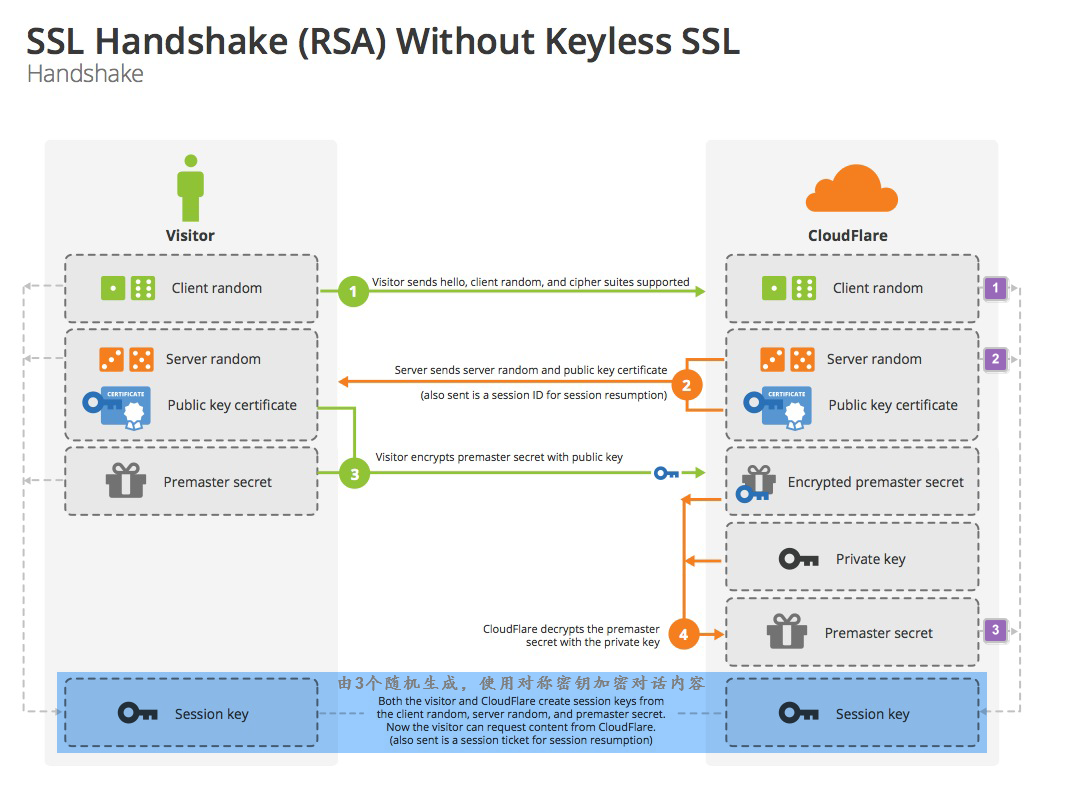
第二步，鲍勃确认双方使用的加密方法，并给出数字证书（证明自己网站的权威性，验证证书的密钥由浏览器自带）、以及一个服务器生成的随机数2（Server random）。如果服务器需要确认客户端的身份，就会再包含一项请求，要求客户端提供"客户端证书"。比如，金融机构往往只允许认证客户连入自己的网络，就会向正式客户提供USB密钥，里面就包含了一张客户端证书。

第三步，爱丽丝确认数字证书有效，然后生成一个新的随机数3（Premaster secret），并使用数字证书中的**公钥**，加密这个随机数，发给鲍勃。如果前一步，服务器要求客户端证书，客户端会在这一步发送证书及相关信息。

第四步，鲍勃使用自己的**私钥**，获取爱丽丝发来的随机数（即Premaster secret）。

第五步，爱丽丝和鲍勃根据约定的加密方法，使用前面的三个随机数，生成"对话密钥"（session key），用来加密接下来的整个对话过程。

如下图所示：



握手阶段有三点需要注意。

（1）生成对话密钥一共需要三个随机数。

（2）握手之后的对话使用"对话密钥"加密（对称加密），服务器的公钥和私钥只用于加密和解密"对话密钥"（非对称加密），无其他作用。

（3）服务器公钥放在服务器的数字证书之中。

至于**为什么一定要用三个随机数**，来生成"会话密钥"，[dog250](http://blog.csdn.net/dog250/article/details/5717162)解释得很好：

"不管是客户端还是服务器，都需要随机数，这样生成的密钥才不会每次都一样。由于SSL协议中证书是静态的，因此十分有必要引入一种随机因素来保证协商出来的密钥的随机性。

对于RSA密钥交换算法来说，pre-master-key本身就是一个随机数，再加上hello消息中的随机，三个随机数通过一个密钥导出器最终导出一个对称密钥。

pre master的存在在于**SSL协议不信任每个主机都能产生完全随机的随机数**，如果随机数不随机，那么pre master secret就有可能被猜出来，那么仅适用pre master secret作为密钥就不合适了，因此必须引入新的随机因素，那么客户端和服务器加上pre master secret三个随机数一同生成的密钥就不容易被猜出了，一个伪随机可能完全不随机，可是是三个伪随机就十分接近随机了，每增加一个自由度，随机性增加的可不是一。"

某些客户（比如银行）想要使用外部CDN，加快自家网站的访问速度，但是出于安全考虑，不能把私钥交给CDN服务商。这时，完全可以把私钥留在自家服务器，只用来解密对话密钥，其他步骤都让CDN服务商去完成。

