1、**在SSL协议中，Web服务器为什么要将自己的证书发送给客户端？**

数字证书是一种实现身份认证的技术。CA认证中心有一个根证书，是信任链的起点，就是大家都相信CA认证中心。CA认证中心给了服务器一个数字证书。客户端连接服务器的时候，下载这个数字证书，并用上一级（CA）的公钥来解密与验证是否合法，从而判断和你通信的服务器的身份是否真实。从而能有效防止钓鱼网站和中间人攻击，

2**、SSL协议采用的是链式加密，这种加密方法的优点是什么？**

通过公开密钥算法交换对称密钥。

（1）公开密钥算法耗时长，对称密钥算法耗时短，可以提高整个系统效率

（2）方便经常性的更换对称密钥，防止被破译，提高通信的安全性

3、**TLS 1.0对SSL3.0做了哪些改进？TLS 1.3对低版本TLS进行了哪些改进？**

TLS1.0于1999年1月发布，与SSL3相比，它有以下的区别：

(1).TLS 1.0 的主版本为3, 次版本为1，而与之对应的SSL 3.0的主版本为3，次版本为0。TLS 1.1的主版本为3，次版本为2

(2).消息认证码:TLS的MAC与SSL3.0的MAC有两点不同：TLS使用RFC2104中定义的HMAC算法；TLS使用称为“PRF”的伪随机函数

(3).告警码:除no\_certificate外，TLS继承了SSL3.0中定义的所有告警码。另外，还定义了新的告警码:

密码套件:TLS和SSL3.0存在细小差别，即TLS不支持Fortezza密钥交换、加密算法，而(4).SSL3.0是支持的

(5).客户端证书类型:在CertificateRequest消息中，TLS支持SSL3.0中定义的rsa\_sign, dss\_sign, rsa\_fixed\_dh和dss\_fixed\_dh证书，但不支持SSL 3.0支持的rsa\_ephemeral\_dh, dss\_ephemeral和fortezza\_kea证书

(6).填充:在SSL中，填充后的数据长度正好是分组加密算法中分组长度的最小整数倍。而TLS填充后的数据长度可以是分组长度的任意整数倍（但填充最大长度为255字节）

TLS 1.3 与之前的协议有较大差异，主要在于：

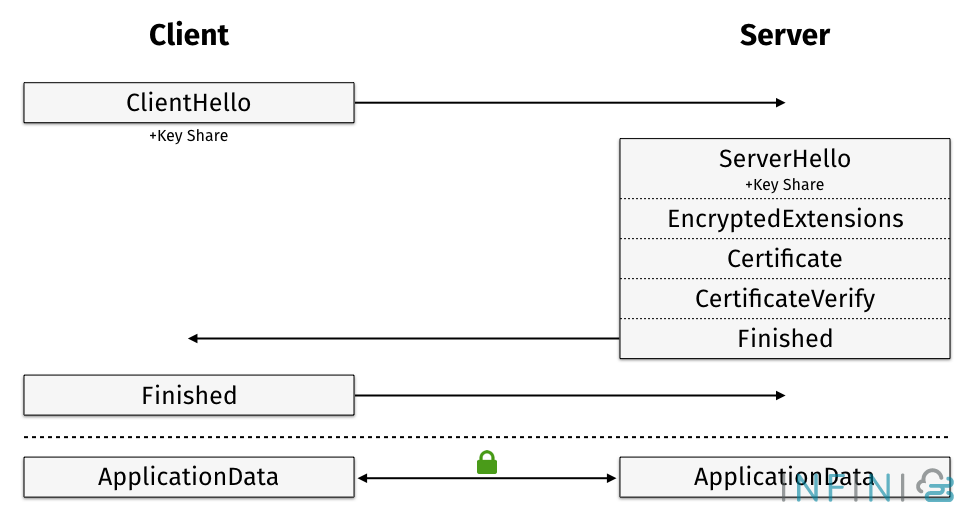
(1)将不再支持静态RSA密钥交换，握手将默认使用前向安全(Perfect Forward Secrecy)，一个安全性足够强的 Diffie-Hellman 参数。

(2) 减少不安全的Diffie-Hellman参数选项

(3) TLS 1.3服务器对整个握手记录进行签名，包括密钥协商，避免三次握手攻击。此外，还实现了握手协议和记录协议的密钥分离

(4) 删除不安全的认证加密方法, TLS 1.3 中允许的唯一认证加密方法是AEAD（Authenticated Encryption with Additional Data），它将机密性和完整性整合到一个无缝操作中

(5) 禁止一些安全性较弱的密码原语

TLS 1.3已删除所有可能存在问题的密码组件和密码模式，包括CBC 模式密码或不安全的流式密码，如 RC4。建议用SHA-2，不建议使用安全性较弱的MD5和SHA-1 

4、**TLS 1.3 为什么可以简化TLS 1.2 握手协议的交互过程？**

使用 TLS 1.2 需要两次往返（ 2-RTT ）才能完成握手，然后才能发送请求。

TLS 1.3 的握手不再支持静态的 RSA 密钥交换，这意味着必须使用带有前向安全的 Diffie-Hellman 进行全面握手。从上图可以看出，使用 TLS 1.3 协议只需要一次往返（ 1-RTT ）就可以完成握手; TLS 1.3除了对新建连接过程进行优化之外，对连接恢复过程也进行了优化，对于近期访问过的站点，可以直接发送有用的数据，而不需要经过握手。做到了零次往返（不额外增加网络延时”模式0-RTT）