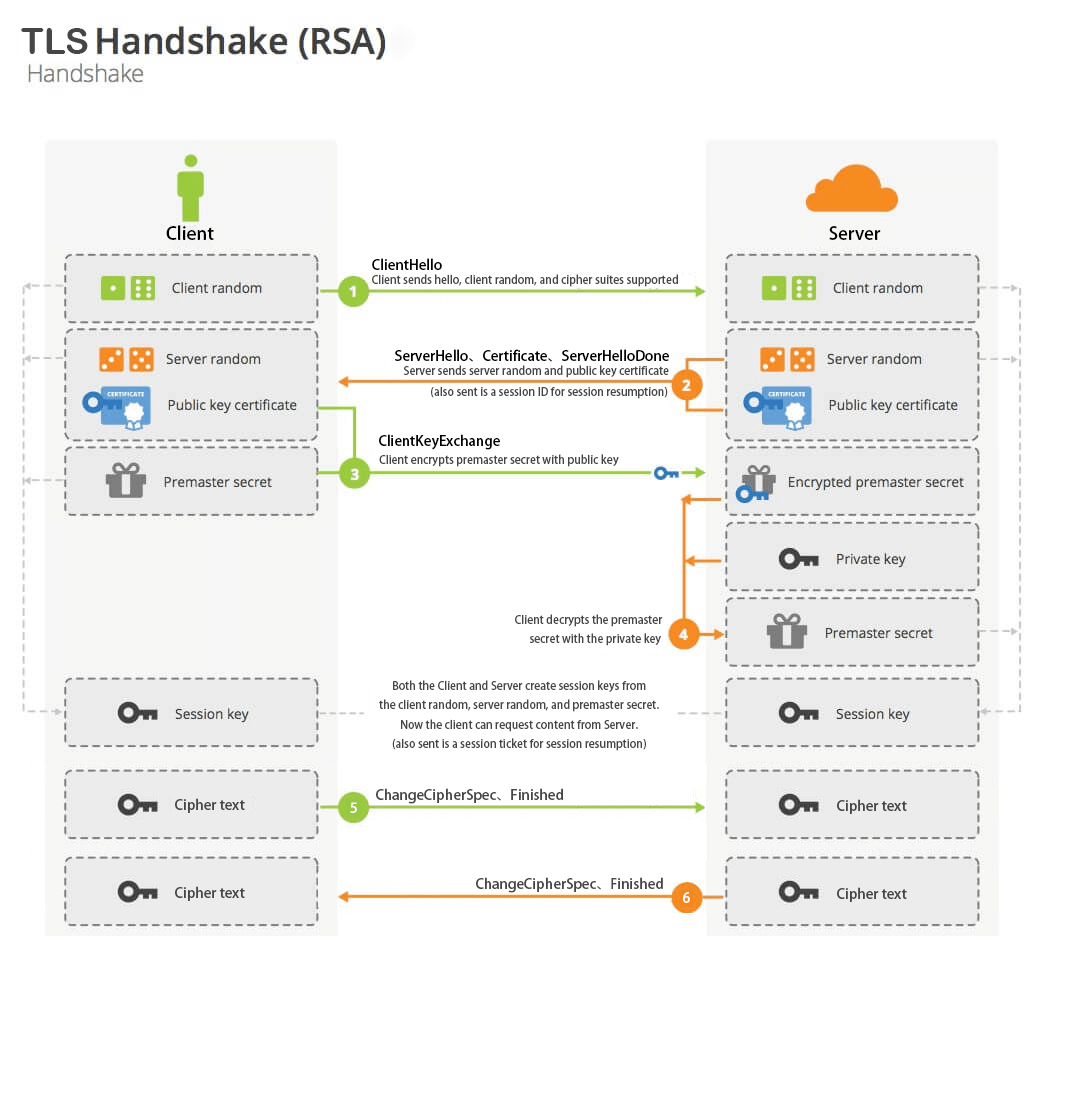
[https://ssl-config.mozilla.org/#server=nginx&version=1.22.0&config=intermediate&openssl=1.1.1q&hsts=false&ocsp=false&guideline=5.6](https://ssl-config.mozilla.org/" \l "server=nginx&version=1.22.0&config=intermediate&openssl=1.1.1q&hsts=false&ocsp=false&guideline=5.6" \t "_blank)

这个网站是关于TLS配置文件的生成器，根据不同的服务器类型、软件版本和安全策略，生成最佳的 TLS 配置。

<https://ciphersuite.info/cs/>

这个网站详细列出了不同的加密套件cipher suite提供有关它们的详细信息，包括支持的加密算法、密钥交换方法、消息认证码 (MAC) 算法等，例如在实际的项目生产环境中选择合适的加密套件

TLS1.2握手流程图基于 DH 密钥协商算法



1. ClientHello（客户端问候）

客户端的行为：

客户端向服务器发送 ClientHello 消息。

内容包括：

客户端随机数 (Client random)：用于生成会话密钥。

支持的加密套件列表（cipher suites），例如 TLS 版本和加密算法。

目的： 让服务器知道客户端的能力，并开始协商用于安全通信的参数。