前提:

服务器拥有公钥A和私钥B

客户端拥有对称加密C

第一次:

客户端向服务器请求公钥A

说明:第一次发送请求时使用的为公钥A私钥B的非对称加密

第二次:

服务器向客户端发送公钥A

说明:第二次发送请求时使用的为公钥A私钥B的非对称加密

第三次:

客户端向服务器发送AC加密建立连接

说明:第三次以及后续的数据传输使用的是AC的对称协议进行加密

客户端通过CA证书来鉴别公钥A是否为请求访问的服务器所返回

CA证书由专门的颁发机构进行颁发,互联网公司来通过购买证书来进行认证

CA证书上记录了一些相关的信息,有颁发者,认证公司等等信息

特点:

除了首次传输时使用的是非对称加密,后续进行数据传输过程中都是采用的堆成加密,因为非对称加密首次传输的过程中的效率相对低,但是后续传输过程中均采用对称加密,效率相对全程采用非对称加密的效率更高,且安全性相比较全程采用对称加密安全性更高