**密码学原理**

**实验四：Web PKI与TLS**

学号：2022112266 姓名：魏圣卓

**实验目的**：通过搭建一个HTTPS网站并分析Web PKI与TLS协议来理解密码学的现实应用。

实验内容：

1. 建立一个部署数字证书的网站

要求：注册一个域名，建立一个Web网站，生成该网站的数字证书并部署，通过HTTPS访问该网站。域名可免费申请。Web服务器推荐购买云服务。证书可以通过自建CA颁发（需在浏览器部署CA信任锚），或者向第三方CA（Let’s Encrypt、GoDaddy等）申请。

域名：[https://cherrling.cn/](https://cherrling.cn/#/)

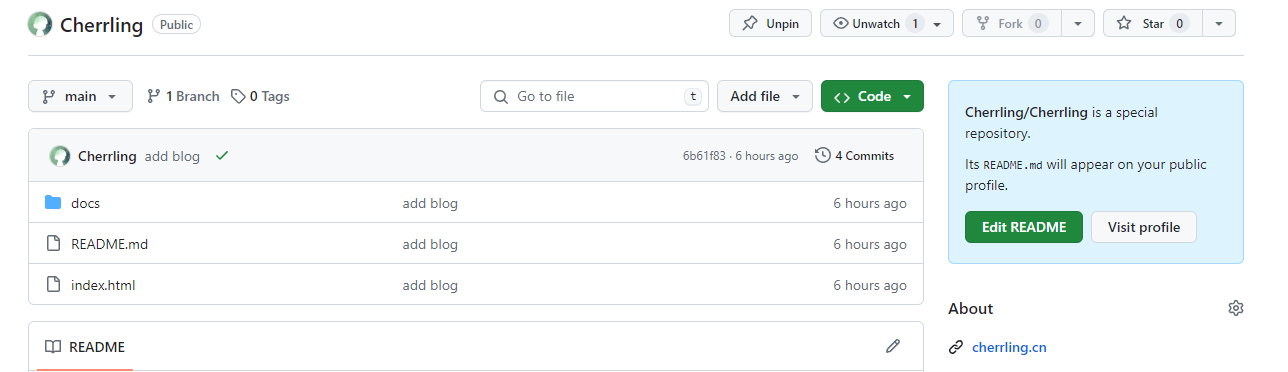


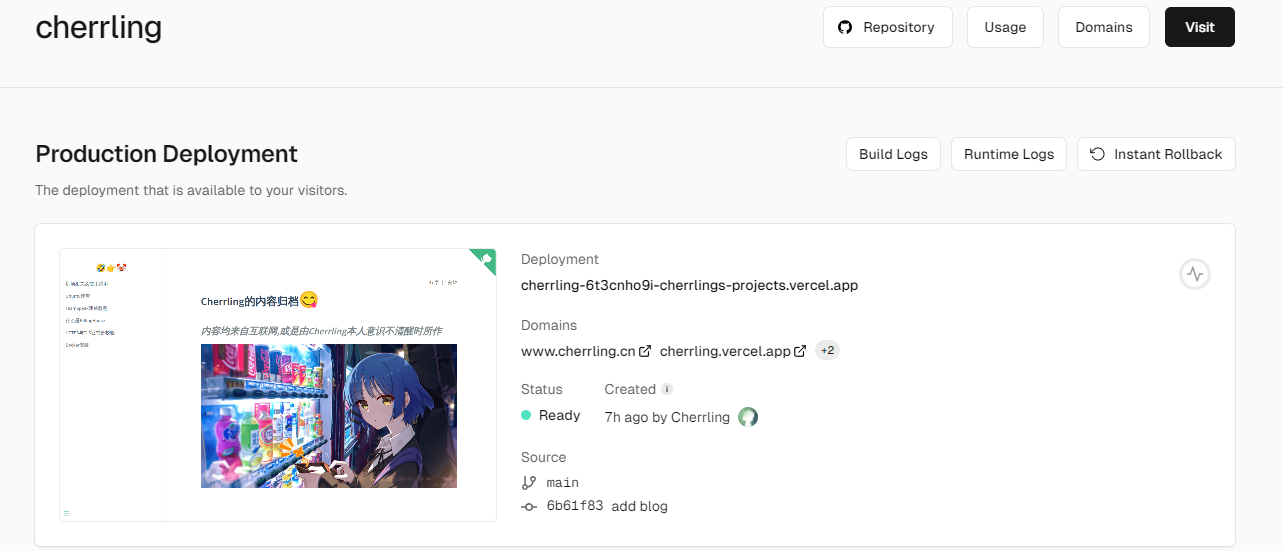
将域名解析至静态托管的服务器：





部署网页的静态文件，由托管服务器拉取：

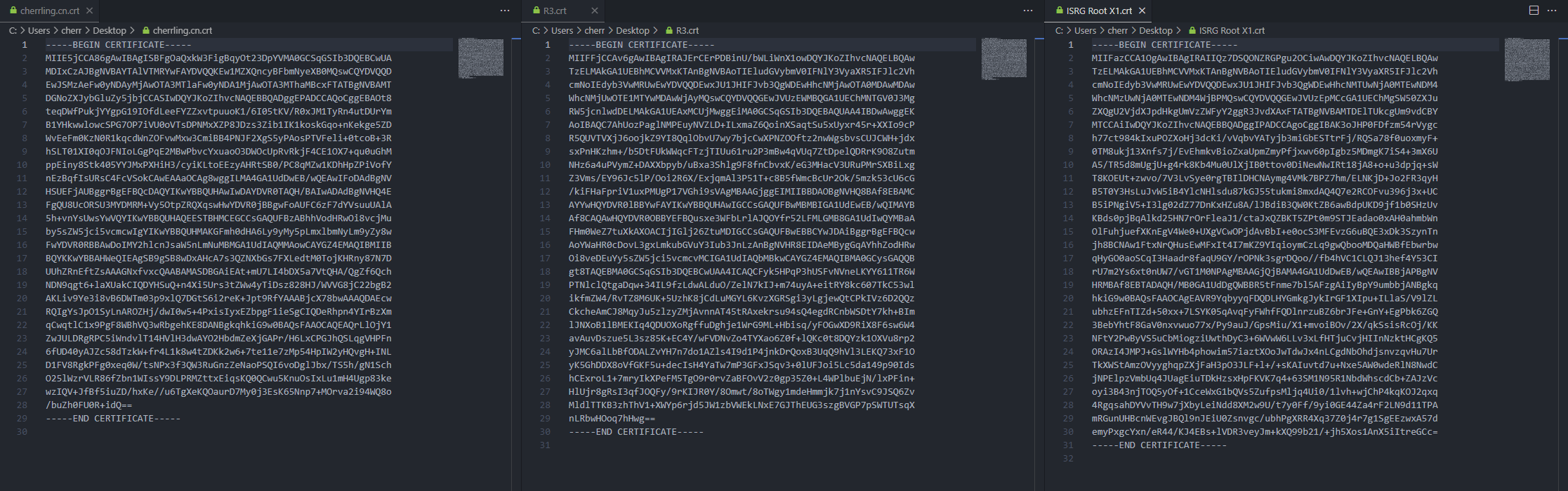




部署后由托管服务商向Let’s Encrypt 申请ssl证书：

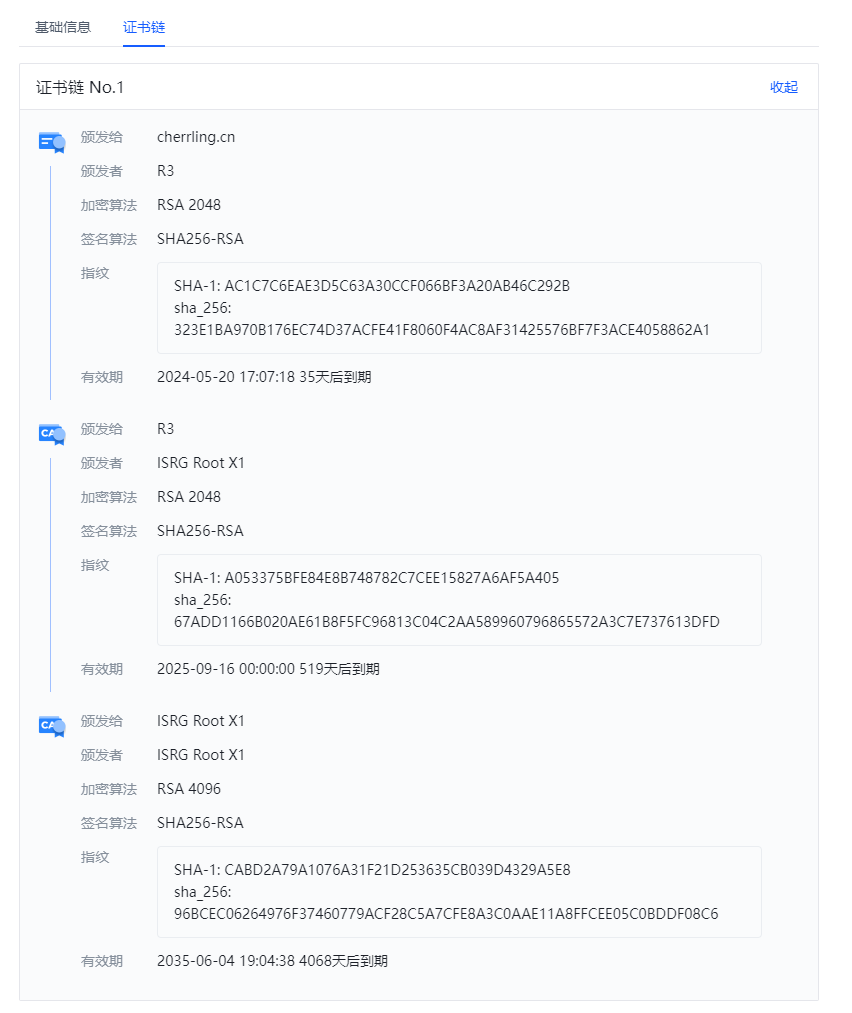


证书文件查看：



1. TLS协议的密码学要素分析

要求：参考TLS1.3协议，通过浏览器自带功能和网络抓包等协议分析方法，详细展示其中的密码学要素信息，包括所涉及的密钥协商协议、数字签名（证书）、非对称加密和对称加密方案。



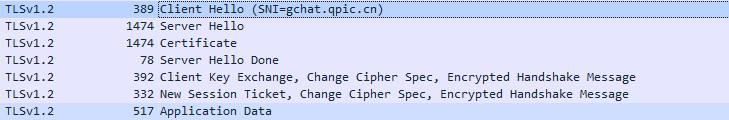






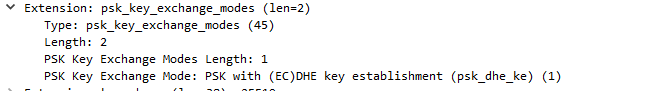
使用wireshark抓取网络数据包，分析对目标服务器的访问数据流：

TLS1.2

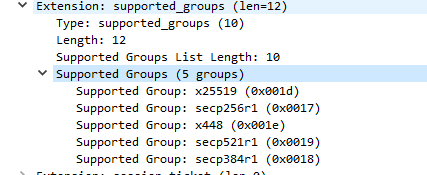


ClientHello

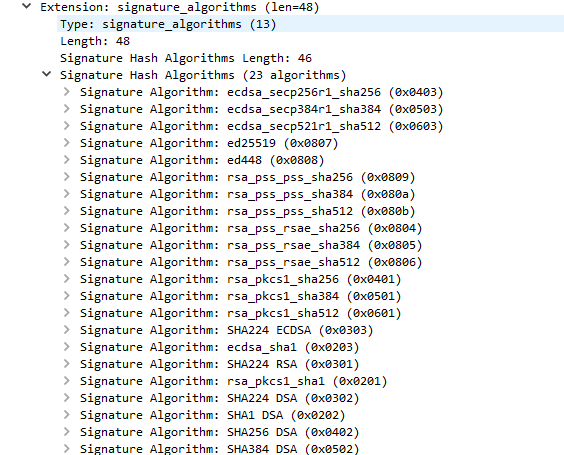
客户端申请的密钥交换模式：



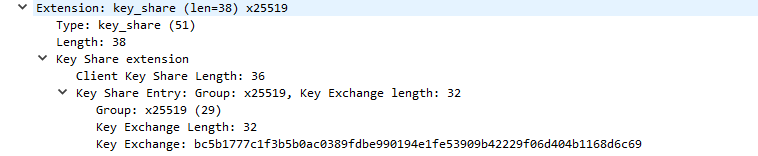
客户端支持的椭圆曲线组：



客户端支持的签名算法：

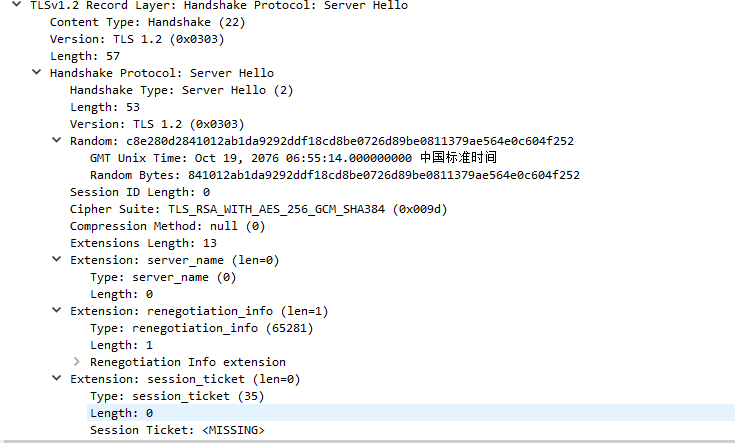


客户端共享的公钥

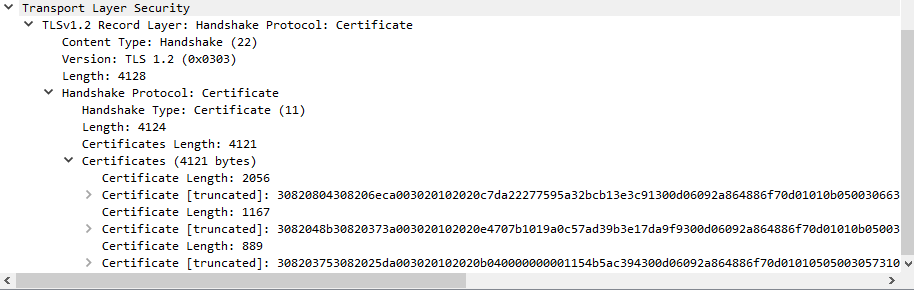


Server hello:

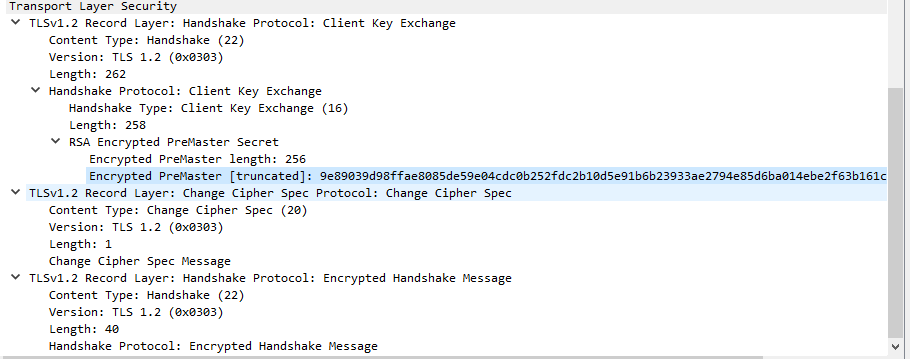
服务器端发送公钥给客户端



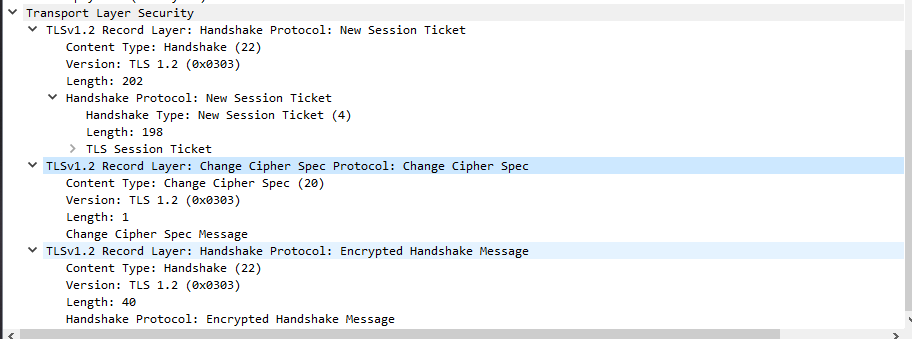
证书部分，服务器将证书发给客户端，客户端逐层验证证书链：



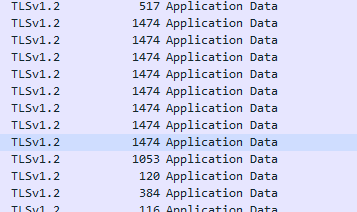
客户端交换premaster密钥，同时要求改变加密模式，再发送一条加密后的消息以作验证：



服务器端改变加密模式，发送加密消息：

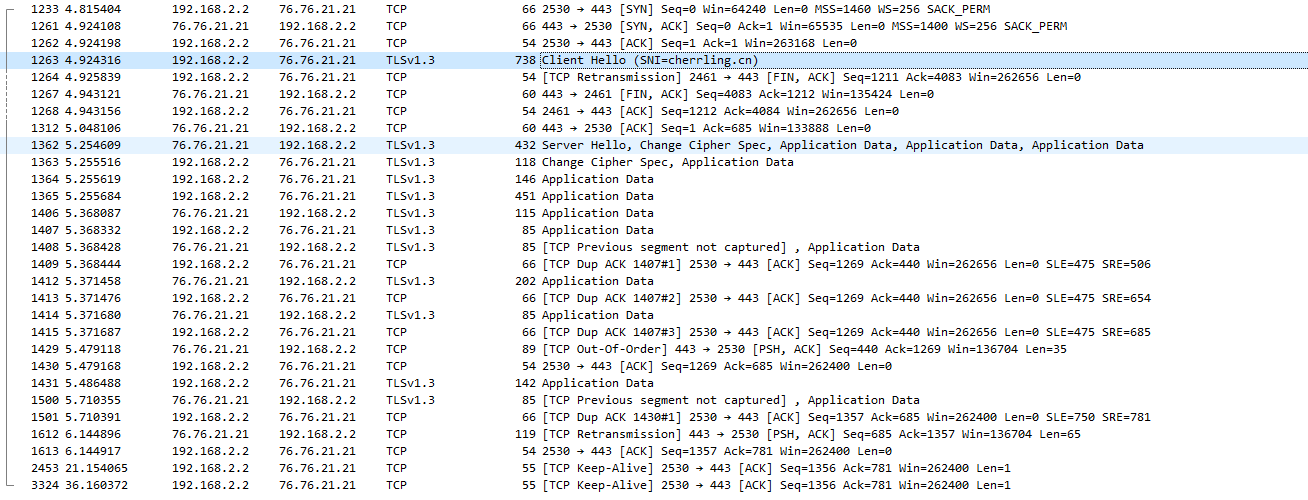


TLS握手结束，后续开始传送应用信息：



TLS1.3

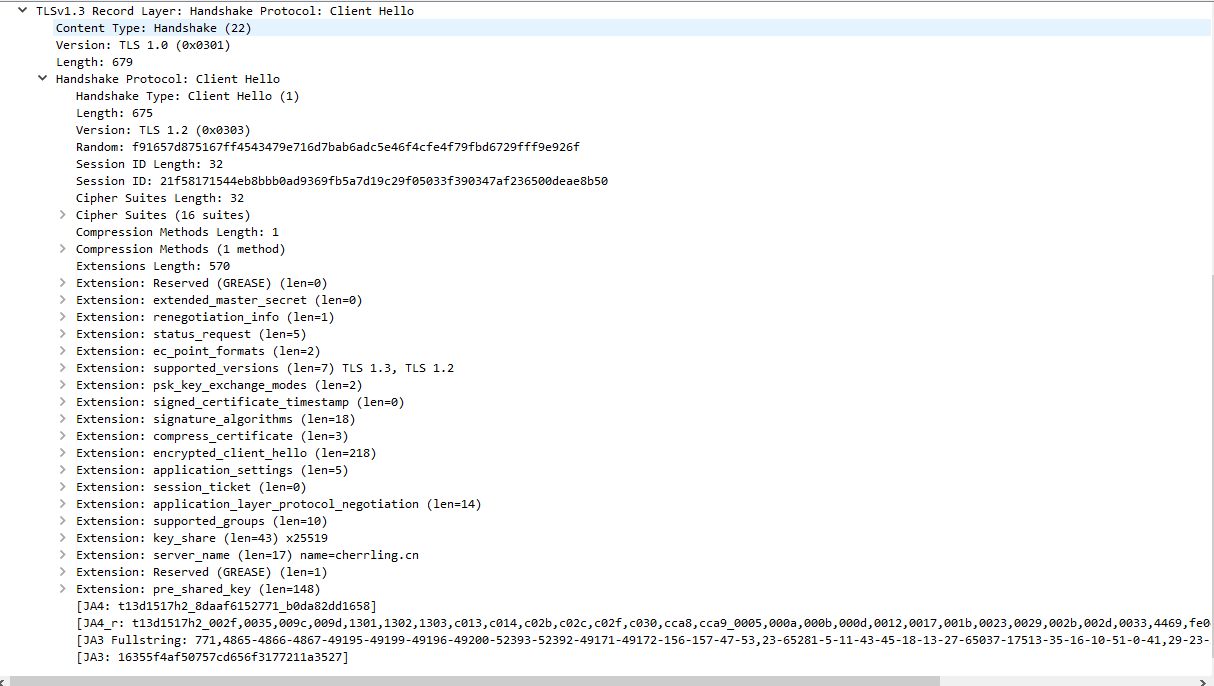
TCP三次握手，Client Hello Server Hello 交换密钥



Client hello:

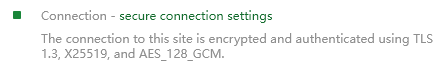
客户端发送hello，传输自己支持的密码学套件和公钥

发送random随机数，本次session id ，客户端指定密钥交换模式为ECDHE(TLS1.3指定)



Server hello：

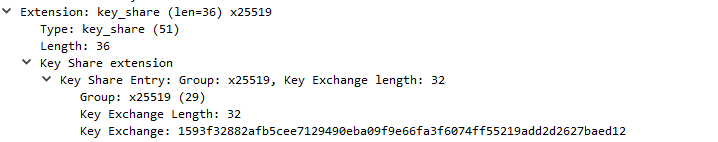
服务器根据客户端选择的加密套件和公钥计算自己的公私钥对

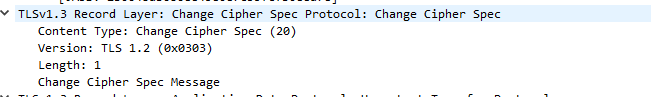


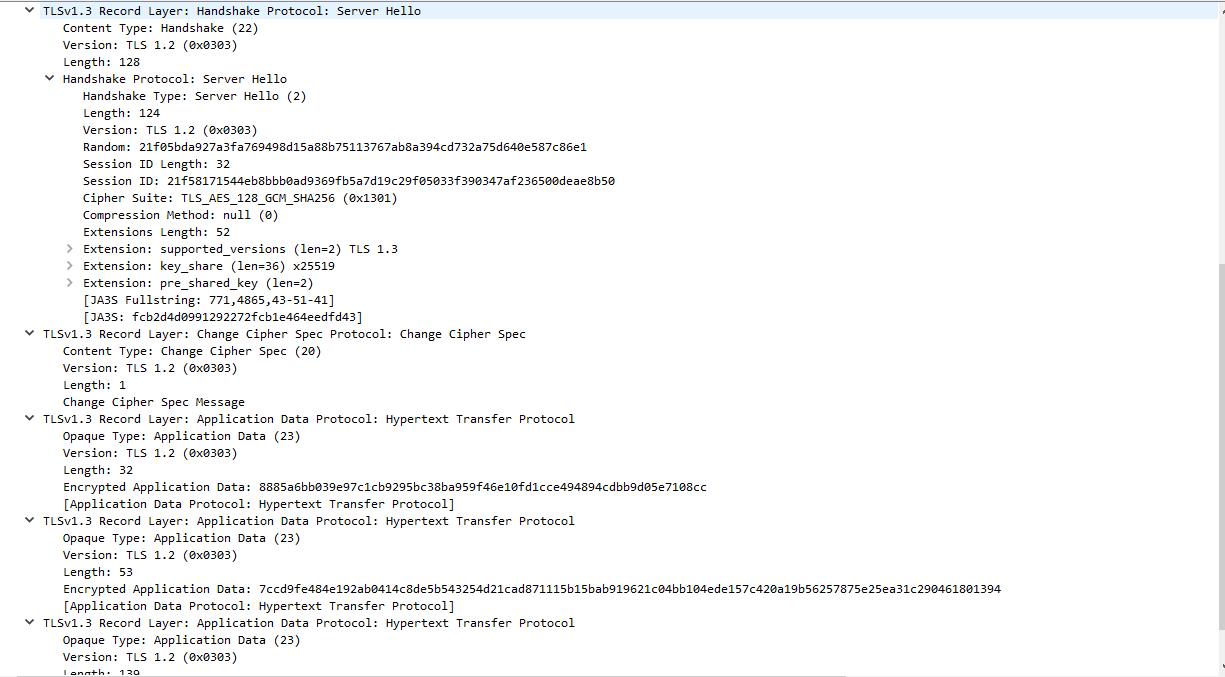
协商后使用AES\_128\_GCM作为对称加密方案

使用x25519椭圆曲线加密，将自己的公钥发给客户端

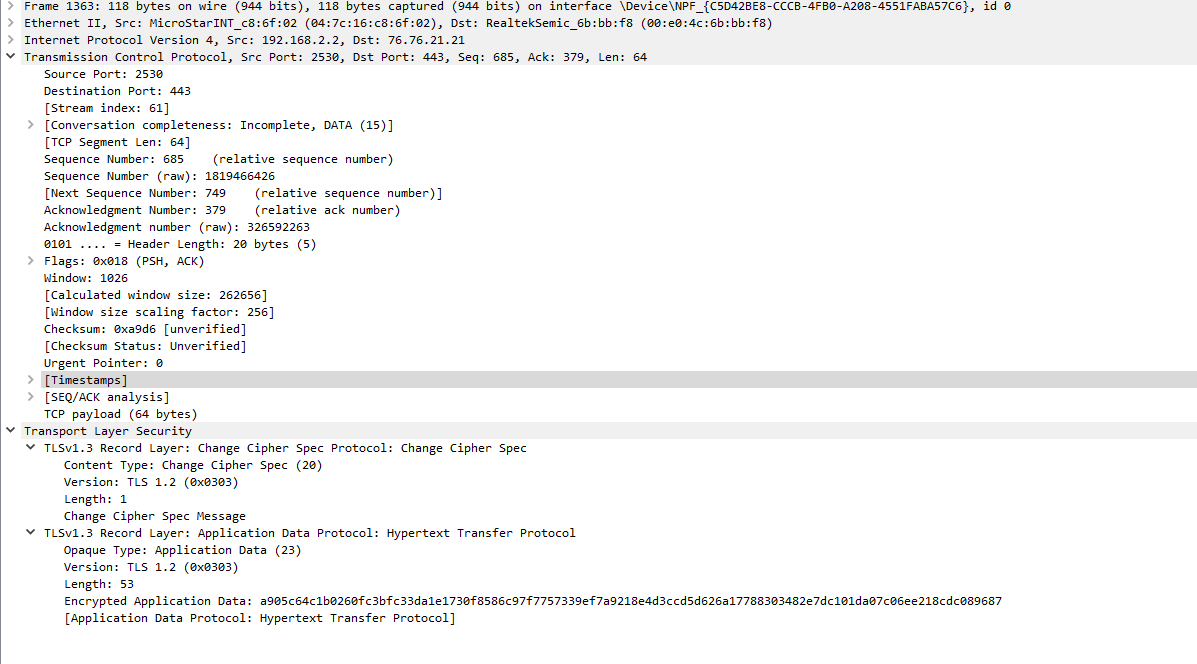
开始转变加密模式，使用对称密钥加密通信

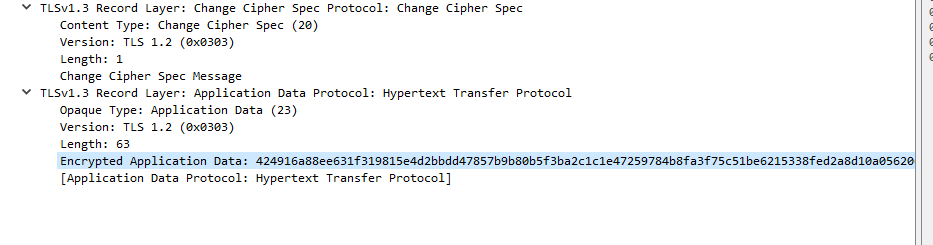




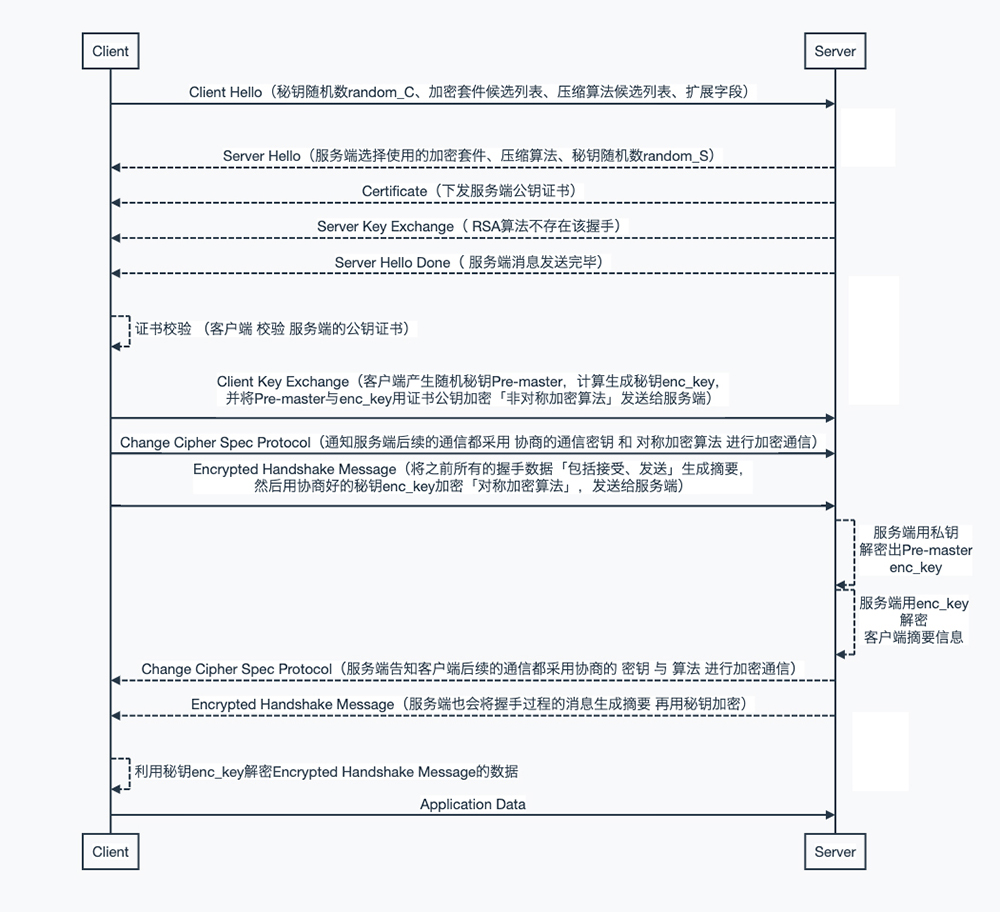


密钥交换：





TLS1.2流程图：



TLS1.3流程图：

