**密码学原理**

**实验四：Web PKI与TLS**

学号： 姓名：

**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。

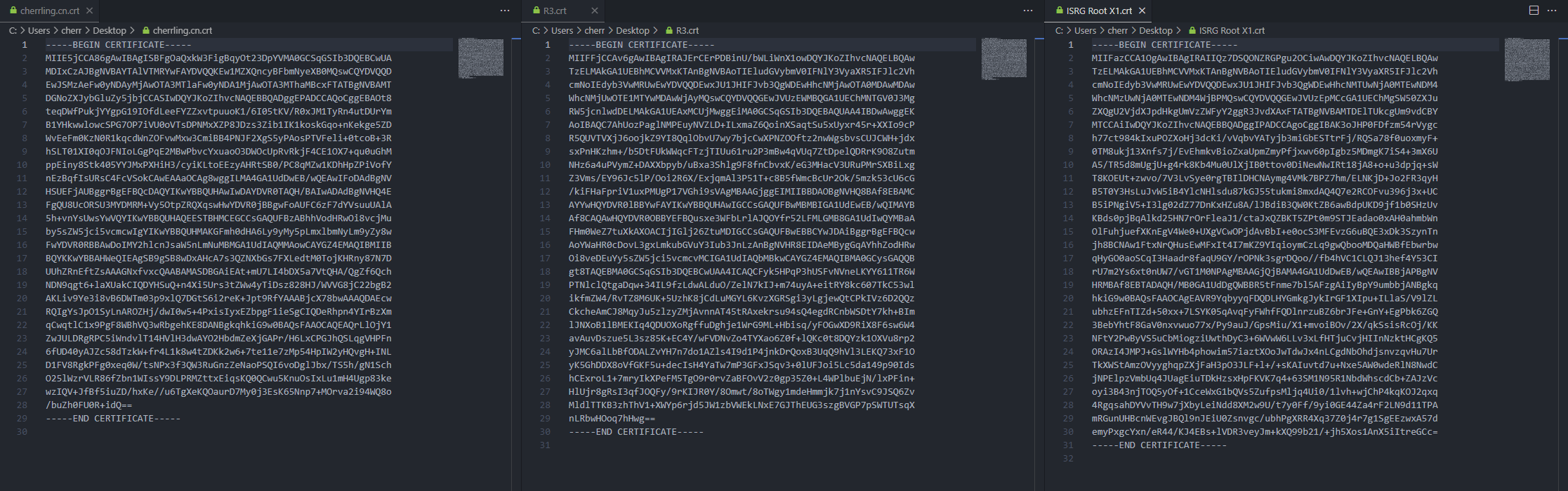
**实验内容：**

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。

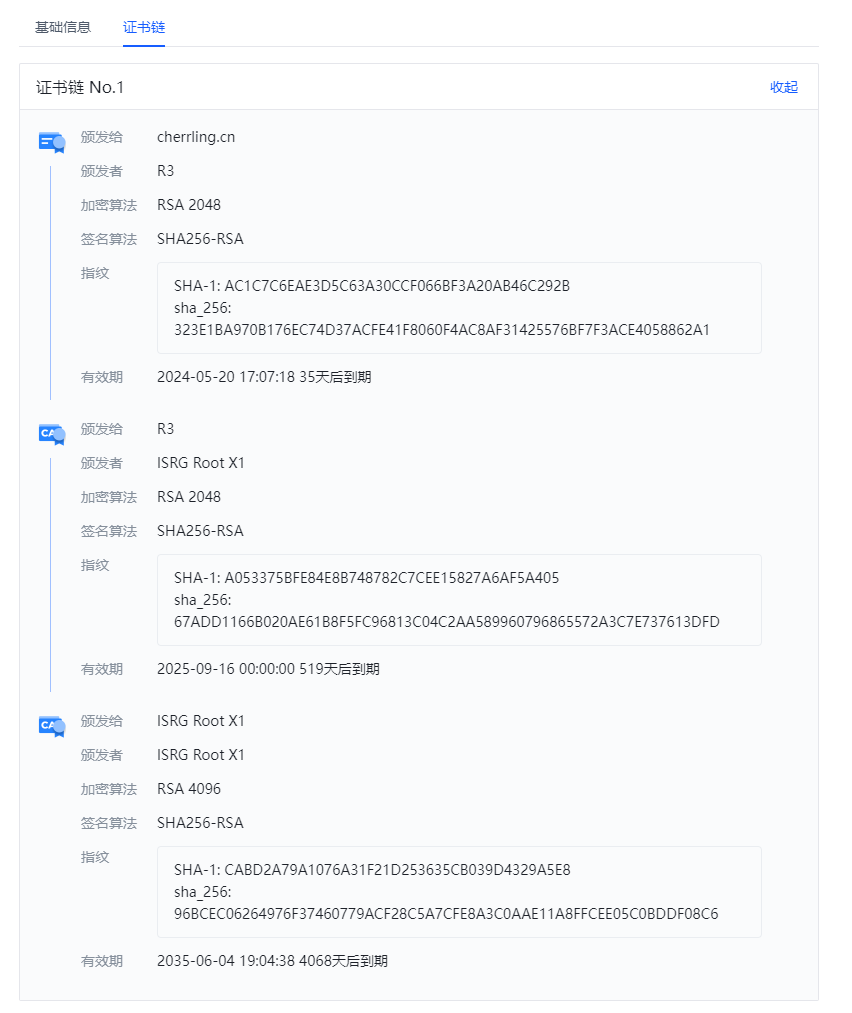
域名：[https://cherrling.cn/](https://cherrling.cn/#/)





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。

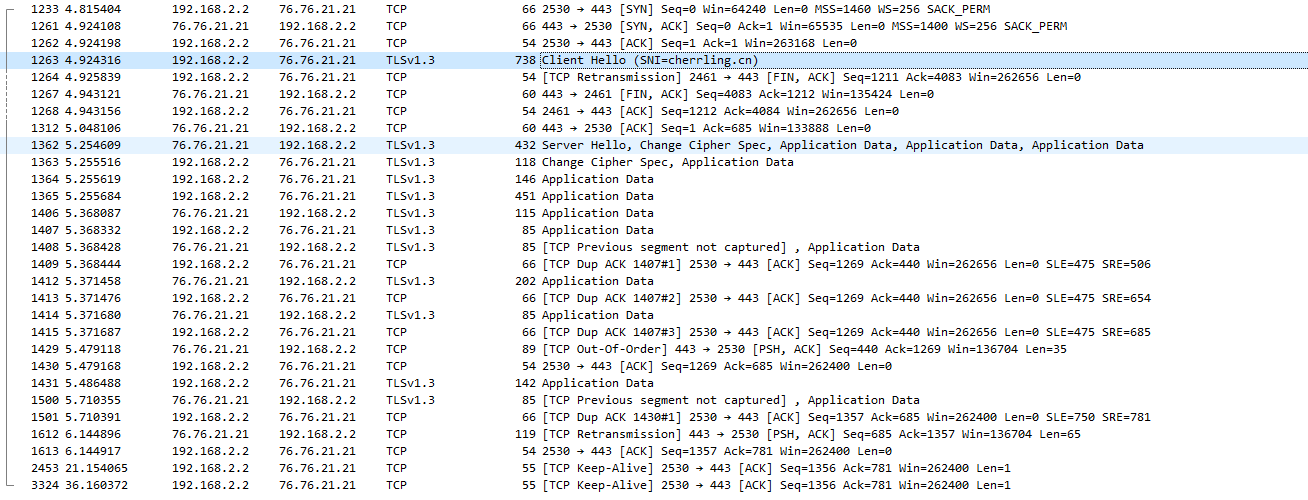




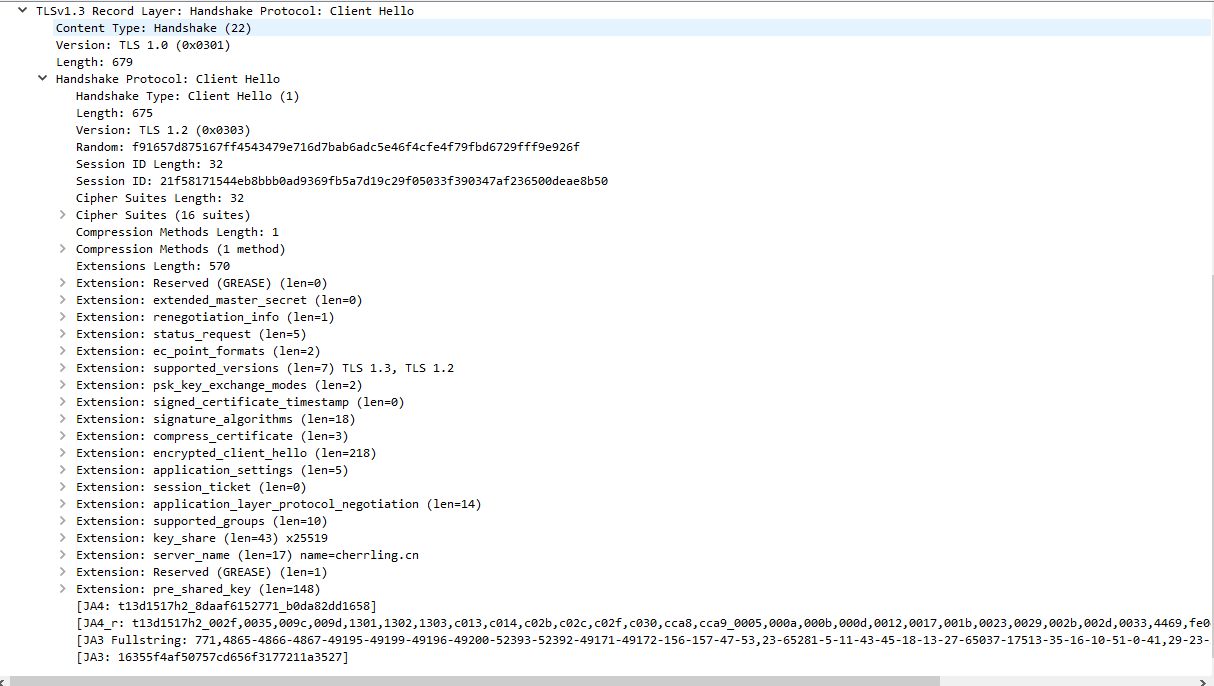




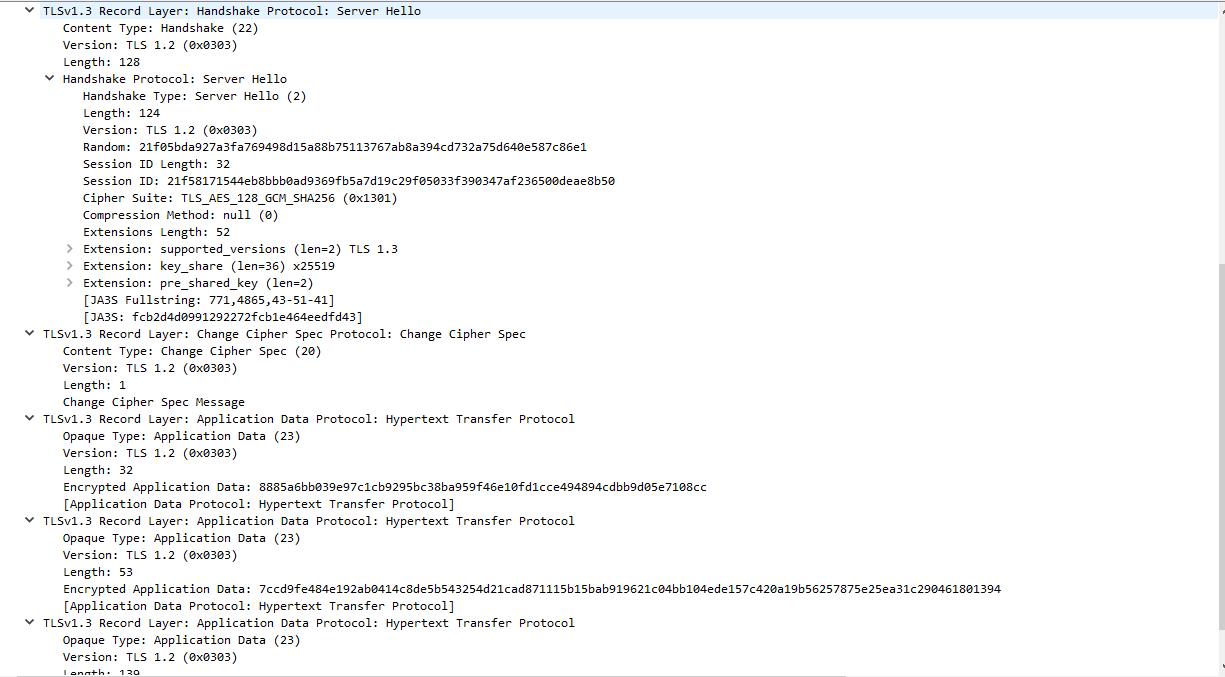
TCP三次握手，Client Hello Server Hello 交换密钥



Client hello:



Server hello：



密钥交换：

