# 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/

将域名解析至静态托管的服务器：

记录类型 查看帮助文档

A- 将域名指向一个IPV4地址

* 主机记录

@ .cherrling.cn

解析请求来源

指域名访问者所在的地区和使用的运营商网络。

默认 - 必填！未匹配到智能解析线路时，返回【默认】线路设置结果

升级至企业版DNS，支持按更精细线路（省份、国家）请求来源返回不同记录值。

* 记录值

76.76.21.21

* TTL

10 分钟

升级至企业版DNS，TTL最小可设置1秒。

记录类型 查看帮助文档

CNAME- 将域名指向另外一个域名

* 主机记录

www .cherrling.cn

解析请求来源

指域名访问者所在的地区和使用的运营商网络。

默认 - 必填！未匹配到智能解析线路时，返回【默认】线路设置结果

升级至企业版DNS，支持按更精细线路（省份、国家）请求来源返回不同记录值。

* 记录值

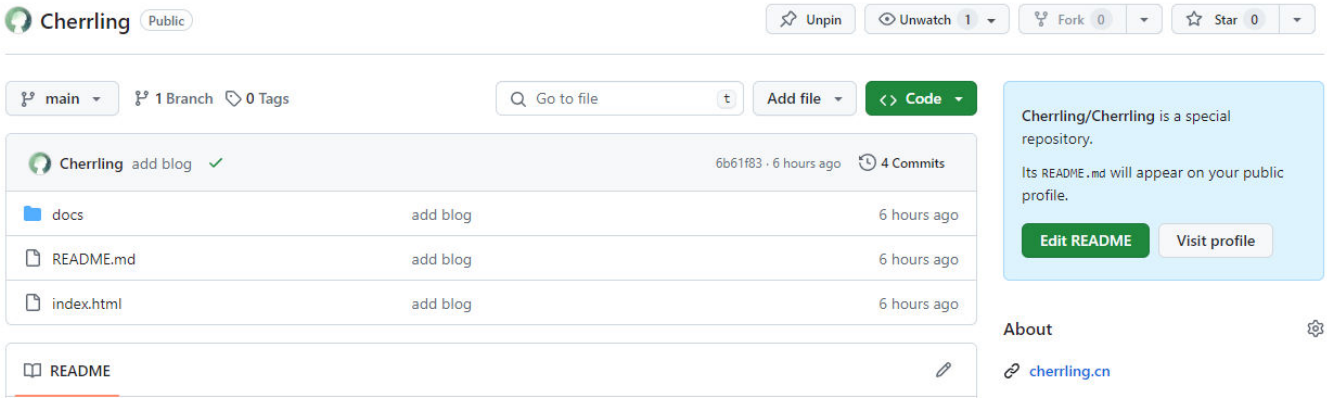
cname.vercel-dns.com

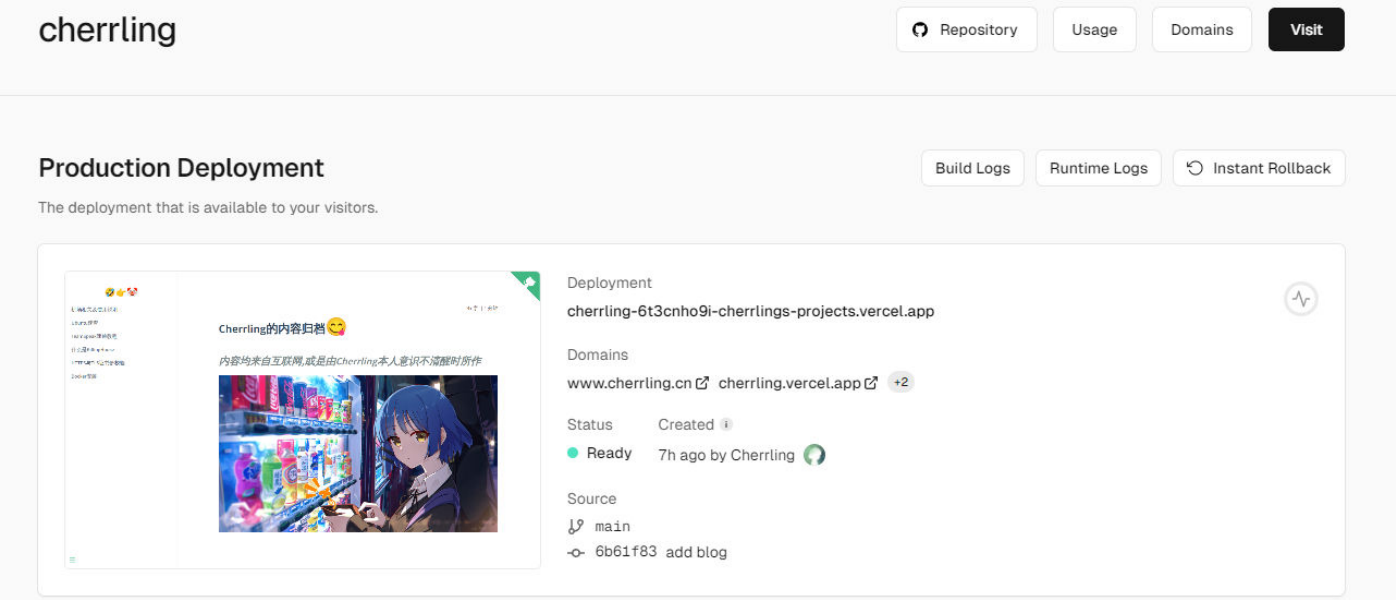
* TTL

10 分钟

升级至企业版DNS，TTL最小可设置1秒。

部署网页的静态文件，由托管服务器拉取：

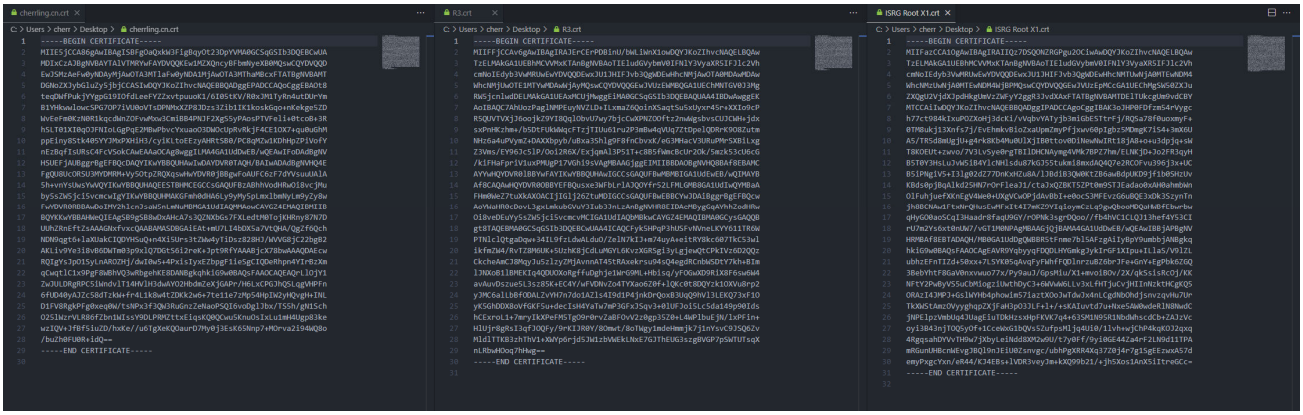



部署后由托管服务商向 Let’s Encrypt 申请 ssl 证书：

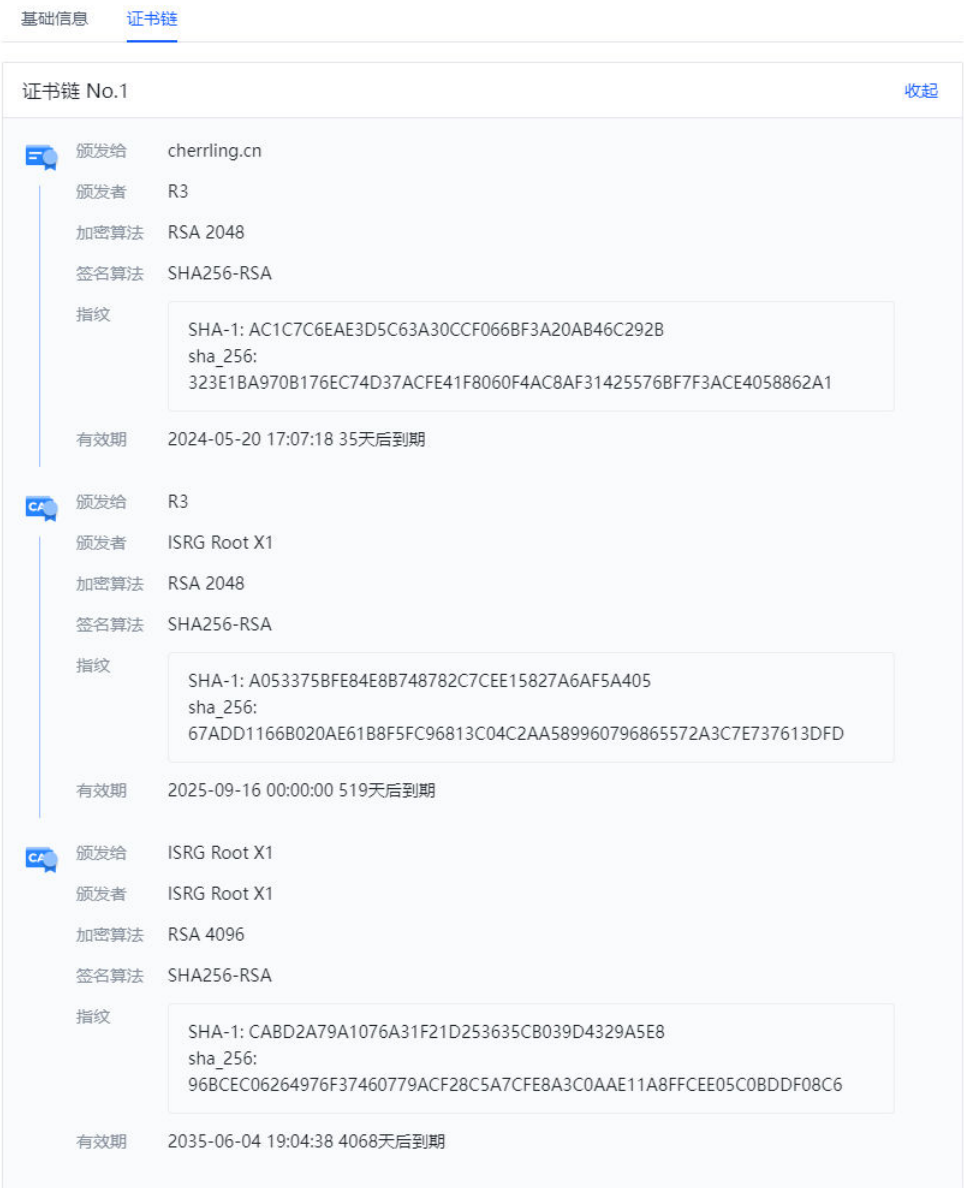

证书查看者：cherrling.cn
基本信息(G)
详细信息(D)
证书层次结构
ISRG Root X1
R3
cherrling.cn
证书字段
有效期
不早于
不晚于
主题背景
证书持有者的公共密钥信息
证书持有者公共密钥算法
证书持有者的公共密钥
扩展程序
字段值
PKCS #1，带有 RSA 加密的 SHA-256

证书文件查看：



2. 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。



基础信息　证书链

证书链 No.1　收起

| | |
|---|---|
| 颁发给 | cherrling.cn |
| 颁发者 | R3 |
| 加密算法 | RSA 2048 |
| 签名算法 | SHA256-RSA |
| 指纹 | SHA-1: AC1C7C6EAE3D5C63A30CCF066BF3A20AB46C292B<br>sha_256:<br>323E1BA970B176EC74D37ACFE41F8060F4AC8AF31425576BF7F3ACE4058862A1 |
| 有效期 | 2024-05-20 17:07:18 35天后到期 |

| | |
|---|---|
| 颁发给 | R3 |
| 颁发者 | ISRG Root X1 |
| 加密算法 | RSA 2048 |
| 签名算法 | SHA256-RSA |
| 指纹 | SHA-1: A053375BFE84E8B748782C7CEE15827A6AF5A405<br>sha_256:<br>67ADD1166B020AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD |
| 有效期 | 2025-09-16 00:00:00 519天后到期 |

| | |
|---|---|
| 颁发给 | ISRG Root X1 |
| 颁发者 | ISRG Root X1 |
| 加密算法 | RSA 4096 |
| 签名算法 | SHA256-RSA |
| 指纹 | SHA-1: CABD2A79A1076A31F21D253635CB039D4329A5E8<br>sha_256:<br>96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6 |
| 有效期 | 2035-06-04 19:04:38 4068天后到期 |

## 主题信息

| | |
|---|---|
| 域名（CN） | cherrling.cn |
| 备用域名（SAN） | cherrling.cn |
| 企业名称（O） | - |

查看详情

## 签发者信息

| | |
|---|---|
| CA名称（CN） | R3 |

查看详情

## 更多信息

| | |
|---|---|
| 序列号 | 4580E690C645B7162801AB23ADDB70E9615 |
| 根证书 | 否 |
| 证书级别 | DV |
| 颁发时间 | 2024-02-20 17:07:19 |
| 到期时间 | 2024-05-20 17:07:18 \| 35天后到期 |
| 加密算法 | RSA 2048 |
| 签名算法 | SHA256-RSA |
| 指纹 | SHA-1：AC1C7C6EAE3D5C63A30CCF066BF3A20AB46C292B<br>SHA-256：<br>323E1BA970B176EC74D37ACFE41F8060F4AC8AF31425576BF7F3ACE4058862A1 |
| 证书密钥用途 | 数字签名，密钥加密 |
| 扩展密钥用途 | 服务器认证，客户端认证 |
| OCSP 在线证书协议状态 | http://r3.o.lencr.org |
| CRL 分发点 | |
| 公钥 | 30820122300D06092A864886F70D0101010500038201 0F003082010A0282010100EB<br>7CB5EA8359F3EE9236188291B5F4839F74B79E158659C6FB69BAEA0AD7FE88D39B4A<br>57F474C493354F2467E2EB4352B626075607930C25A307123C6ECE3FB895534A154E<br>C0CF34CC5764FF090F3B376626F520AD64A2C906AA8FA729E9207B96435AF11E166<br>D0ACCDD11D64A9C7569D9385BF0331C370A68810783CD245D97812E723C0A2C3D<br>35457A58BED2D72807EDD18522D3D355C8D2A38914D2282C680FA84D8C0703DBB<br>DC631B9AA0EDC358E714A51BD1923178084D4E5FBFAABB4B8684CA691229F2F12B<br>64E34E586093313D71E21E7EDCCA228BB68104CE200746D481D3E3C2E2A319C3528 |

**主题信息**

| | |
|---|---|
| 域名（CN） | R3 |
| 备用域名（SAN） | R3 |
| 企业名称（O） | Let's Encrypt |

查看详情

**签发者信息**

| | |
|---|---|
| CA名称（CN） | ISRG Root X1 |

查看详情

**更多信息**

| | |
|---|---|
| 序列号 | 912B084ACF0C18A753F6D62E25A75F5A |
| 根证书 | 否 |
| 证书级别 | OV |
| 颁发时间 | 2020-09-04 08:00:00 |
| 到期时间 | 2025-09-16 00:00:00 \| 519天后到期 |
| 加密算法 | RSA 2048 |
| 签名算法 | SHA256-RSA |
| 指纹 | SHA-1：A053375BFE84E8B748782C7CEE15827A6AF5A405<br>SHA-256：<br>67ADD1166B020AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD |
| 证书密钥用途 | 数字签名，证书签名，CRL 签名 |
| 扩展密钥用途 | 客户端认证，服务器认证 |
| OCSP 在线证书协议状态 | |
| CRL 分发点 | http://x1.c.lencr.org/ |
| 公钥 | 30820122300D06092A864886F70D0101010500038201 0F003082010A0282010100BB<br>021528CCF6A094D30F12EC8D5592C3F882F199A67A4288A75D26AAB52BB9C54CB1<br>AF8E6BF975C8A3D70F4794145535578C9EA8A23919F5823C42A94E6EF53BC32EDB8<br>DC0B05CF35938E7EDCF69F05A0B1BBEC094242587FA3771B313E71CACE19BEFDBE4<br>3B45524596A9C153CE34C852EEB5AEED8FDE6070E2A554ABB66D0E97A540346B2BD |

**主题信息**

| | |
|---|---|
| 域名（CN） | ISRG Root X1 |
| 备用域名（SAN） | ISRG Root X1 |
| 企业名称（O） | Internet Security Research Group |

查看详情

**签发者信息**

| | |
|---|---|
| CA名称（CN） | ISRG Root X1 |

查看详情

**更多信息**

| | |
|---|---|
| 序列号 | 8210CFB0D240E3594463E0BB63828B00 |
| 根证书 | 是 |
| 证书级别 | OV |
| 颁发时间 | 2015-06-04 19:04:38 |
| 到期时间 | 2035-06-04 19:04:38 \| 4068天后到期 |
| 加密算法 | RSA 4096 |
| 签名算法 | SHA256-RSA |
| 指纹 | SHA-1：CABD2A79A1076A31F21D253635CB039D4329A5E8<br>SHA-256：<br>96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6 |
| 证书密钥用途 | 证书签名，CRL 签名 |
| 扩展密钥用途 | |
| OCSP 在线证书协议状态 | |
| CRL 分发点 | |
| 公钥 | 30820222300D06092A864886F70D01010105000382020F003082020A0282020100AD<br>E82473F41437F39B9E2B57281C87BEDCB7DF38908C6E3CE657A078F775C2A2FEF56A<br>6EF6004F28DBDE68866C4493B6B163FD14126BBF1FD2EA319B217ED1333CBA48F5D<br>D79DFB3B8FF12F1219A4BC18A8671694A66666C8F7E3C70BFAD292206F3E4C0E680 |

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

```
TLSv1.2          389 Client Hello (SNI=gchat.qpic.cn)
TLSv1.2         1474 Server Hello
TLSv1.2         1474 Certificate
TLSv1.2           78 Server Hello Done
TLSv1.2          392 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
TLSv1.2          332 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
TLSv1.2          517 Application Data
```

ClientHello

客户端申请的密钥交换模式：

```
Extension: psk_key_exchange_modes (len=2)
    Type: psk_key_exchange_modes (45)
    Length: 2
    PSK Key Exchange Modes Length: 1
    PSK Key Exchange Mode: PSK with (EC)DHE key establishment (psk_dhe_ke) (1)
```

客户端支持的椭圆曲线组：

```
Extension: supported_groups (len=12)
    Type: supported_groups (10)
    Length: 12
    Supported Groups List Length: 10
  Supported Groups (5 groups)
      Supported Group: x25519 (0x001d)
      Supported Group: secp256r1 (0x0017)
      Supported Group: x448 (0x001e)
      Supported Group: secp521r1 (0x0019)
      Supported Group: secp384r1 (0x0018)
```

客户端支持的签名算法：

```
Extension: signature_algorithms (len=48)
    Type: signature_algorithms (13)
    Length: 48
    Signature Hash Algorithms Length: 46
  Signature Hash Algorithms (23 algorithms)
    > Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
    > Signature Algorithm: ecdsa_secp384r1_sha384 (0x0503)
    > Signature Algorithm: ecdsa_secp521r1_sha512 (0x0603)
    > Signature Algorithm: ed25519 (0x0807)
    > Signature Algorithm: ed448 (0x0808)
    > Signature Algorithm: rsa_pss_pss_sha256 (0x0809)
    > Signature Algorithm: rsa_pss_pss_sha384 (0x080a)
    > Signature Algorithm: rsa_pss_pss_sha512 (0x080b)
    > Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
    > Signature Algorithm: rsa_pss_rsae_sha384 (0x0805)
    > Signature Algorithm: rsa_pss_rsae_sha512 (0x0806)
    > Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
    > Signature Algorithm: rsa_pkcs1_sha384 (0x0501)
    > Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
    > Signature Algorithm: SHA224 ECDSA (0x0303)
    > Signature Algorithm: ecdsa_sha1 (0x0203)
    > Signature Algorithm: SHA224 RSA (0x0301)
```

客户端共享的公钥

```
Extension: key_share (len=38) x25519
    Type: key_share (51)
    Length: 38
  Key Share extension
      Client Key Share Length: 36
    Key Share Entry: Group: x25519, Key Exchange length: 32
        Group: x25519 (29)
        Key Exchange Length: 32
        Key Exchange: bc5b1777c1f3b5b0ac0389fdbe990194e1fe53909b42229f06d404b1168d6c69
```

Server hello:

服务器端发送公钥给客户端

```
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 57
  Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 53
      Version: TLS 1.2 (0x0303)
    Random: c8e280d2841012ab1da9292ddf18cd8be0726d89be0811379ae564e0c604f252
        GMT Unix Time: Oct 19, 2076 06:55:14.000000000 中国标准时间
        Random Bytes: 841012ab1da9292ddf18cd8be0726d89be0811379ae564e0c604f252
      Session ID Length: 0
      Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
      Compression Method: null (0)
      Extensions Length: 13
    Extension: server_name (len=0)
        Type: server_name (0)
        Length: 0
    Extension: renegotiation_info (len=1)
        Type: renegotiation_info (65281)
        Length: 1
      Renegotiation Info extension
    Extension: session_ticket (len=0)
        Type: session_ticket (35)
        Length: 0
        Session Ticket: <MISSING>
```

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：

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4128
    Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4124
        Certificates Length: 4121
      Certificates (4121 bytes)
          Certificate Length: 2056
        Certificate [truncated]: 30820804308206eca003020102020c7da22277595a32bcb13e3c91300d06092a864886f70d01010b050030663
          Certificate Length: 1167
        Certificate [truncated]: 3082048b30820373a003020102020e4707b1019a0c57ad39b3e17da9f9300d06092a864886f70d01010b05003
          Certificate Length: 889
        Certificate [truncated]: 308203753082025da003020102020b04000000000001154b5ac394300d06092a864886f70d01010505003057310
```

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：

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 262
    Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 258
      RSA Encrypted PreMaster Secret
        Encrypted PreMaster length: 256
        Encrypted PreMaster [truncated]: 9e89039d98ffae8085de59e04cdc0b252fdc2b10d5e91b6b23933ae2794e85d6ba014ebe2f63b161c
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

服务器端改变加密模式，发送加密消息：

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 202
    Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 198
      TLS Session Ticket
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

TLS 握手结束，后续开始传送应用信息：

| | | |
|---|---|---|
| TLSv1.2 | 517 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1474 | Application Data |
| TLSv1.2 | 1053 | Application Data |
| TLSv1.2 | 120 | Application Data |
| TLSv1.2 | 384 | Application Data |
| TLSv1.2 | 116 | Application Data |

TLS1.3

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 1233 | 4.815404 | 192.168.2.2 | 76.76.21.21 | TCP | 66 | 2530 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 1261 | 4.924108 | 76.76.21.21 | 192.168.2.2 | TCP | 66 | 443 → 2530 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM |
| 1262 | 4.924198 | 192.168.2.2 | 76.76.21.21 | TCP | 54 | 2530 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0 |
| 1263 | 4.924316 | 192.168.2.2 | 76.76.21.21 | TLSv1.3 | 738 | Client Hello (SNI=cherrling.cn) |
| 1264 | 4.925839 | 192.168.2.2 | 76.76.21.21 | TCP | 54 | [TCP Retransmission] 2461 → 443 [FIN, ACK] Seq=1211 Ack=4083 Win=262656 Len=0 |
| 1267 | 4.943121 | 76.76.21.21 | 192.168.2.2 | TCP | 60 | 443 → 2461 [FIN, ACK] Seq=4083 Ack=1212 Win=135424 Len=0 |
| 1268 | 4.943156 | 192.168.2.2 | 76.76.21.21 | TCP | 54 | 2461 → 443 [ACK] Seq=1212 Ack=4084 Win=262656 Len=0 |
| 1312 | 5.048106 | 76.76.21.21 | 192.168.2.2 | TCP | 60 | 443 → 2530 [ACK] Seq=1 Ack=685 Win=133888 Len=0 |
| 1362 | 5.254609 | 76.76.21.21 | 192.168.2.2 | TLSv1.3 | 432 | Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data |
| 1363 | 5.255516 | 192.168.2.2 | 76.76.21.21 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |
| 1364 | 5.255619 | 192.168.2.2 | 76.76.21.21 | TLSv1.3 | 146 | Application Data |
| 1365 | 5.255684 | 192.168.2.2 | 76.76.21.21 | TLSv1.3 | 451 | Application Data |
| 1406 | 5.368087 | 76.76.21.21 | 192.168.2.2 | TLSv1.3 | 115 | Application Data |
| 1407 | 5.368332 | 192.168.2.2 | 76.76.21.21 | TLSv1.3 | 85 | Application Data |
| 1408 | 5.368428 | 76.76.21.21 | 192.168.2.2 | TLSv1.3 | 85 | [TCP Previous segment not captured] , Application Data |
| 1409 | 5.368444 | 192.168.2.2 | 76.76.21.21 | TCP | 66 | [TCP Dup ACK 1407#1] 2530 → 443 [ACK] Seq=1269 Ack=440 Win=262656 Len=0 SLE=475 SRE=506 |
| 1412 | 5.371458 | 76.76.21.21 | 192.168.2.2 | TLSv1.3 | 202 | Application Data |
| 1413 | 5.371476 | 192.168.2.2 | 76.76.21.21 | TCP | 66 | [TCP Dup ACK 1407#2] 2530 → 443 [ACK] Seq=1269 Ack=440 Win=262656 Len=0 SLE=475 SRE=654 |
| 1414 | 5.371680 | 76.76.21.21 | 192.168.2.2 | TLSv1.3 | 85 | Application Data |
| 1415 | 5.371687 | 192.168.2.2 | 76.76.21.21 | TCP | 66 | [TCP Dup ACK 1407#3] 2530 → 443 [ACK] Seq=1269 Ack=440 Win=262656 Len=0 SLE=475 SRE=685 |
| 1429 | 5.479118 | 76.76.21.21 | 192.168.2.2 | TCP | 89 | [TCP Out-Of-Order] 443 → 2530 [PSH, ACK] Seq=440 Ack=1269 Win=136704 Len=35 |
| 1430 | 5.479168 | 192.168.2.2 | 76.76.21.21 | TCP | 54 | 2530 → 443 [ACK] Seq=1269 Ack=685 Win=262400 Len=0 |
| 1431 | 5.486488 | 192.168.2.2 | 76.76.21.21 | TLSv1.3 | 142 | Application Data |
| 1500 | 5.710355 | 76.76.21.21 | 192.168.2.2 | TLSv1.3 | 85 | [TCP Previous segment not captured] , Application Data |
| 1501 | 5.710391 | 192.168.2.2 | 76.76.21.21 | TCP | 66 | [TCP Dup ACK 1430#1] 2530 → 443 [ACK] Seq=1357 Ack=685 Win=262400 Len=0 SLE=750 SRE=781 |
| 1612 | 6.144896 | 76.76.21.21 | 192.168.2.2 | TCP | 119 | [TCP Retransmission] 443 → 2530 [PSH, ACK] Seq=685 Ack=1357 Win=136704 Len=65 |
| 1613 | 6.144917 | 192.168.2.2 | 76.76.21.21 | TCP | 54 | 2530 → 443 [ACK] Seq=1357 Ack=781 Win=262400 Len=0 |
| 2453 | 21.154065 | 192.168.2.2 | 76.76.21.21 | TCP | 55 | [TCP Keep-Alive] 2530 → 443 [ACK] Seq=1356 Ack=781 Win=262400 Len=1 |
| 3324 | 36.160372 | 192.168.2.2 | 76.76.21.21 | TCP | 55 | [TCP Keep-Alive] 2530 → 443 [ACK] Seq=1356 Ack=781 Win=262400 Len=1 |

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)

```
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 679
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 675
        Version: TLS 1.2 (0x0303)
        Random: f91657d875167ff4543479e716d7bab6adc5e46f4cfe4f79fbd6729fff9e926f
        Session ID Length: 32
        Session ID: 21f58171544eb8bbb0ad9369fb5a7d19c29f05033f390347af236500deae8b50
        Cipher Suites Length: 32
        Cipher Suites (16 suites)
        Compression Methods Length: 1
        Compression Methods (1 method)
        Extensions Length: 570
        Extension: Reserved (GREASE) (len=0)
        Extension: extended_master_secret (len=0)
        Extension: renegotiation_info (len=1)
        Extension: status_request (len=5)
        Extension: ec_point_formats (len=2)
        Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
        Extension: psk_key_exchange_modes (len=2)
        Extension: signed_certificate_timestamp (len=0)
        Extension: signature_algorithms (len=18)
        Extension: compress_certificate (len=3)
        Extension: encrypted_client_hello (len=218)
        Extension: application_settings (len=5)
        Extension: session_ticket (len=0)
        Extension: application_layer_protocol_negotiation (len=14)
        Extension: supported_groups (len=10)
        Extension: key_share (len=43) x25519
        Extension: server_name (len=17) name=cherrling.cn
        Extension: Reserved (GREASE) (len=1)
        Extension: pre_shared_key (len=148)
        [JA4: t13d1517h2_8daaf6152771_b0da82dd1658]
        [JA4_r: t13d1517h2_002f,0035,009c,009d,1301,1302,1303,c013,c014,c02b,c02c,c02f,c030,cca8,cca9_0005,000a,000b,000d,0012,0017,001b,0023,0029,002b,002d,0033,4469,fe0
        [JA3 Fullstring: 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,23-65281-5-11-43-45-18-13-27-65037-17513-35-16-10-51-0-41,29-23-
        [JA3: 16355f4af50757cd656f3177211a3527]
```

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

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_128_GCM.

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

```
Extension: key_share (len=36) x25519
    Type: key_share (51)
    Length: 36
  Key Share extension
    Key Share Entry: Group: x25519, Key Exchange length: 32
        Group: x25519 (29)
        Key Exchange Length: 32
        Key Exchange: 1593f32882afb5cee7129490eba09f9e66fa3f6074ff55219add2d2627baed12
```

```
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
```

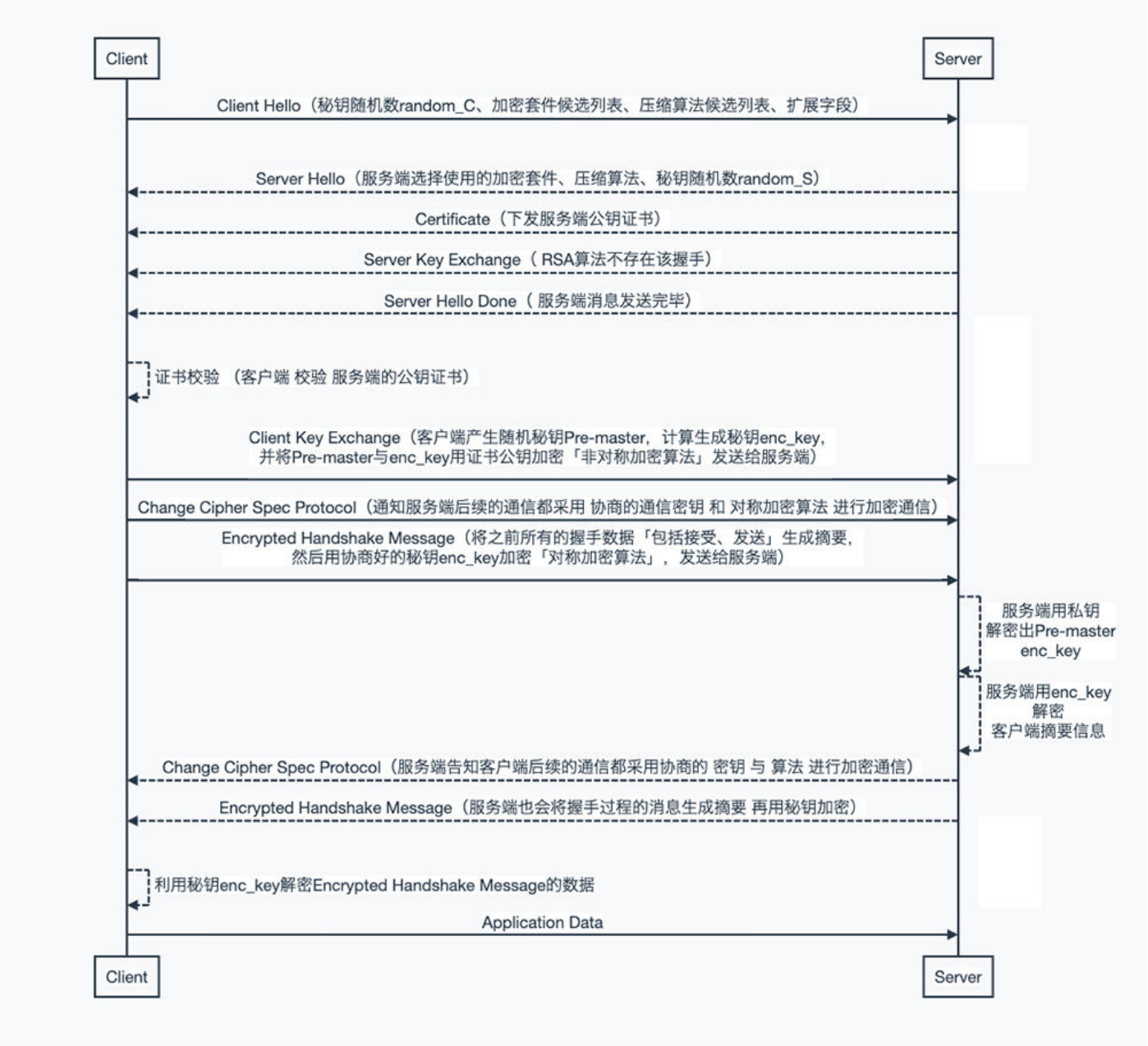
```
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 128
  Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 124
      Version: TLS 1.2 (0x0303)
      Random: 21f05bda927a3fa769498d15a88b75113767ab8a394cd732a75d640e587c86e1
      Session ID Length: 32
      Session ID: 21f58171544eb8bbb0ad9369fb5a7d19c29f05033f390347af236500deae8b50
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Compression Method: null (0)
      Extensions Length: 52
    > Extension: supported_versions (len=2) TLS 1.3
    > Extension: key_share (len=36) x25519
    > Extension: pre_shared_key (len=2)
      [JA3S Fullstring: 771,4865,43-51-41]
      [JA3S: fcb2d4d0991292272fcb1e464eedfd43]
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 32
    Encrypted Application Data: 8885a6bb039e97c1cb9295bc38ba959f46e10fd1cce494894cdbb9d05e7108cc
    [Application Data Protocol: Hypertext Transfer Protocol]
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 53
    Encrypted Application Data: 7ccd9fe484e192ab0414c8de5b543254d21cad871115b15bab919621c04bb104ede157c420a19b56257875e25ea31c290461801394
    [Application Data Protocol: Hypertext Transfer Protocol]
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 139
```

密钥交换：

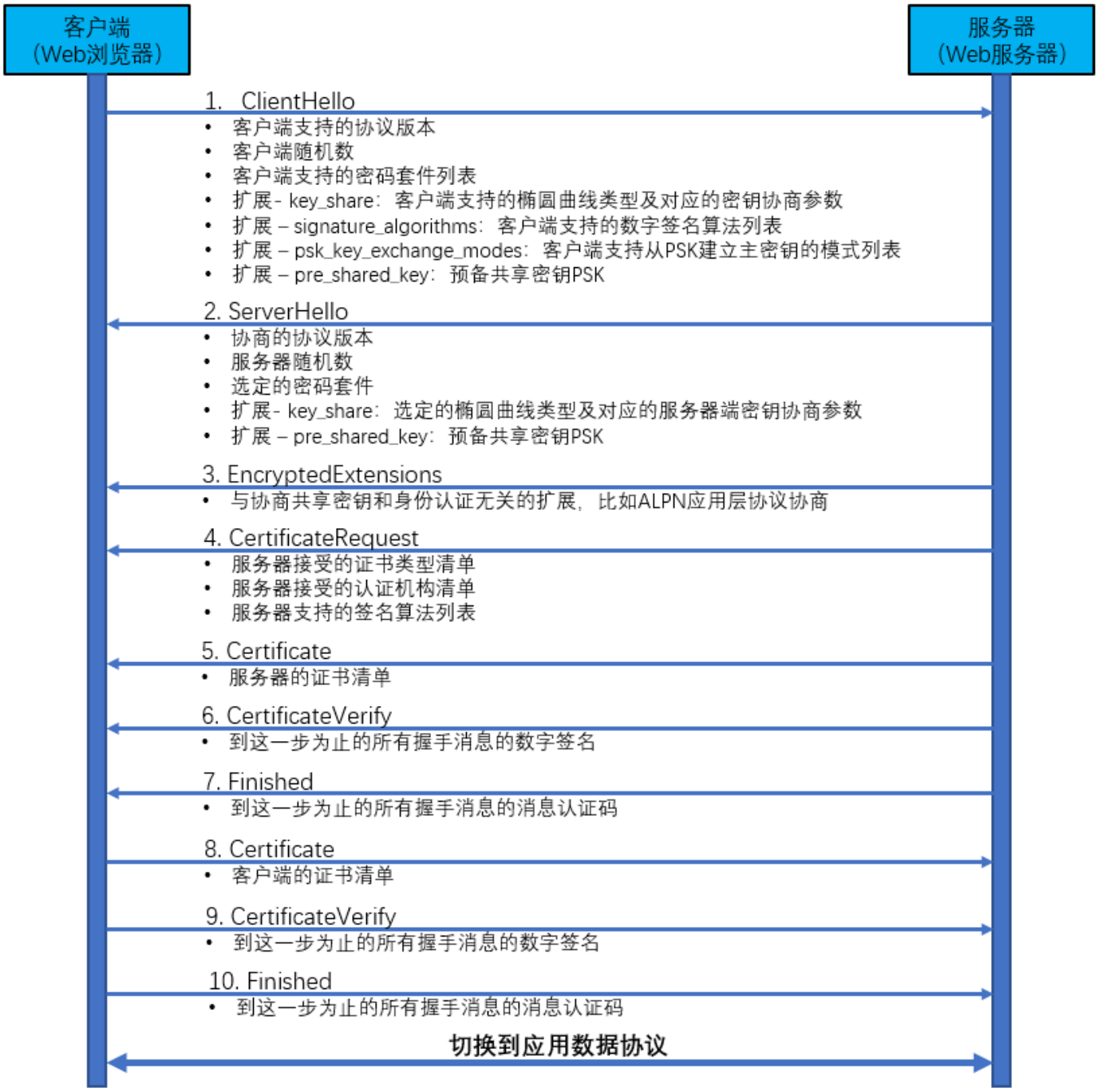
```
> Frame 1363: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{C5D42BE8-CCCB-4FB0-A208-4551FABA57C6}, id 0
> Ethernet II, Src: MicroStarINT_c8:6f:02 (04:7c:16:c8:6f:02), Dst: RealtekSemic_6b:bb:f8 (00:e0:4c:6b:bb:f8)
> Internet Protocol Version 4, Src: 192.168.2.2, Dst: 76.76.21.21
Transmission Control Protocol, Src Port: 2530, Dst Port: 443, Seq: 685, Ack: 379, Len: 64
    Source Port: 2530
    Destination Port: 443
    [Stream index: 61]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 64]
    Sequence Number: 685    (relative sequence number)
    Sequence Number (raw): 1819466426
    [Next Sequence Number: 749    (relative sequence number)]
    Acknowledgment Number: 379    (relative ack number)
    Acknowledgment number (raw): 326592263
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0xa9d6 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (64 bytes)
Transport Layer Security
  TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 53
      Encrypted Application Data: a905c64c1b0260fc3bfc33da1e1730f8586c97f7757339ef7a9218e4d3ccd5d626a17788303482e7dc101da07c06ee218cdc089687
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 63
    Encrypted Application Data: 424916a88ee631f319815e4d2bbdd47857b9b80b5f3ba2c1c1e47259784b8fa3f75c51be6215338fed2a8d10a05620
    [Application Data Protocol: Hypertext Transfer Protocol]
```

TLS1.2 流程图：



TLS1.3 流程图：




**TLS 1.3 完整握手过程**