

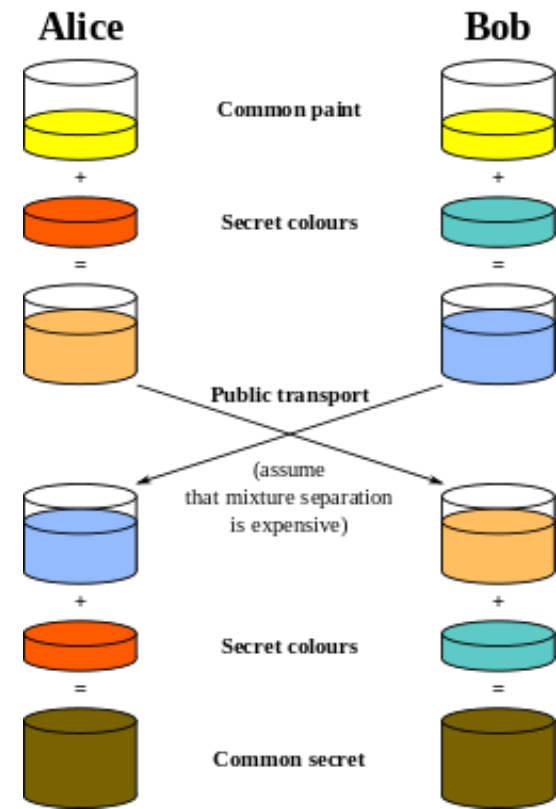
# Diffie- Hellman 密钥交换算法

DH算法属于公钥加密算法

公钥加密算法加解密复杂，花费时间久

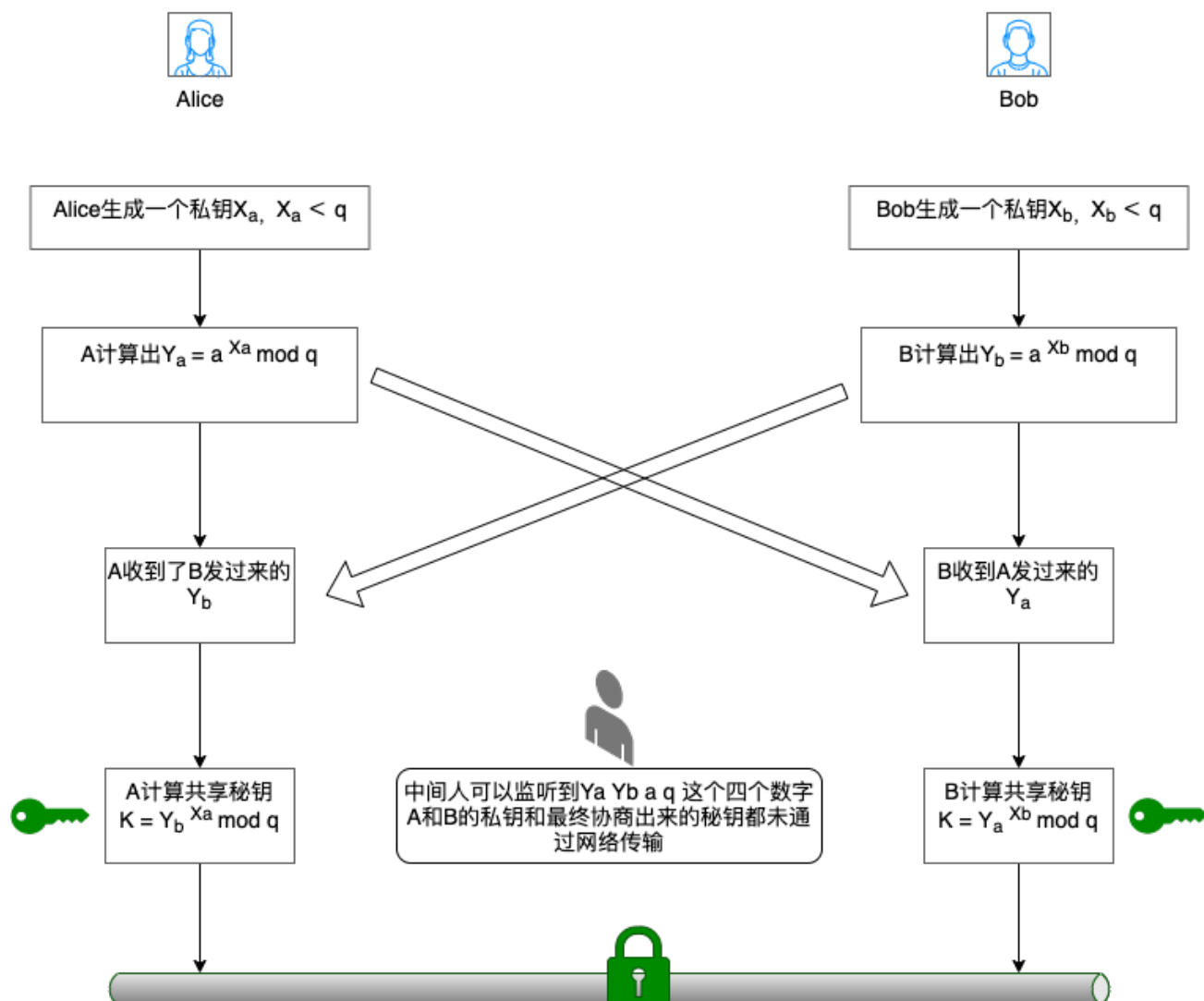
加解密数据时使用对称密码算法，密钥管理使用公钥密码技术

其解决问题的主要思想可以用下图来解释



具体交换的过程如下：

Alice和Bob共享一个素数 $q$ ，以及整数 $a(a < q)$ ，且 $a$ 是 $q$ 的原根。



1. Alice和Bob协商一个有限循环群 $G$ 和它的一个生成元 $g$ ，一个大素数 $p$ ；
2. Alice生成一个随机数 $a$ ，计算 $A = g^a \bmod p$ ，将 $A$ 发送给Bob；
3. Bob生成一个随机数 $b$ ，计算 $B = g^b \bmod p$ ，将 $B$ 发送给Alice；
4. Alice计算 $K = B^a \bmod p = (g^b)^a \bmod p$ ，得到共享密钥 $K$ ；
5. Bob计算 $K = A^b \bmod p = (g^a)^b \bmod p$ ，得到共享密钥 $K$ ；

$(g^b)^a = (g^a)^b$  因为群是乘法交换的，涉及到数论及代数的内容。Alice和Bob同时协商出 $K$ ，作为共享密钥。

# TLS握手过程

## 1.Client Hello

- TLS Version, TLS的版本号
- Cipher Suite, 客户端支持的加密套件列表; 加密算法密钥长度等等
  - Client Random, 随机数,

5	2.195834	45.113.192.102	192.168.31.155	TCP	78	443 → 56981 [SYN, ACK] Seq=0 Ack=
6	2.195889	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=1 Ack=1 Win
7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286	Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=1 Ack=233 W
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506	Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506	443 → 56981 [ACK] Seq=1453 Ack=23
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383	Certificate, Server Key Exchange,
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383	[TCP Retransmission] 443 → 56981
13	2.504306	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=233 Ack=423
14	2.504372	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#1] 56981 → 443 [A
15	2.508950	192.168.31.155	45.113.192.102	TCP	54	[TCP Window Update] 56981 → 443 [
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180	Client Key Exchange, Change Cipe
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506	[TCP Out-Of-Order] 443 → 56981 [A
18	2.652497	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#2] 56981 → 443 [A
19	2.751516	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4234 Ack=35
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105	Change Cipher Spec, Encrypted Han
21	2.751604	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=359 Ack=428
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160	Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90	Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66	63655 → 5223 [FIN, ACK] Seq=59 Ac
25	3.002772	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4285 Ack=46

> Frame 7: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface en0, id 0

> Ethernet II, Src: Apple\_d5:01:72 (38:f9:d3:d5:01:72), Dst: BeijingX\_d7:1b:ed (28:d1:27:d7:1b:ed)

> Internet Protocol Version 4, Src: 192.168.31.155, Dst: 45.113.192.102

> Transmission Control Protocol, Src Port: 56981, Dst Port: 443, Seq: 1, Ack: 1, Len: 232

> Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 227
    - ▼ Handshake Protocol: Client Hello
      - Handshake Type: Client Hello (1)
      - Length: 223
        - Version: TLS 1.2 (0x0303)
        - > Random: d81c8256bdd1505c8a2205d2fb76086a1c38c85f5ff09e81...
        - Session ID Length: 0
        - Cipher Suites Length: 92
          - ▼ Cipher Suites (46 suites)
            - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
            - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)
            - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)
            - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)
            - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)
            - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)
            - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)

0000 28 d1 27 d7 1b ed 38 f9 d3 d5 01 72 08 00 45 00 (.....8.....r..E..

0010 01 10 00 00 40 00 40 06 6b cd c0 a8 1f 9b 2d 71 .....@.@.k.....q

0020 c0 66 de 95 01 bb 9e f7 36 25 b4 cc 32 f4 50 18 .f.....6%.2.P.

0030 10 00 58 5f 00 00 16 03 01 00 e3 01 00 00 df 03 ..X.....

## 2. Server Hello

- TLS Version
- 服务端选中的加密组件, 从客户端发送过来的加密套件中选择其中一个

- Server Random, 服务端生成的随机数

8	2.504203	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=1 Ack=
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506	Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506	443 → 56981 [ACK] Seq=1453 A
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383	Certificate, Server Key Exch
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383	[TCP Retransmission] 443 → 5
13	2.504306	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=233 Ac
14	2.504372	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#1] 56981 → 4
15	2.508950	192.168.31.155	45.113.192.102	TCP	54	[TCP Window Update] 56981 →
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180	Client Key Exchange, Change
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506	[TCP Out-Of-Order] 443 → 569
18	2.652497	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#2] 56981 → 4
19	2.751516	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4234 A
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105	Change Cipher Spec, Encrypte
21	2.751604	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=359 Ac
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160	Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90	Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66	63655 → 5223 [FIN, ACK] Seq=
25	3.002772	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4285 A

Frame 9: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface en0, id 0

Ethernet II, Src: BeijingX\_d7:1b:ed (28:d1:27:d7:1b:ed), Dst: Apple\_d5:01:72 (38:f9:d3:d5:01:72)

Internet Protocol Version 4, Src: 45.113.192.102, Dst: 192.168.31.155

Transmission Control Protocol, Src Port: 443, Dst Port: 56981, Seq: 1, Ack: 233, Len: 1452

Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 102

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 98

Version: TLS 1.2 (0x0303)

➤ Random: 622d9fb1fb80f84c55367a734f1825ada4ebb8895879a58c...

Session ID Length: 32

Session ID: 5e267a2863a19c29e9a71ebc11b91b2f54859f3d2f73cda6...

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Compression Method: null (0)

Extensions Length: 26

➤ Extension: renegotiation\_info (len=1)

➤ Extension: application\_layer\_protocol\_negotiation (len=11)

➤ Extension: ec\_point\_formats (len=2)

### 3. Certificate

- 服务器的公钥证书 (被CA签过名的)

7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286 Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=0
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506 Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506 443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a reassembled TCP segment (SSE=1)]
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383 Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383 [TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Len=13
13	2.504306	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SLE=29
15	2.508950	192.168.31.155	45.113.192.102	TCP	54 [TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506 [TCP Out-Of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SLE=1
19	2.751516	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160 Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90 Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66 63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885325 TSecr=16
25	3.002772	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

[3 Reassembled TCP Segments (3779 bytes): #9(1345), #10(1452), #11(982)]

Transport Layer Security

- TLV1.2 Record Layer: Handshake Protocol: Certificate
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 3774
  - Handshake Protocol: Certificate
    - Handshake Type: Certificate (11)
    - Length: 3770
    - Certificates Length: 3767
    - Certificates (3767 bytes)
      - Certificate Length: 2628
        - Certificate: 308204030820928a003020102020c7239d9c9beb5c9cd79... (id-at-commonName=baidu.com,id-at-organizationName=Beijing Baidu Netcom Science Techno
        - > signedCertificate
        - > algorithmIdentifier (sha256WithRSAEncryption)
        - Padding: 0
        - encrypted: 398a004992481658de3e9cce83391bb1ac9a95f956ff7c2d...
      - Certificate Length: 1133
        - Certificate: 3082046930820351a003020102020b04000000001444ef0... (id-at-commonName=GlobalSign Organization Validation CA - SHA256,id-at-organizationName=
        - > signedCertificate
        - > algorithmIdentifier (sha256WithRSAEncryption)
        - Padding: 0
        - encrypted: 462aee5ebdae0160373111867174b64649c81016fe2f6223...

#### 4. Server Key Exchange

- Server Params, ECDHE算法需要用到

7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286 Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=0
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506 Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506 443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a reassembled TCP segment (SSE=1)]
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383 Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383 [TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Len=13
13	2.504306	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SLE=29
15	2.508950	192.168.31.155	45.113.192.102	TCP	54 [TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506 [TCP Out-Of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SLE=1
19	2.751516	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160 Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90 Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66 63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885325 TSecr=16
25	3.002772	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

Handshake Type: Certificate (11)

Length: 3770

Certificates Length: 3767

> Certificates (3767 bytes)

Transport Layer Security

- TLV1.2 Record Layer: Handshake Protocol: Server Key Exchange
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 333
  - Handshake Protocol: Server Key Exchange
    - Handshake Type: Server Key Exchange (12)
    - Length: 329
    - EC Diffie-Hellman Server Params
      - Curve Type: named\_curve (0x03)
      - Named Curve: secp256r1 (0x0017)
      - Pubkey Length: 65
      - Pubkey: 043c5537cdc1d99ba4f808bd0678d4ceb8009031f1793432...
      - > Signature Algorithm: rsa\_pkcs1\_sha512 (0x0601)
      - Signature Length: 256
      - Signature: 57bb38ab8bc88bf36ce9778fb21c82944f96a79b719fe497...
  - TLV1.2 Record Layer: Handshake Protocol: Server Hello Done
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 4

ECDHE是一种密钥交换算法

为了防止伪造，Server Params是经过服务器的私钥签名的

## 5. Server Hello Done

告诉客户端：协商部分结束

目前为止，客户端和服务端共享了

1. Client Random
2. Server Random
3. Server Params

并且，客户端已经得到了服务器给过来的证书（包含公钥），接下来客户端需要验证证书是否真实有效

7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286 Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=0
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506 Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506 443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a reassembled
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383 Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383 [TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Len=1329
13	2.504306	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SLE=2905 SRE=1
15	2.508950	192.168.31.155	45.113.192.102	TCP	54 [TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506 [TCP Out-of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SLE=1 SRE=1
19	2.751516	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160 Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90 Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66 63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885325 TSecr=1656934
25	3.002772	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

Frame 11: 1383 bytes on wire (11064 bits), 1383 bytes captured (11064 bits) on interface en0, id 0  
Ethernet II, Src: BeijingX\_d7:1b:ed (28:d1:27:d7:1b:ed), Dst: Apple\_d5:01:72 (38:f9:d3:d5:01:72)  
Internet Protocol Version 4, Src: 45.113.192.102, Dst: 192.168.31.155  
Transmission Control Protocol, Src Port: 443, Dst Port: 56981, Seq: 2905, Ack: 233, Len: 1329  
3 Reassembled TCP Segments (3779 bytes): #9(1345), #10(1452), #11(982)]  
Transport Layer Security  
TLSv1.2 Record Layer: Handshake Protocol: Certificate  
Content Type: Handshake (22)  
Version: TLS 1.2 (0x0303)  
Length: 3774  
Handshake Protocol: Certificate  
Handshake Type: Certificate (11)  
Length: 3770  
Certificates Length: 3767  
Certificates (3767 bytes)  
Transport Layer Security  
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange  
TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done  
Content Type: Handshake (22)  
Version: TLS 1.2 (0x0303)  
Length: 4  
Handshake Protocol: Server Hello Done  
Handshake Type: Server Hello Done (14)  
Length: 0

## 6. Client Key Exchange

- Client Params, ECDHE算法需要用到



7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286	Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=0
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506	Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506	443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a r
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383	Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383	[TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Le
13	2.504306	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SL
15	2.508950	192.168.31.155	45.113.192.102	TCP	54	[TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506	[TCP Out-Of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SL
19	2.751516	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160	Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90	Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66	63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885
25	3.002772	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

> Frame 16: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface en0, id 0  
 > Ethernet II, Src: Apple\_d5:01:72 (38:f9:d3:d5:01:72), Dst: Beijing\_X\_d7:1b:ed (28:d1:27:d7:1b:ed)  
 > Internet Protocol Version 4, Src: 192.168.31.155, Dst: 45.113.192.102  
 > Transmission Control Protocol, Src Port: 56981, Dst Port: 443, Seq: 233, Ack: 4234, Len: 126  
 > Transport Layer Security  
 > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange  
 Content Type: Handshake (22)  
 Version: TLS 1.2 (0x0303)  
 Length: 70  
 > Handshake Protocol: Client Key Exchange  
 Handshake Type: Client Key Exchange (16)  
 Length: 66  
 > EC Diffie-Hellman Client Params  
 Pubkey Length: 65  
 Pubkey: 04a336b0873158bc22bfa2ee124adcf4cd161fb51b1dde1b...  
 > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
 > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

到这一步，客户端和服务端都拥有了Server Params、Client Params；

客户端和服务端都可以使用ECDHE算法根据Server Params、Client Params计算出一个新的随机秘钥串  
Pre-master Secret

## 7. Change Cipher Spec

告知服务器之后的通信会采用计算出来的会话秘钥进行加密

7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286	Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=0
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506	Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506	443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a r
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383	Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383	[TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Le
13	2.504306	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SL
15	2.508950	192.168.31.155	45.113.192.102	TCP	54	[TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506	[TCP Out-Of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66	[TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SL
19	2.751516	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54	56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160	Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90	Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66	63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885325 TSec
25	3.002772	45.113.192.102	192.168.31.155	TCP	54	443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

Frame 16: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface en0, id 0  
 Ethernet II, Src: Apple\_d5:01:72 (38:f9:d3:d5:01:72), Dst: Beijing\_X\_d7:1b:ed (28:d1:27:d7:1b:ed)  
 Internet Protocol Version 4, Src: 192.168.31.155, Dst: 45.113.192.102  
 Transmission Control Protocol, Src Port: 56981, Dst Port: 443, Seq: 233, Ack: 4234, Len: 126  
 Transport Layer Security  
 > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange  
 > 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

## 8. Finished

1. 包括链接到这一步所有的报文的摘要值，加密之后发送给服务器
2. 这次握手是否成功要以服务器是否能够正确解密报文作为判断标准

7	2.205112	192.168.31.155	45.113.192.102	TLSv1.2	286 Client Hello
8	2.504203	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=0
9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506 Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506 443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383 Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383 [TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Len=1329
13	2.504306	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SLE=2905 SRE=4234
15	2.508950	192.168.31.155	45.113.192.102	TCP	54 [TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506 [TCP Out-Of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SLE=1 SRE=1453
19	2.751516	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160 Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90 Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66 63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885325 TSecr=1656934461
25	3.002772	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

Frame 16: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_d5:01:72 (38:f9:d3:d5:01:72), Dst: BeijingX\_d7:1b:ed (28:d1:27:d7:1b:ed)  
Internet Protocol Version 4, Src: 192.168.31.155, Dst: 45.113.192.102  
Transmission Control Protocol, Src Port: 56981, Dst Port: 443, Seq: 233, Ack: 4234, Len: 126  
Transport Layer Security  
> TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange  
> TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
> 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

## 9. Change Cipher Spec

## 10. Finished

1. 到此为止，客户端服务器都验证了加解密没有问题，握手正式结束
2. 后面开始传输加密的请求和响应

9	2.504204	45.113.192.102	192.168.31.155	TLSv1.2	1506 Server Hello
10	2.504204	45.113.192.102	192.168.31.155	TCP	1506 443 → 56981 [ACK] Seq=1453 Ack=233 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
11	2.504205	45.113.192.102	192.168.31.155	TLSv1.2	1383 Certificate, Server Key Exchange, Server Hello Done
12	2.504207	45.113.192.102	192.168.31.155	TCP	1383 [TCP Retransmission] 443 → 56981 [PSH, ACK] Seq=2905 Ack=233 Win=30336 Len=1329
13	2.504306	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0
14	2.504372	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#1] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=257856 Len=0 SLE=2905 SRE=4234
15	2.508950	192.168.31.155	45.113.192.102	TCP	54 [TCP Window Update] 56981 → 443 [ACK] Seq=233 Ack=4234 Win=262144 Len=0
16	2.511025	192.168.31.155	45.113.192.102	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.652446	45.113.192.102	192.168.31.155	TCP	1506 [TCP Out-Of-Order] 443 → 56981 [ACK] Seq=1 Ack=233 Win=30336 Len=1452
18	2.652497	192.168.31.155	45.113.192.102	TCP	66 [TCP Dup ACK 13#2] 56981 → 443 [ACK] Seq=359 Ack=4234 Win=262144 Len=0 SLE=1 SRE=1453
19	2.751516	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4234 Ack=359 Win=30336 Len=0
20	2.751517	45.113.192.102	192.168.31.155	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
21	2.751604	192.168.31.155	45.113.192.102	TCP	54 56981 → 443 [ACK] Seq=359 Ack=4285 Win=262080 Len=0
22	2.752275	192.168.31.155	45.113.192.102	TLSv1.2	160 Application Data
23	2.834310	192.168.31.155	17.57.145.165	TLSv1.2	90 Application Data
24	2.834647	192.168.31.155	17.57.145.165	TCP	66 63655 → 5223 [FIN, ACK] Seq=59 Ack=1 Win=2048 Len=0 TSval=1517885325 TSecr=1656934461
25	3.002772	45.113.192.102	192.168.31.155	TCP	54 443 → 56981 [ACK] Seq=4285 Ack=465 Win=30336 Len=0

> Frame 20: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface en0, id 0  
> Ethernet II, Src: BeijingX\_d7:1b:ed (28:d1:27:d7:1b:ed), Dst: Apple\_d5:01:72 (38:f9:d3:d5:01:72)  
> Internet Protocol Version 4, Src: 45.113.192.102, Dst: 192.168.31.155  
> Transmission Control Protocol, Src Port: 443, Dst Port: 56981, Seq: 4234, Ack: 359, Len: 51  
Transport Layer Security  
> 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