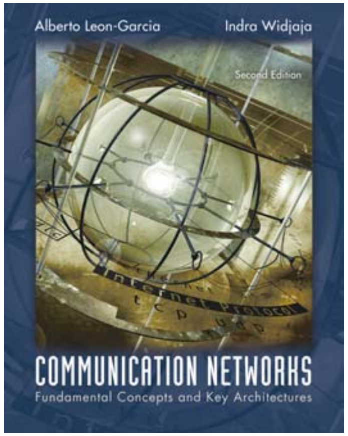
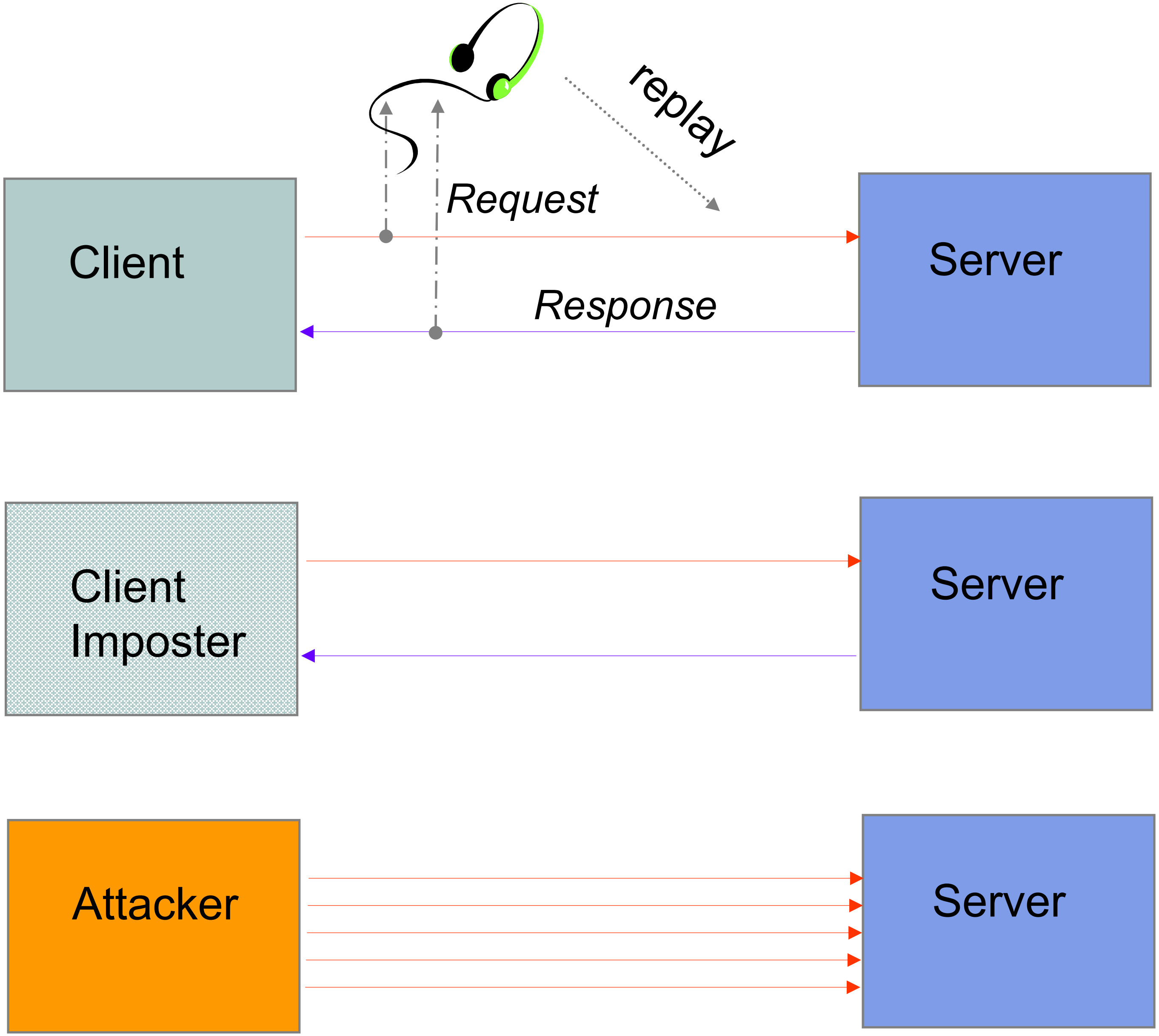
Chapter 11
Security Protocols



Chapter Figures



replay

Request

Client

Server

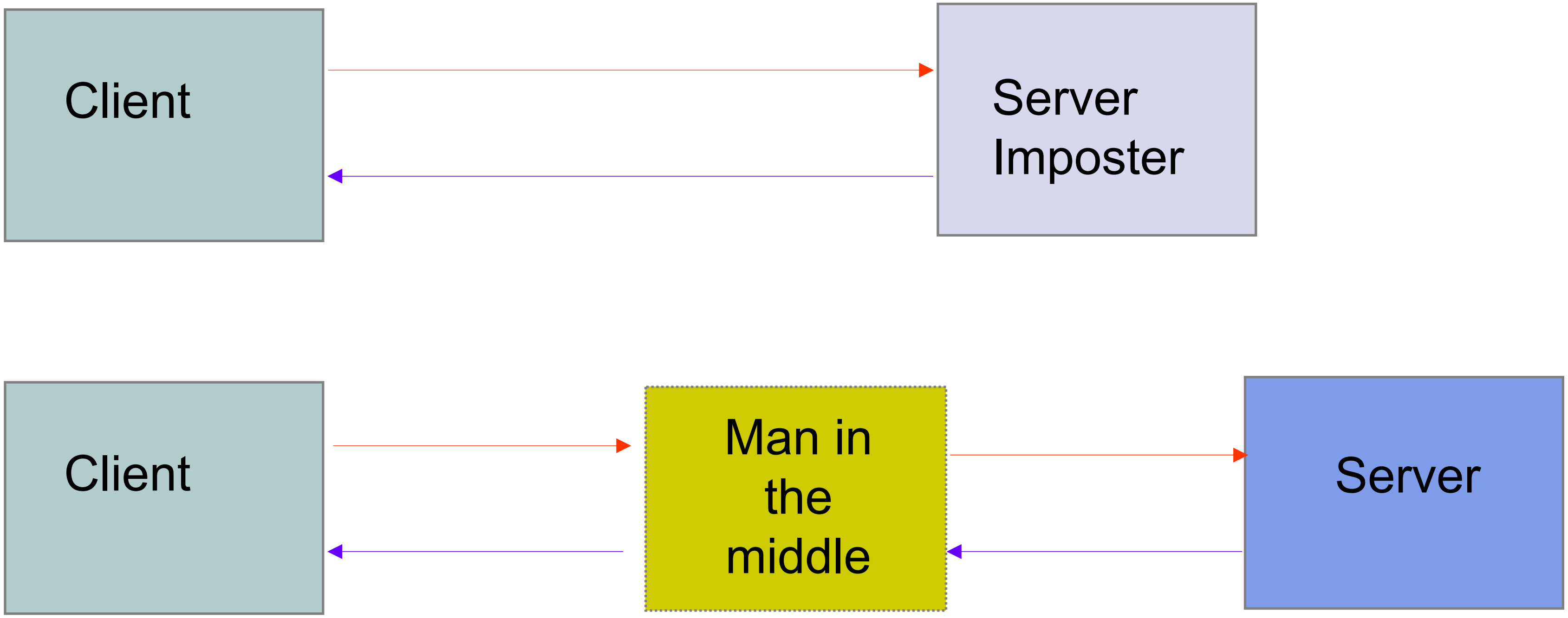
Response

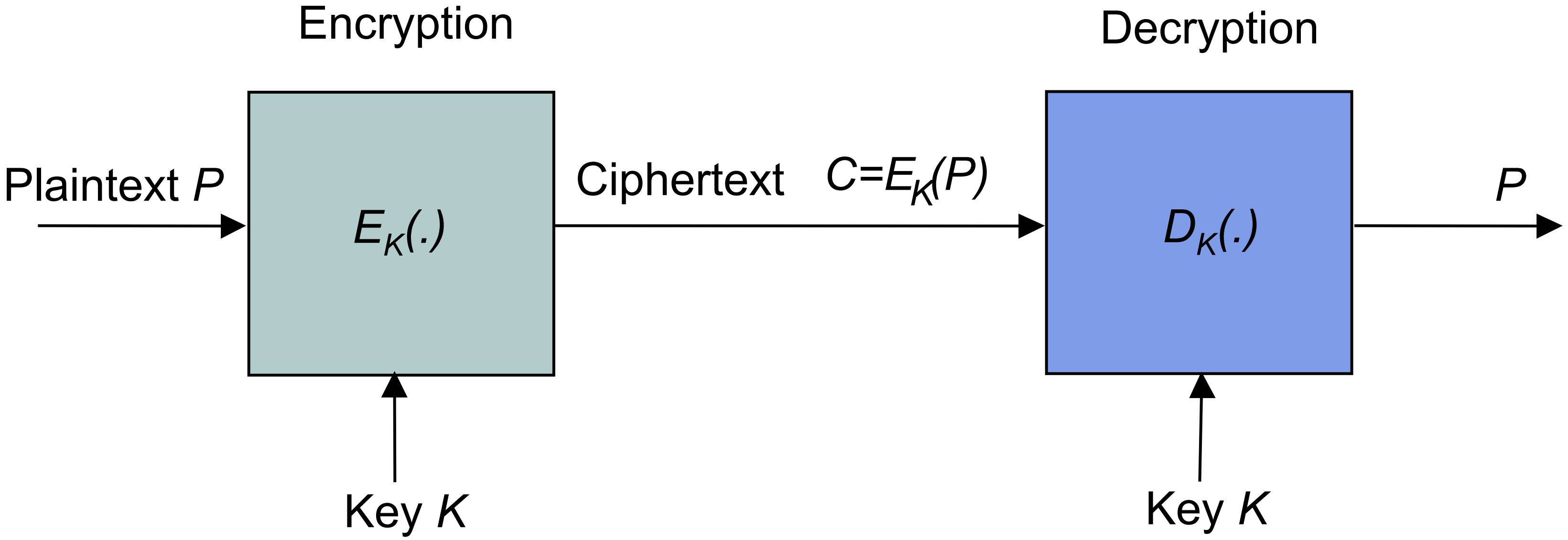
Client Imposter

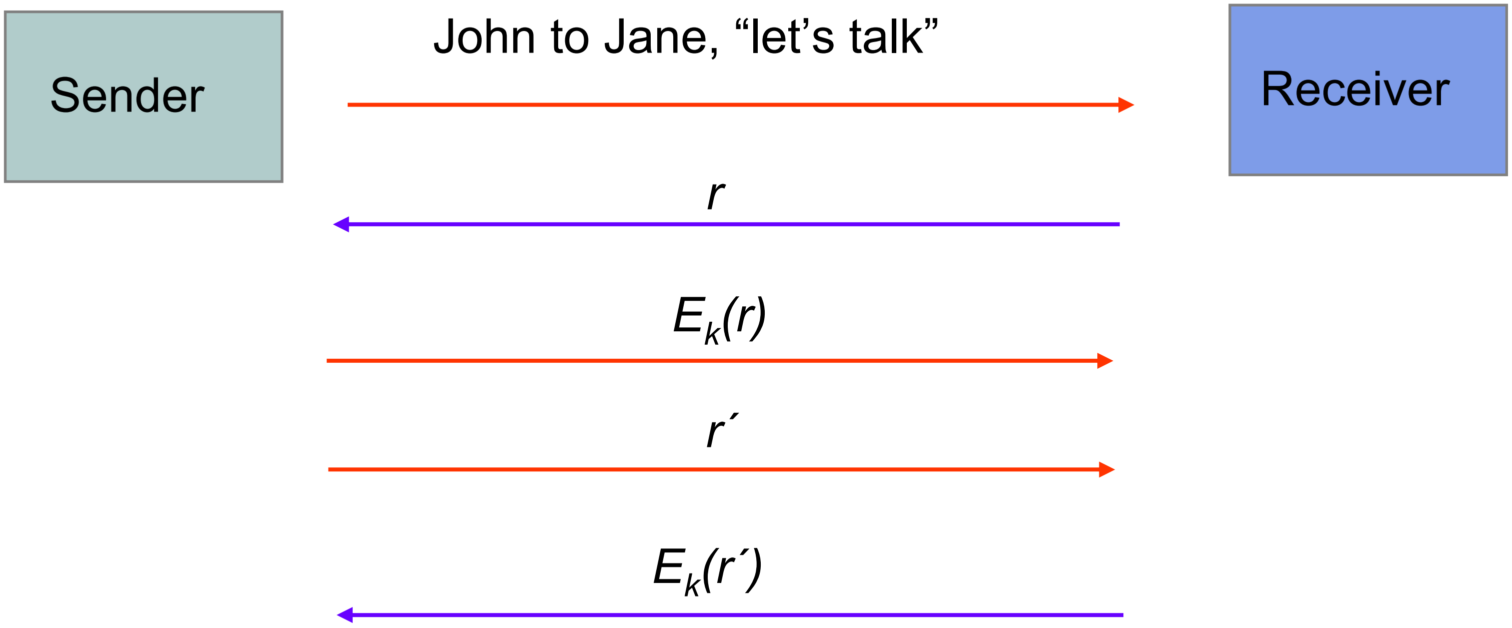
Server

Attacker

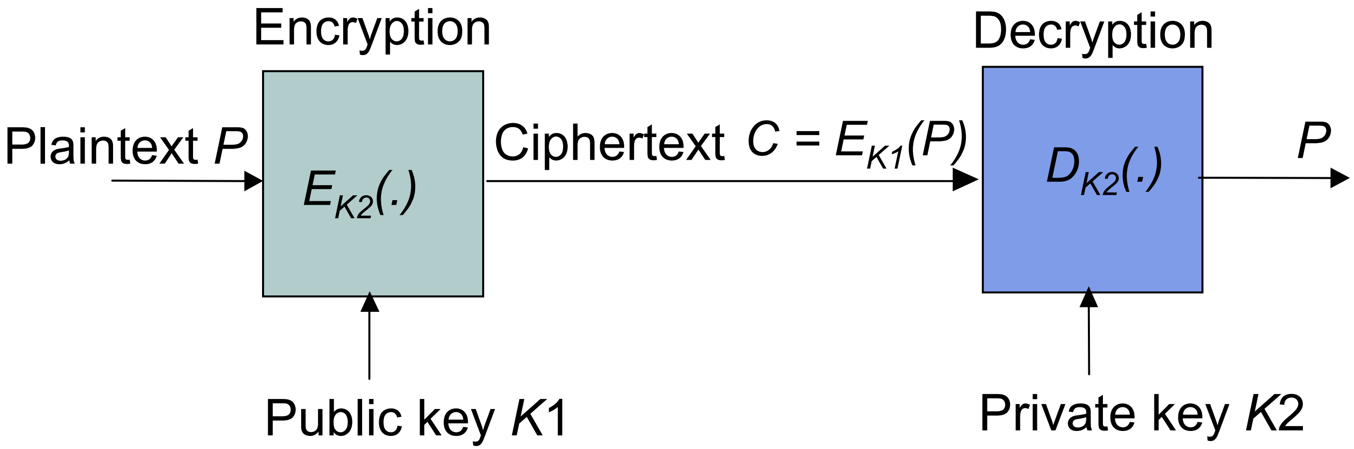
Server


Client
Server Imposter
Client
Man in the middle
Server


Encryption
Decryption
Plaintext *P*
$E_K(.)$
Ciphertext $C=E_K(P)$
$D_K(.)$
P
Key *K*
Key *K*



Sender
Receiver
John to Jane, “let’s talk”
r
$E_k(r)$
r'
$E_k(r')$



Encryption

Decryption

Plaintext P

$E_{K2}(.)$

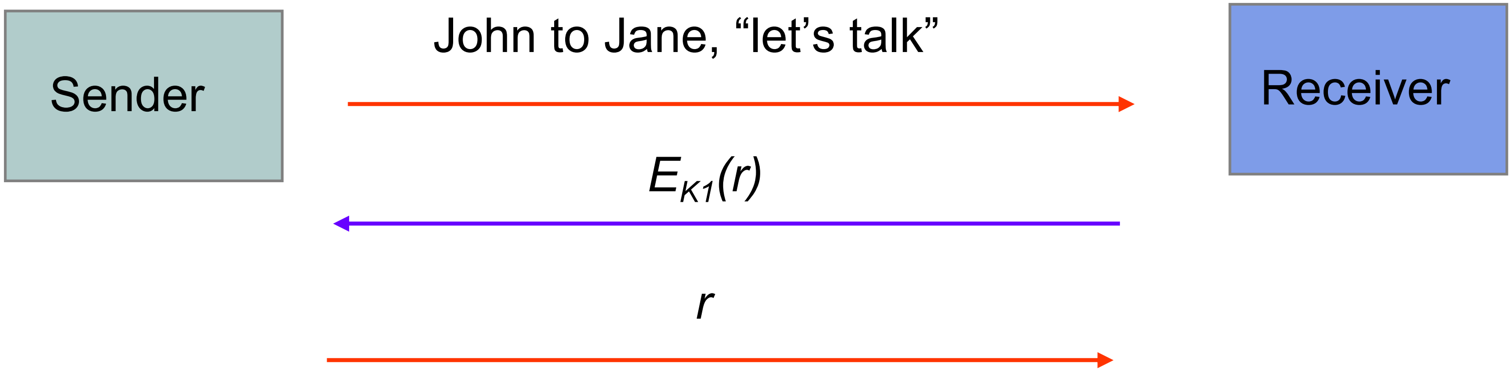
Ciphertext $C = E_{K1}(P)$

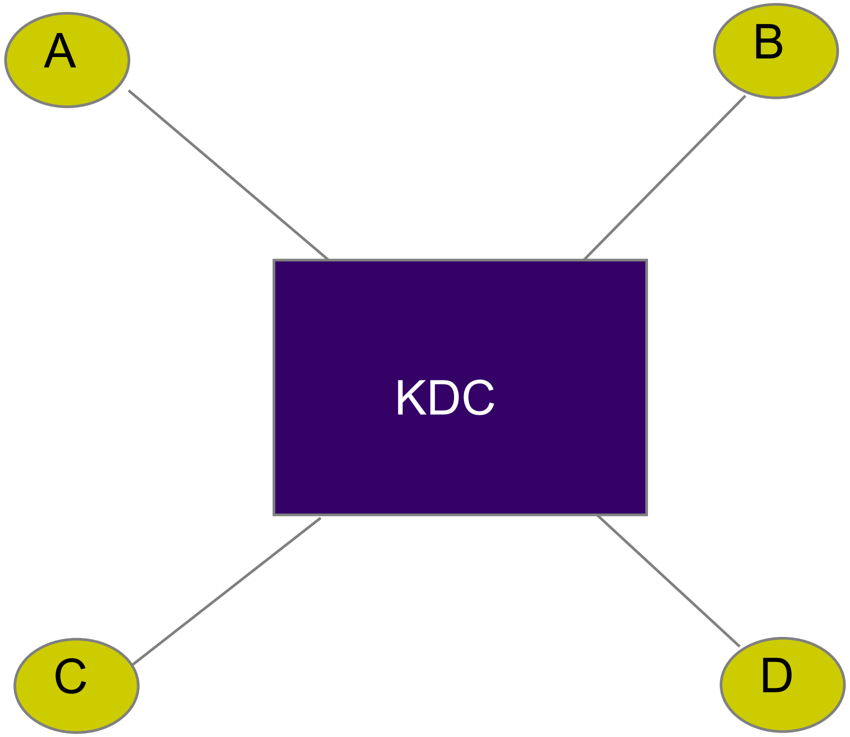
$D_{K2}(.)$

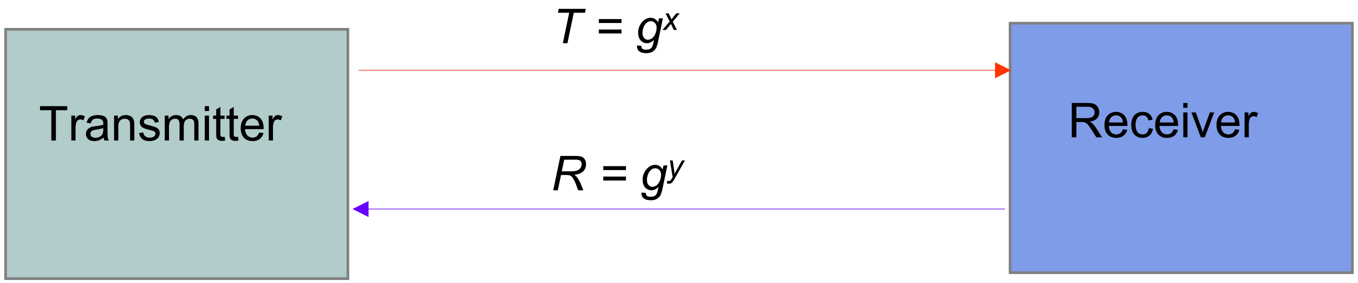
P

Public key $K1$

Private key $K2$

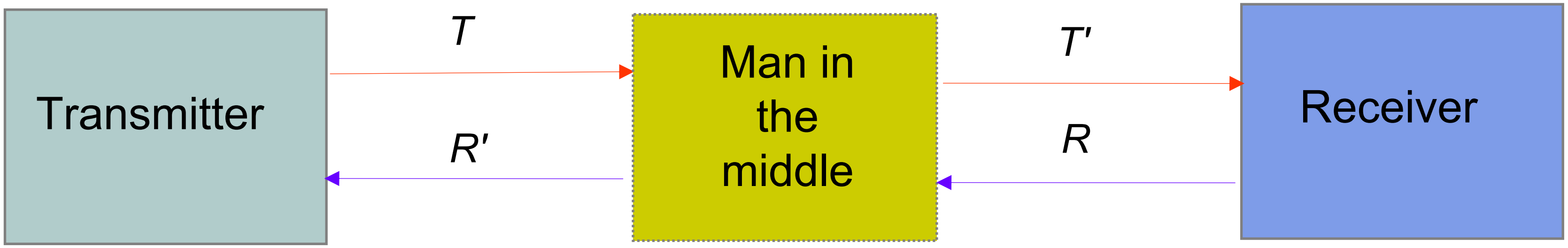

Sender
John to Jane, "let's talk"
Receiver
$E_{K1}(r)$
r


A
B
KDC
C
D



$$K = R^x \bmod p$$
$$= g^{xy} \bmod p$$

$$K = T^y \bmod p$$
$$= g^{xy} \bmod p$$



$K_1 = R'^{x}$

$= g^{xy'}$

$K_1 = T^{y'}$

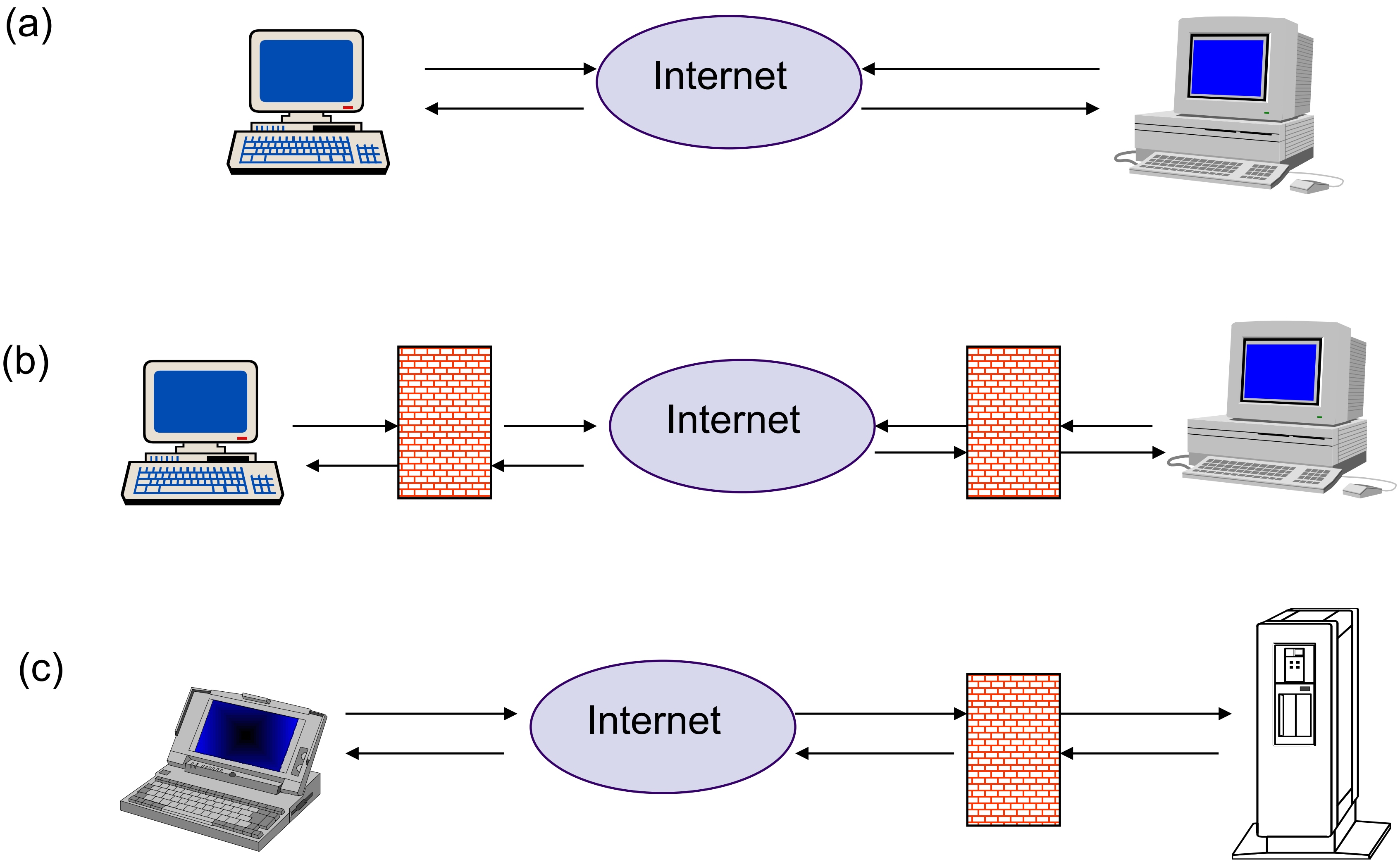
$= g^{xy'}$

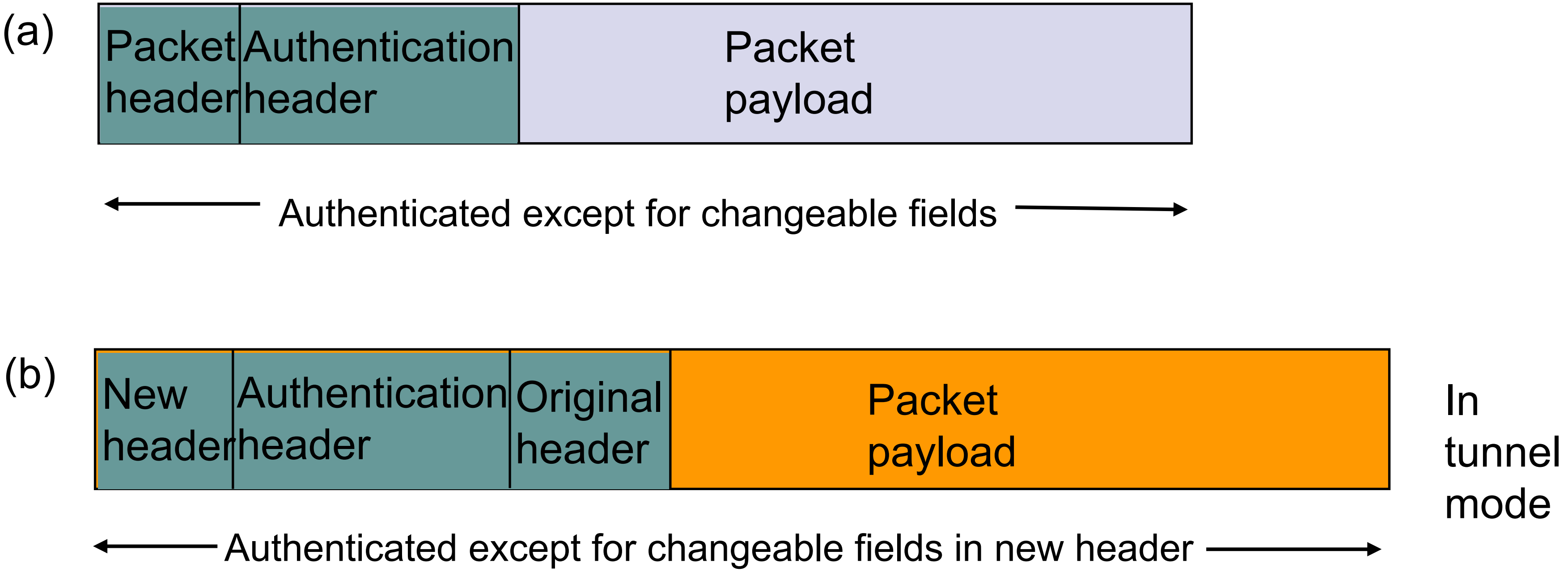
$K_2 = R^{x'}$

$= g^{x'y}$

$K_2 = T'^{y}$

$= g^{x'y}$


(a)
Internet
(b)
Internet
(c)
Internet



(a)

Packet header | Authentication header | Packet payload

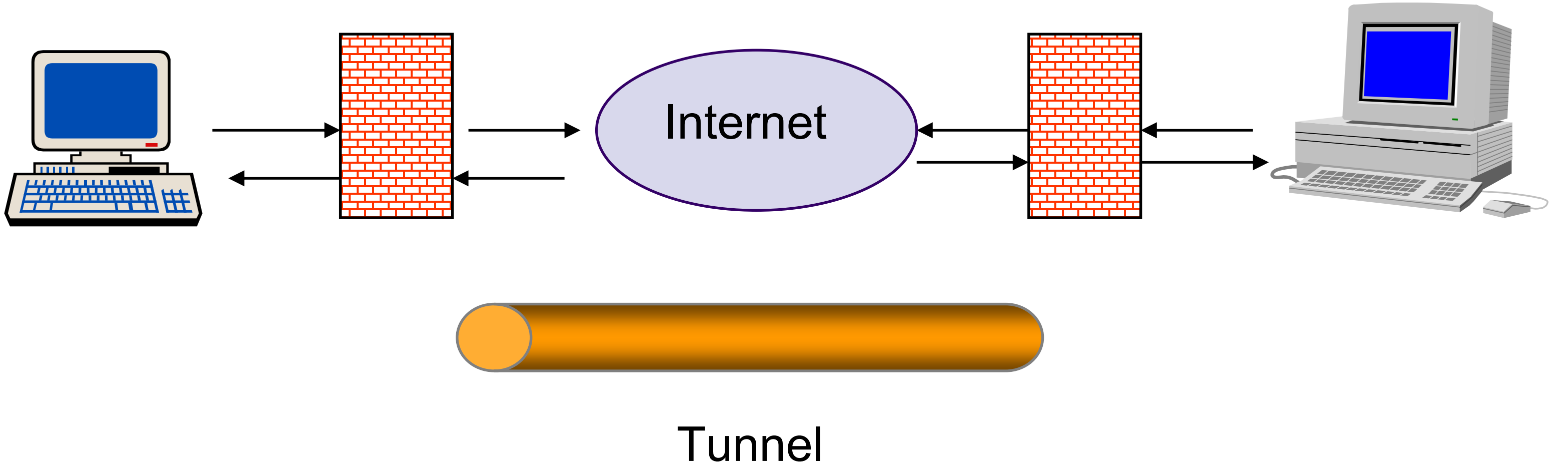
Authenticated except for changeable fields

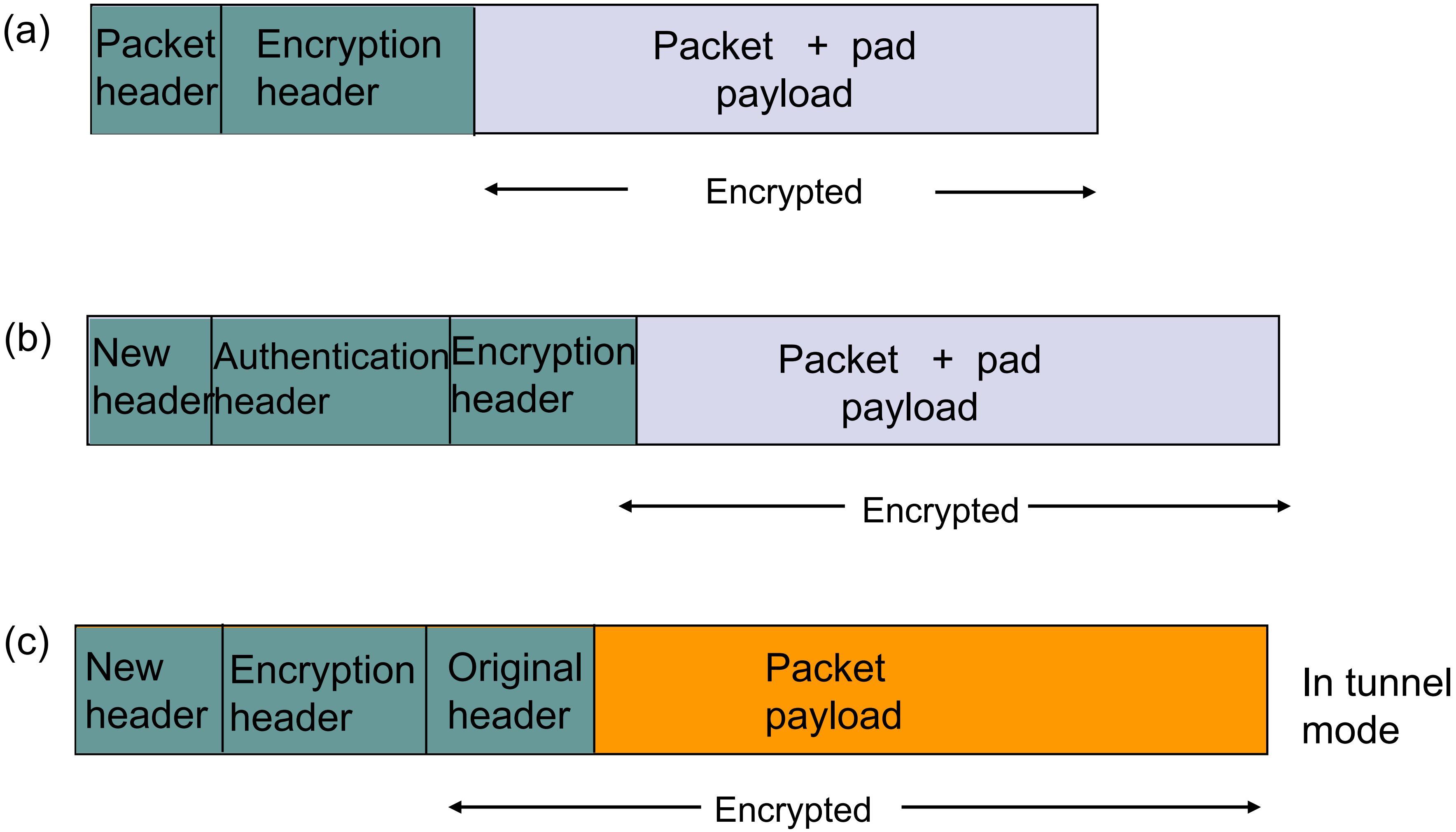
(b)

New header | Authentication header | Original header | Packet payload

In tunnel mode

Authenticated except for changeable fields in new header


Internet
Tunnel



(a)

Packet header

Encryption header

Packet + pad payload

Encrypted

(b)

New header

Authentication header

Encryption header

Packet + pad payload

Encrypted

(c)

New header

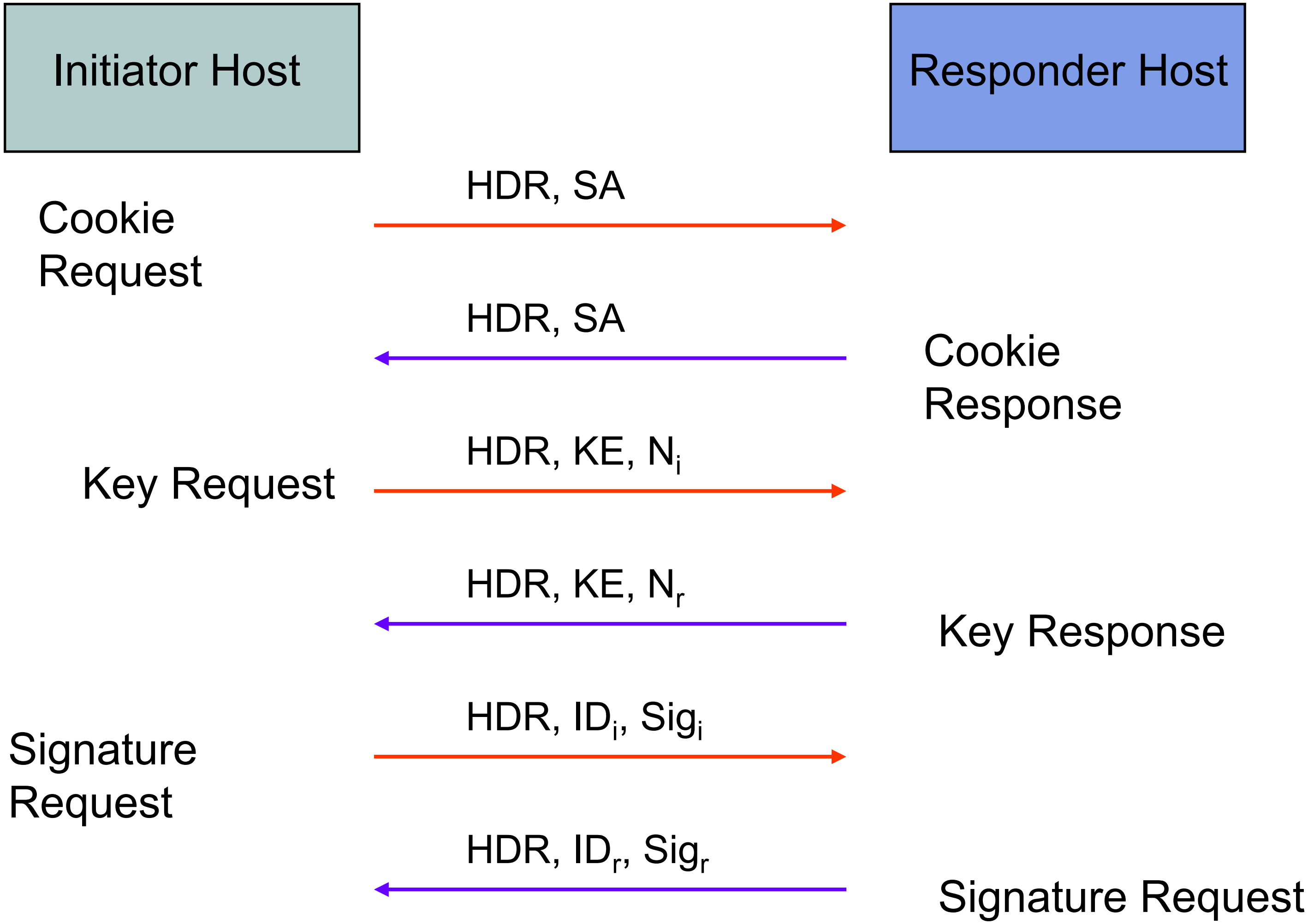
Encryption header

Original header

Packet payload

In tunnel mode

Encrypted



Initiator Host

Responder Host

Cookie Request

HDR, SA

HDR, SA

Cookie Response

Key Request

HDR, KE, N_i

HDR, KE, N_r

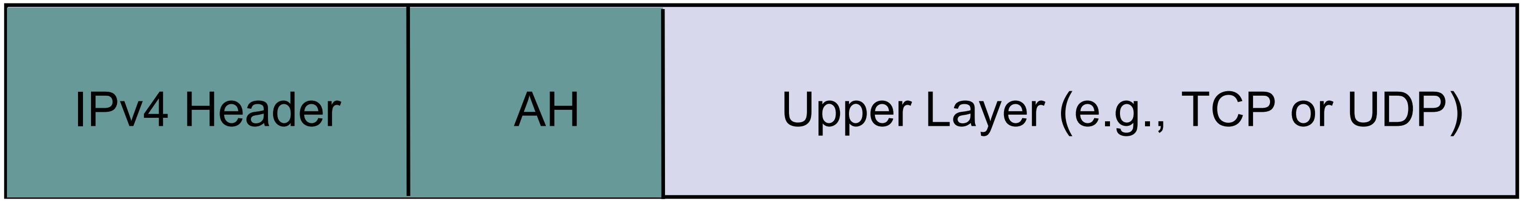
Key Response

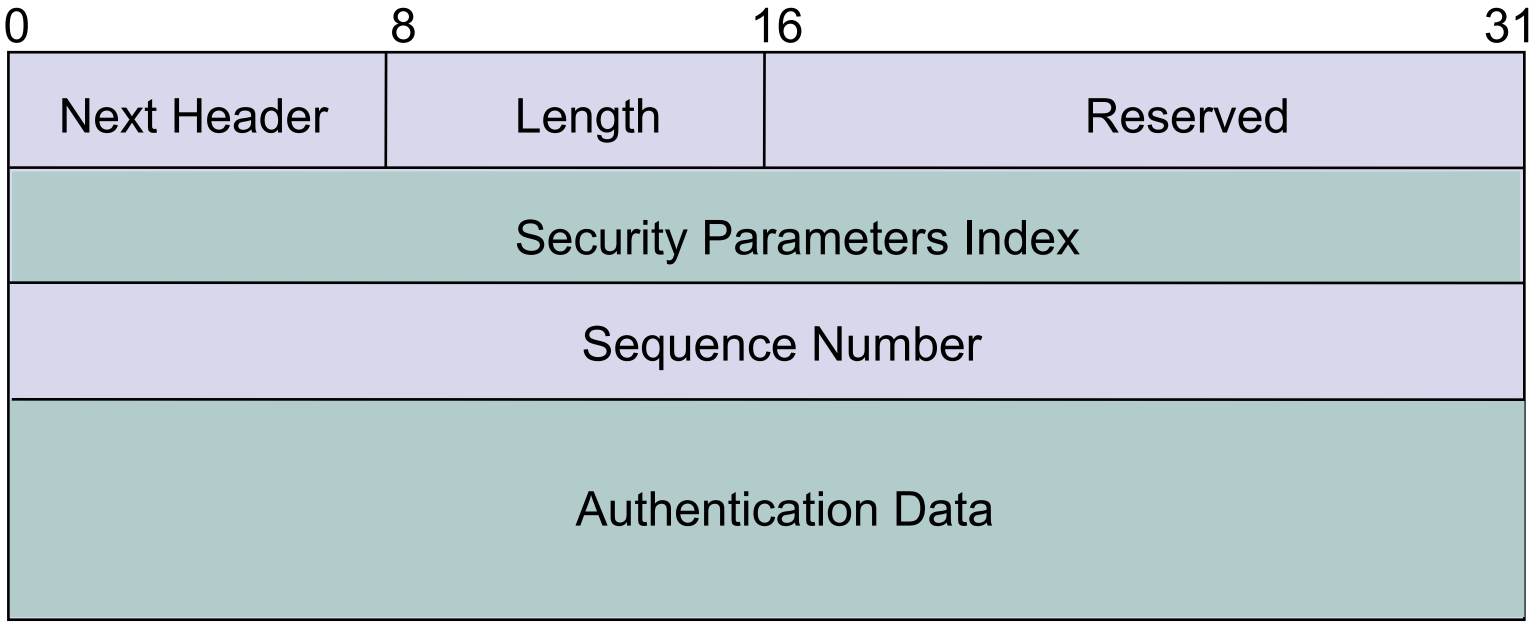
Signature Request

HDR, ID_i, Sig_i

HDR, ID_r, Sig_r

Signature Request


IPv4 Header
AH
Upper Layer (e.g., TCP or UDP)



0 8 16 31

Next Header

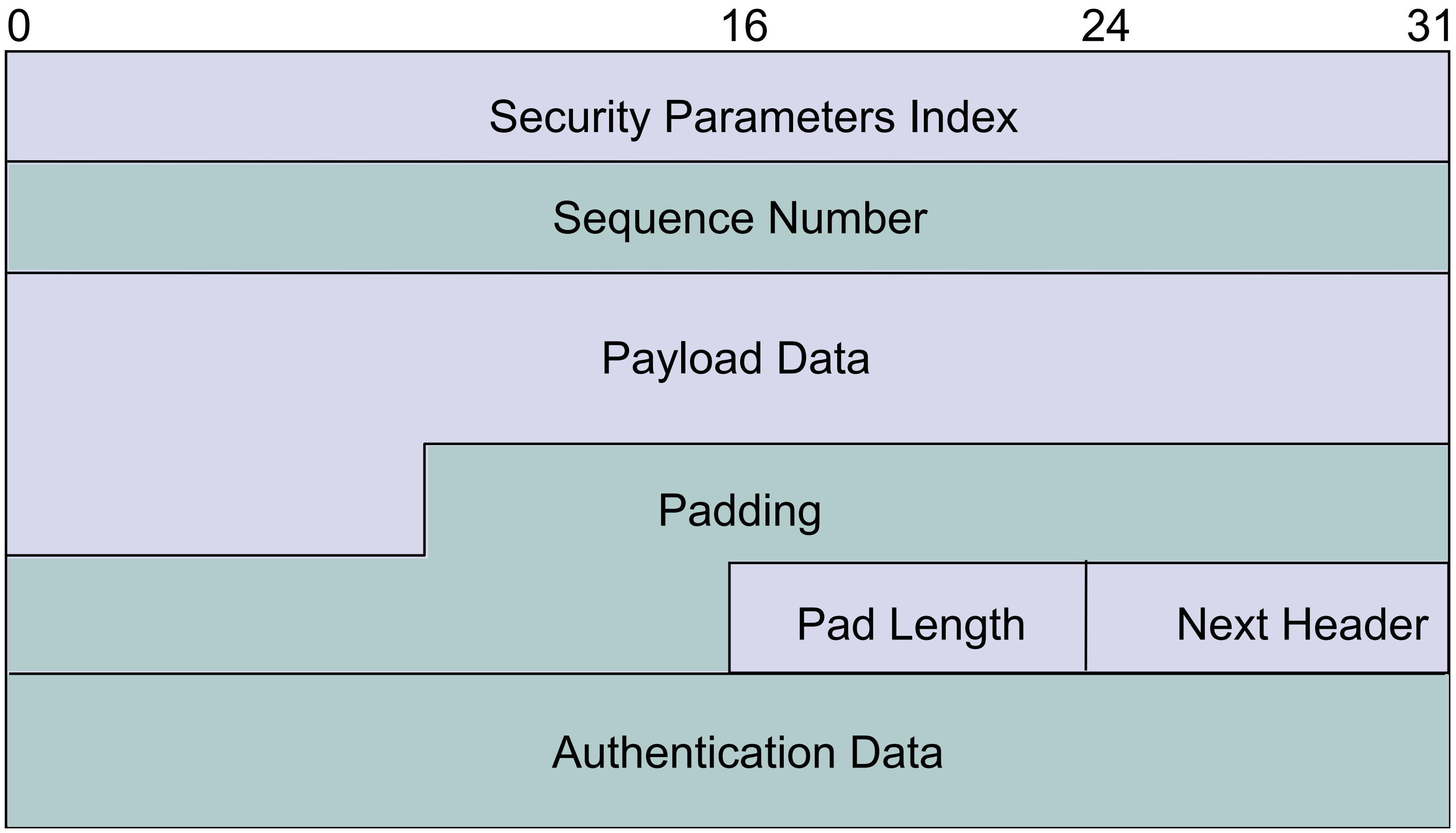
Length

Reserved

Security Parameters Index

Sequence Number

Authentication Data



0

16

24

31

Security Parameters Index

Sequence Number

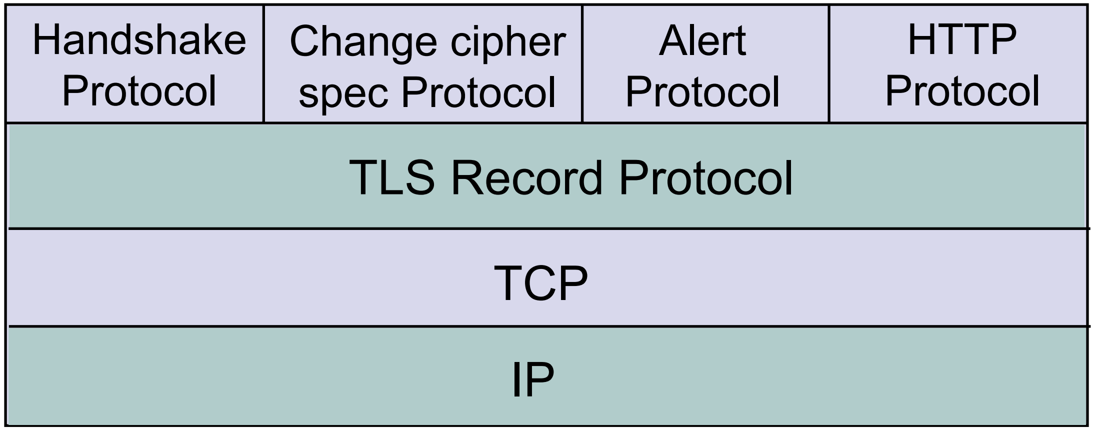
Payload Data

Padding

Pad Length

Next Header

Authentication Data



Handshake Protocol

Change cipher spec Protocol

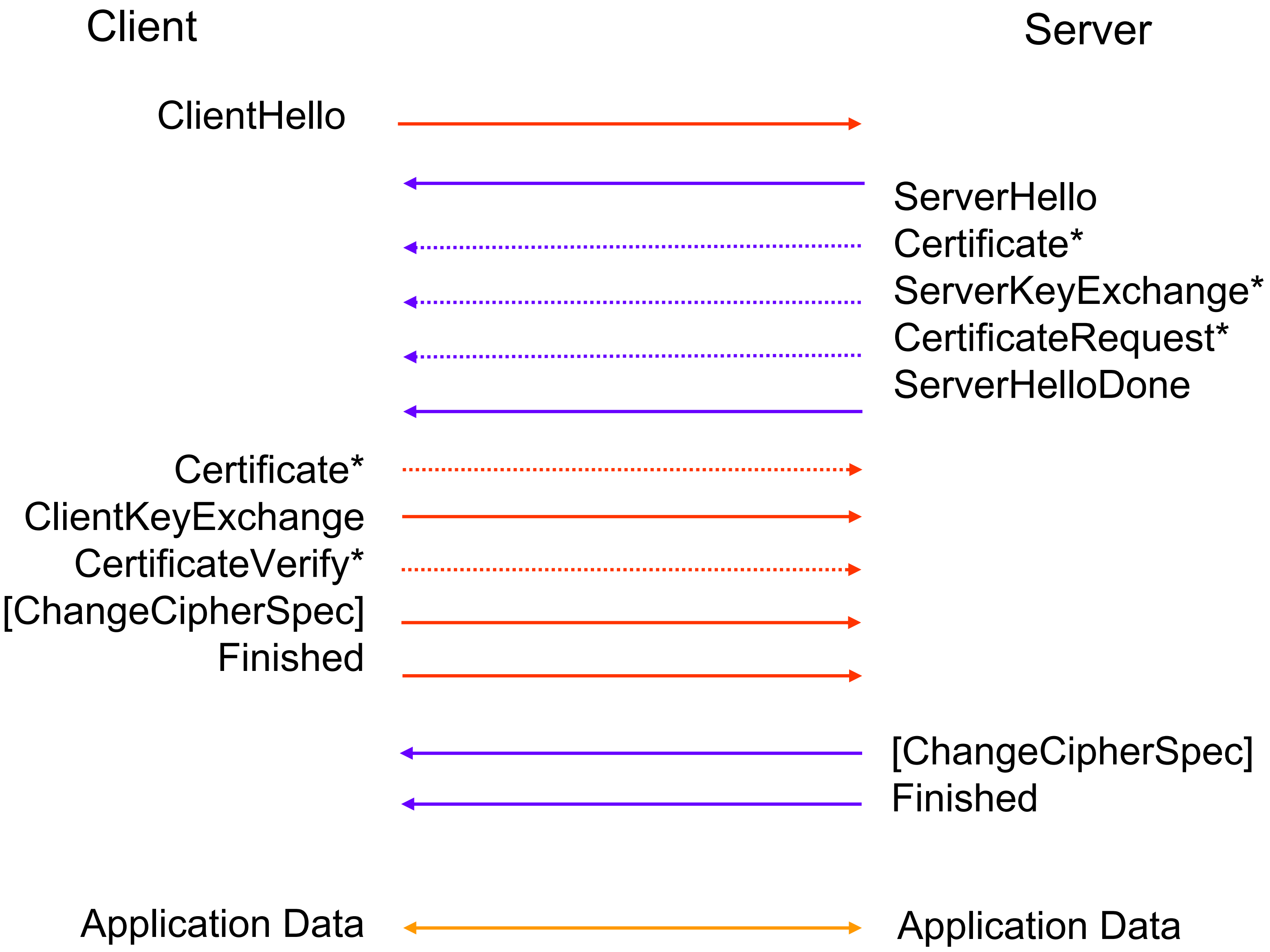
Alert Protocol

HTTP Protocol

TLS Record Protocol

TCP

IP



Client

Server

ClientHello

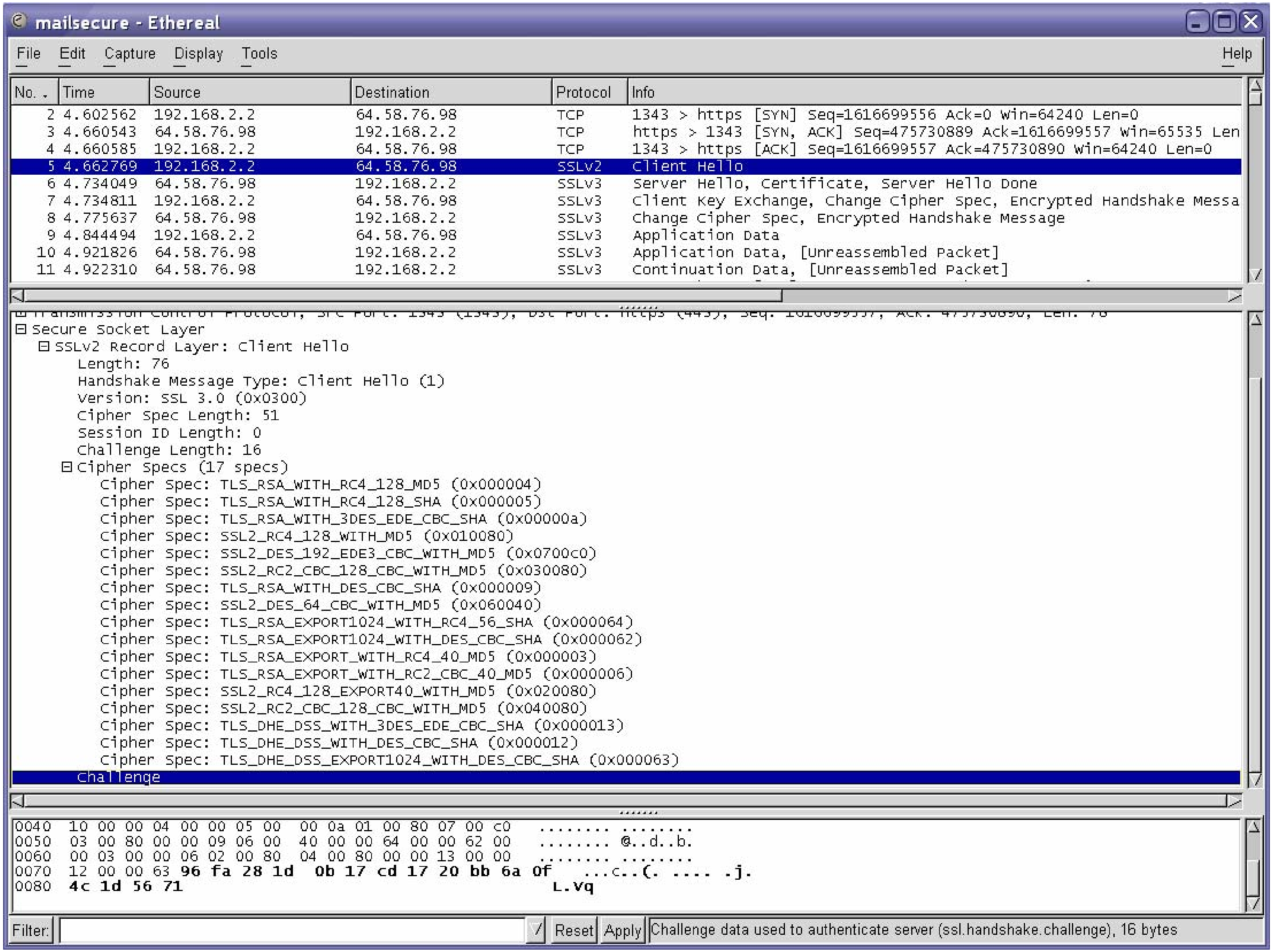
ServerHello
Certificate*
ServerKeyExchange*
CertificateRequest*
ServerHelloDone

Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished

[ChangeCipherSpec]
Finished

Application Data

Application Data

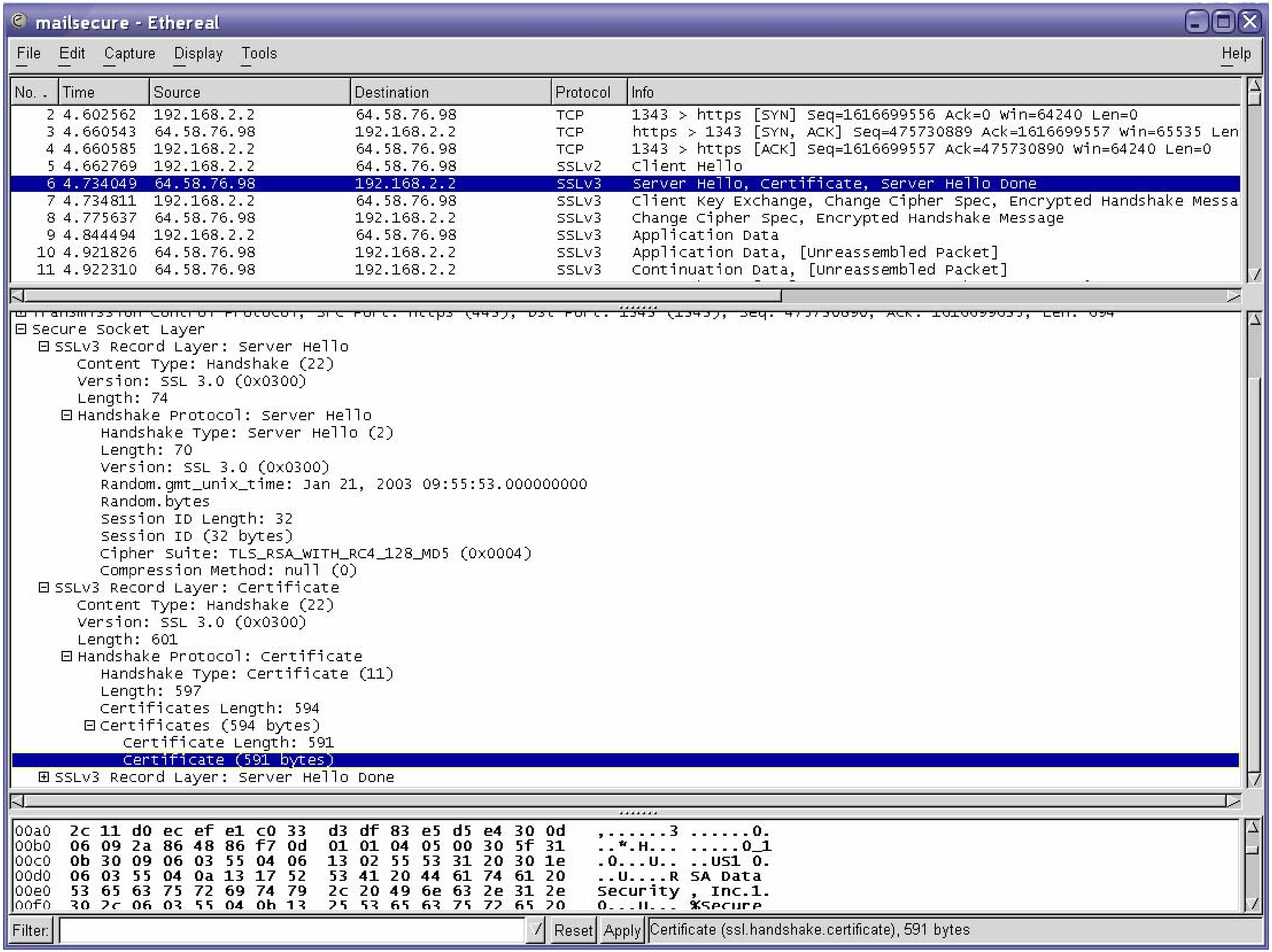


```
No. .  Time       Source          Destination     Protocol  Info
    2  4.602562   192.168.2.2     64.58.76.98     TCP       1343 > https [SYN] Seq=1616699556 Ack=0 Win=64240 Len=0
    3  4.660543   64.58.76.98     192.168.2.2     TCP       https > 1343 [SYN, ACK] Seq=475730889 Ack=1616699557 Win=65535 Len
    4  4.660585   192.168.2.2     64.58.76.98     TCP       1343 > https [ACK] Seq=1616699557 Ack=475730890 Win=64240 Len=0
    5  4.662769   192.168.2.2     64.58.76.98     SSLv2     Client Hello
    6  4.734049   64.58.76.98     192.168.2.2     SSLv3     Server Hello, Certificate, Server Hello Done
    7  4.734811   192.168.2.2     64.58.76.98     SSLv3     Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messa
    8  4.775637   64.58.76.98     192.168.2.2     SSLv3     Change Cipher Spec, Encrypted Handshake Message
    9  4.844494   192.168.2.2     64.58.76.98     SSLv3     Application Data
   10  4.921826   64.58.76.98     192.168.2.2     SSLv3     Application Data, [Unreassembled Packet]
   11  4.922310   64.58.76.98     192.168.2.2     SSLv3     Continuation Data, [Unreassembled Packet]
```

```
⊞ Transmission Control Protocol, Src Port: 1343 (1343), Dst Port: https (443), Seq: 1616699557, Ack: 475730890, Len: 76
⊟ Secure Socket Layer
  ⊟ SSLv2 Record Layer: Client Hello
        Length: 76
        Handshake Message Type: Client Hello (1)
        Version: SSL 3.0 (0x0300)
        Cipher Spec Length: 51
        Session ID Length: 0
        Challenge Length: 16
    ⊟ Cipher Specs (17 specs)
          Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
          Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)
          Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)
          Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
          Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
          Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x030080)
          Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)
          Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
          Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x000064)
          Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x000062)
          Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x000003)
          Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x000006)
          Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
          Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x040080)
          Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)
          Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)
          Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)
        Challenge
```

```
0040  10 00 00 04 00 00 05 00  00 0a 01 00 80 07 00 c0   ........ ........
0050  03 00 80 00 00 09 06 00  40 00 00 64 00 00 62 00   ........ @..d..b.
0060  00 03 00 00 06 02 00 80  04 00 80 00 00 13 00 00   ........ ........
0070  12 00 00 63 96 fa 28 1d  0b 17 cd 17 20 bb 6a 0f   ...c..(. .... .j.
0080  4c 1d 56 71                                        L.Vq
```

Challenge data used to authenticate server (ssl.handshake.challenge), 16 bytes



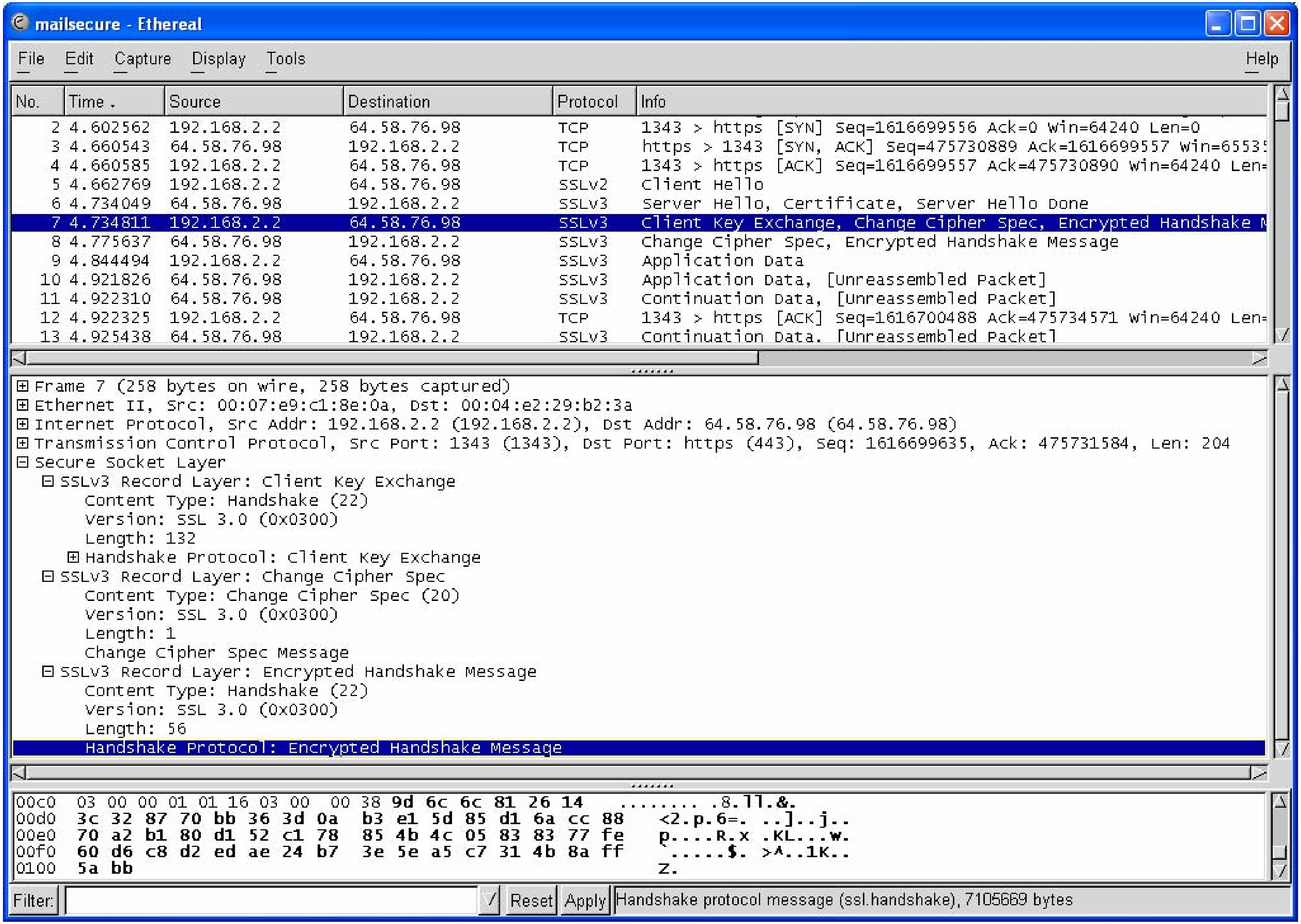
```
No. .  Time      Source          Destination     Protocol  Info
    2 4.602562  192.168.2.2     64.58.76.98     TCP       1343 > https [SYN] Seq=1616699556 Ack=0 Win=64240 Len=0
    3 4.660543  64.58.76.98     192.168.2.2     TCP       https > 1343 [SYN, ACK] Seq=475730889 Ack=1616699557 Win=65535 Len
    4 4.660585  192.168.2.2     64.58.76.98     TCP       1343 > https [ACK] Seq=1616699557 Ack=475730890 Win=64240 Len=0
    5 4.662769  192.168.2.2     64.58.76.98     SSLv2     Client Hello
    6 4.734049  64.58.76.98     192.168.2.2     SSLv3     Server Hello, Certificate, Server Hello Done
    7 4.734811  192.168.2.2     64.58.76.98     SSLv3     Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messa
    8 4.775637  64.58.76.98     192.168.2.2     SSLv3     Change Cipher Spec, Encrypted Handshake Message
    9 4.844494  192.168.2.2     64.58.76.98     SSLv3     Application Data
   10 4.921826  64.58.76.98     192.168.2.2     SSLv3     Application Data, [Unreassembled Packet]
   11 4.922310  64.58.76.98     192.168.2.2     SSLv3     Continuation Data, [Unreassembled Packet]
```

```
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 1343 (1343), Seq: 475730890, Ack: 1616699635, Len: 694
⊟ Secure Socket Layer
  ⊟ SSLv3 Record Layer: Server Hello
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 74
    ⊟ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 70
        Version: SSL 3.0 (0x0300)
        Random.gmt_unix_time: Jan 21, 2003 09:55:53.000000000
        Random.bytes
        Session ID Length: 32
        Session ID (32 bytes)
        Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
        Compression Method: null (0)
  ⊟ SSLv3 Record Layer: Certificate
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 601
    ⊟ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 597
        Certificates Length: 594
      ⊟ Certificates (594 bytes)
          Certificate Length: 591
          Certificate (591 bytes)
  ⊞ SSLv3 Record Layer: Server Hello Done
```

```
00a0  2c 11 d0 ec ef e1 c0 33  d3 df 83 e5 d5 e4 30 0d   ,......3 ......0.
00b0  06 09 2a 86 48 86 f7 0d  01 01 04 05 00 30 5f 31   ..*.H... .....0_1
00c0  0b 30 09 06 03 55 04 06  13 02 55 53 31 20 30 1e   .0...U.. ..US1 0.
00d0  06 03 55 04 0a 13 17 52  53 41 20 44 61 74 61 20   ..U....R SA Data 
00e0  53 65 63 75 72 69 74 79  2c 20 49 6e 63 2e 31 2e   Security , Inc.1.
00f0  30 2c 06 03 55 04 0b 13  25 53 65 63 75 72 65 20   0,..U... %Secure 
```

Certificate (ssl.handshake.certificate), 591 bytes

Figure 11.20

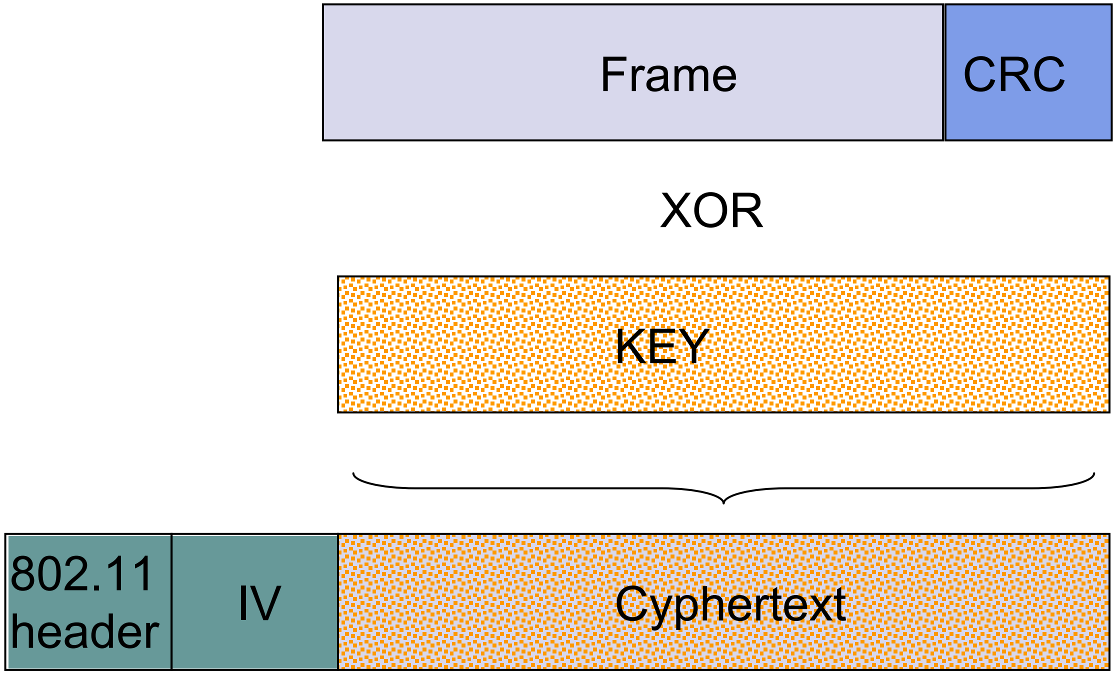


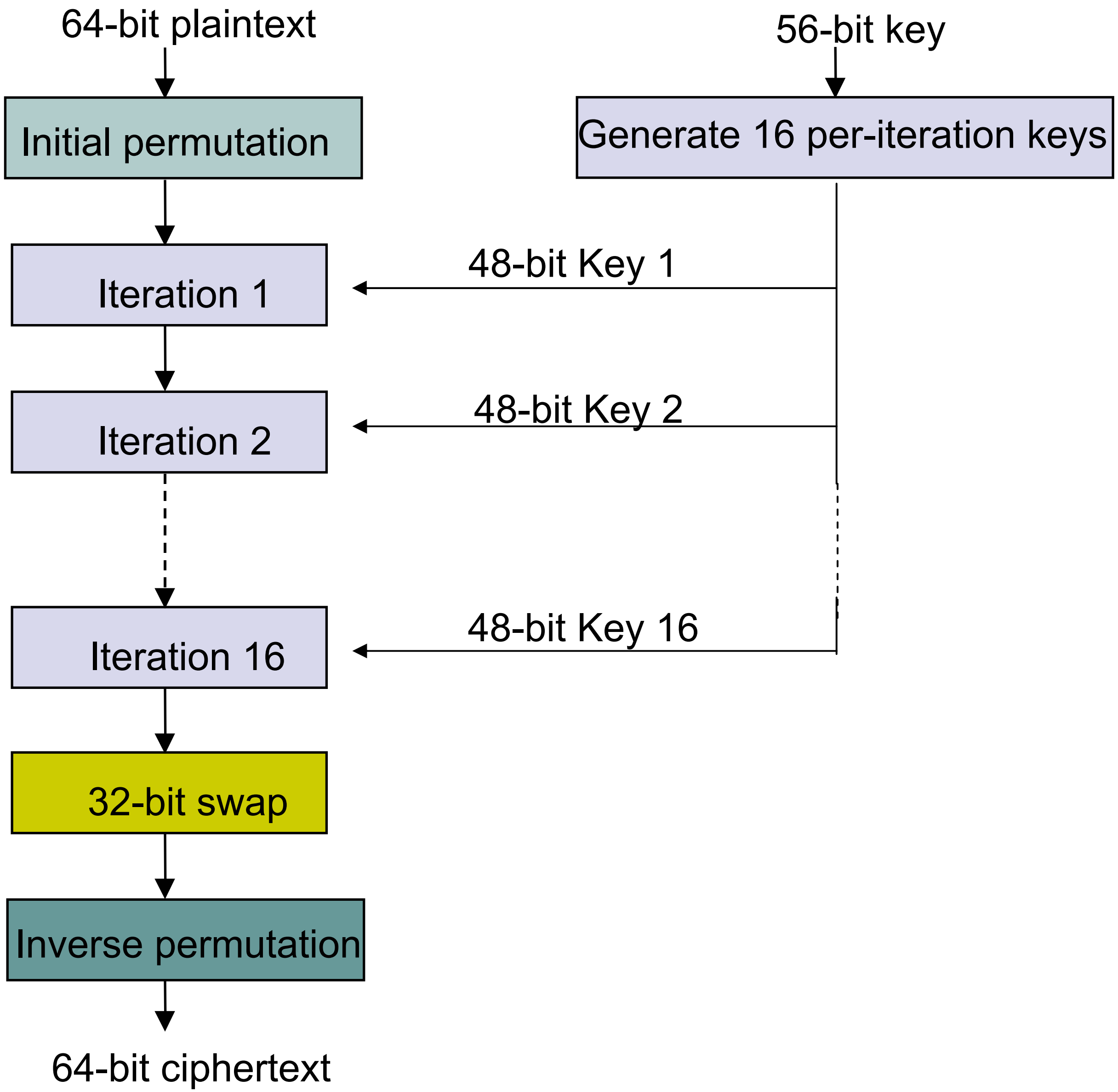
```
No. Time .   Source        Destination    Protocol Info
  2 4.602562 192.168.2.2   64.58.76.98    TCP      1343 > https [SYN] Seq=1616699556 Ack=0 Win=64240 Len=0
  3 4.660543 64.58.76.98   192.168.2.2    TCP      https > 1343 [SYN, ACK] Seq=475730889 Ack=1616699557 Win=6553
  4 4.660585 192.168.2.2   64.58.76.98    TCP      1343 > https [ACK] Seq=1616699557 Ack=475730890 Win=64240 Len=
  5 4.662769 192.168.2.2   64.58.76.98    SSLv2    Client Hello
  6 4.734049 64.58.76.98   192.168.2.2    SSLv3    Server Hello, Certificate, Server Hello Done
  7 4.734811 192.168.2.2   64.58.76.98    SSLv3    Client Key Exchange, Change Cipher Spec, Encrypted Handshake M
  8 4.775637 64.58.76.98   192.168.2.2    SSLv3    Change Cipher Spec, Encrypted Handshake Message
  9 4.844494 192.168.2.2   64.58.76.98    SSLv3    Application Data
 10 4.921826 64.58.76.98   192.168.2.2    SSLv3    Application Data, [Unreassembled Packet]
 11 4.922310 64.58.76.98   192.168.2.2    SSLv3    Continuation Data, [Unreassembled Packet]
 12 4.922325 192.168.2.2   64.58.76.98    TCP      1343 > https [ACK] Seq=1616700488 Ack=475734571 Win=64240 Len=
 13 4.925438 64.58.76.98   192.168.2.2    SSLv3    Continuation Data, [Unreassembled Packet]
```

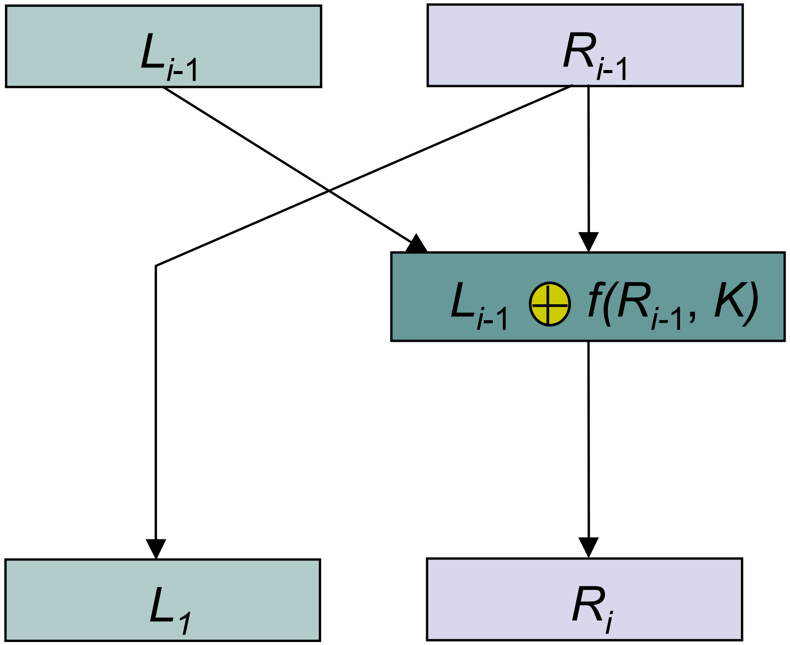
```
⊞ Frame 7 (258 bytes on wire, 258 bytes captured)
⊞ Ethernet II, Src: 00:07:e9:c1:8e:0a, Dst: 00:04:e2:29:b2:3a
⊞ Internet Protocol, Src Addr: 192.168.2.2 (192.168.2.2), Dst Addr: 64.58.76.98 (64.58.76.98)
⊞ Transmission Control Protocol, Src Port: 1343 (1343), Dst Port: https (443), Seq: 1616699635, Ack: 475731584, Len: 204
⊟ Secure Socket Layer
  ⊟ SSLv3 Record Layer: Client Key Exchange
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 132
    ⊞ Handshake Protocol: Client Key Exchange
  ⊟ SSLv3 Record Layer: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: SSL 3.0 (0x0300)
      Length: 1
      Change Cipher Spec Message
  ⊟ SSLv3 Record Layer: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 56
      Handshake Protocol: Encrypted Handshake Message
```

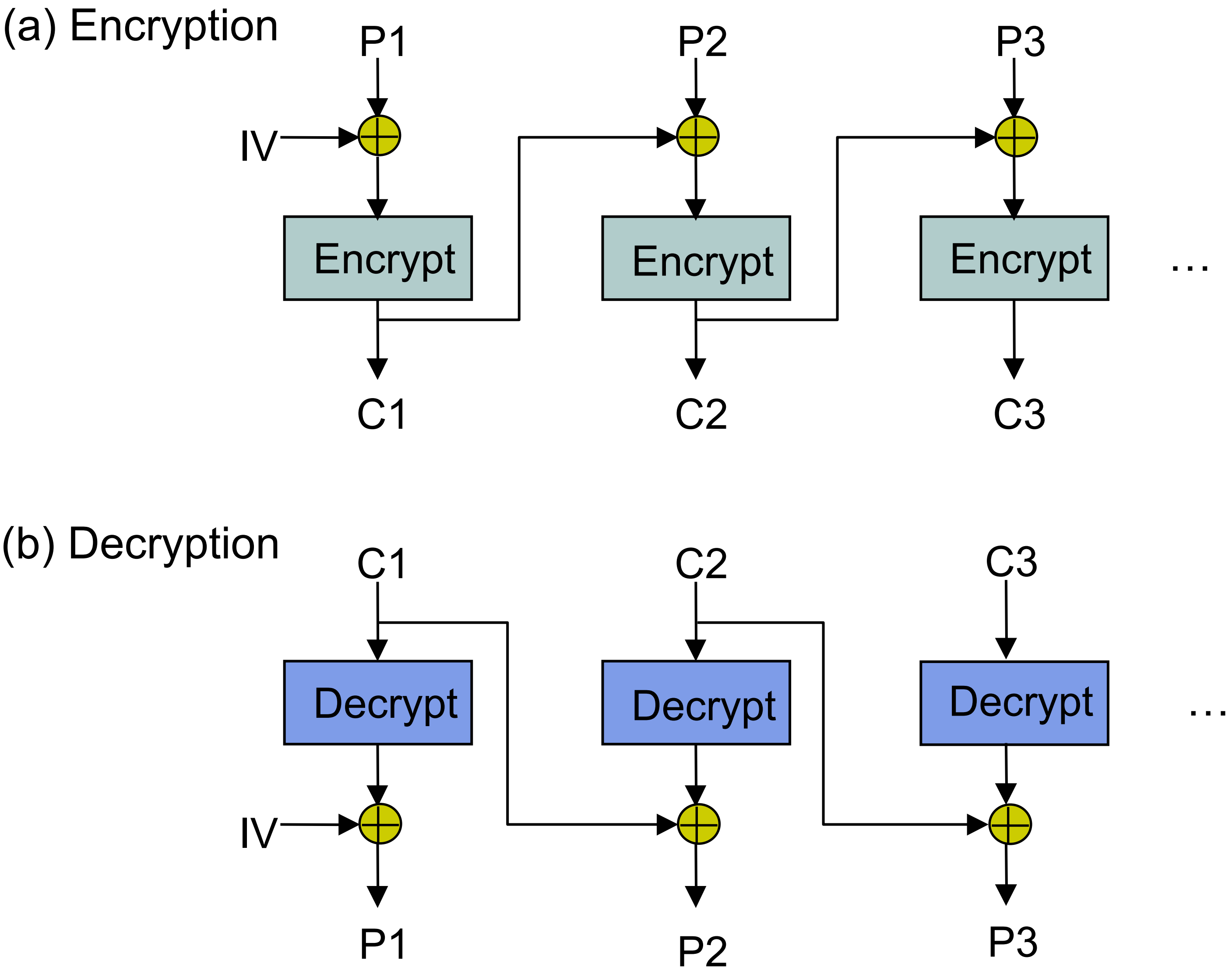
```
00c0  03 00 00 01 01 16 03 00  00 38 9d 6c 6c 81 26 14   ........ .8.ll.&.
00d0  3c 32 87 70 bb 36 3d 0a  b3 e1 5d 85 d1 6a cc 88   <2.p.6=. ..]..j..
00e0  70 a2 b1 80 d1 52 c1 78  85 4b 4c 05 83 83 77 fe   p....R.x .KL...w.
00f0  60 d6 c8 d2 ed ae 24 b7  3e 5e a5 c7 31 4b 8a ff   `.....$. >^..1K..
0100  5a bb                                              Z.
```

Handshake protocol message (ssl.handshake), 7105669 bytes


Frame
CRC
XOR
KEY
802.11 header
IV
Cyphertext


64-bit plaintext
56-bit key
Initial permutation
Generate 16 per-iteration keys
Iteration 1
48-bit Key 1
Iteration 2
48-bit Key 2
Iteration 16
48-bit Key 16
32-bit swap
Inverse permutation
64-bit ciphertext


L_{i-1}
R_{i-1}
$L_{i-1} \oplus f(R_{i-1}, K)$
L_1
R_i


(a) Encryption
P1
P2
P3
IV
Encrypt
Encrypt
Encrypt
…
C1
C2
C3
(b) Decryption
C1
C2
C3
Decrypt
Decrypt
Decrypt
…
IV
P1
P2
P3