

امنیت داده ها

امنیت داده ها

دکتر یعقوب فرجامی

دکتر یعقوب فرجامی

عضو هیات علمی دانشکده فنی قم

عضو هیات علمی دانشکده فنی قم

فصل چهاردهم : امنیت در

معماری لایه ای شبکه

خطرات تهدیدکننده وب

○ با توجه به سادگی و گستردگی استفاده از مرورگرها و خدمات وب و راه اندازی سرورها، امنیت وب از پیچیدگی بالایی برخوردار است.

○ نمونه ای از خطرات متداول:

- حمله به وب سرورها
- تهدید اعتبار برنامه های تجاری مهم
- وجود کاربران عام و ناآشنا به خطرات امنیتی
- دسترسی به حریم خصوصی افراد و آزار و اذیت آنها



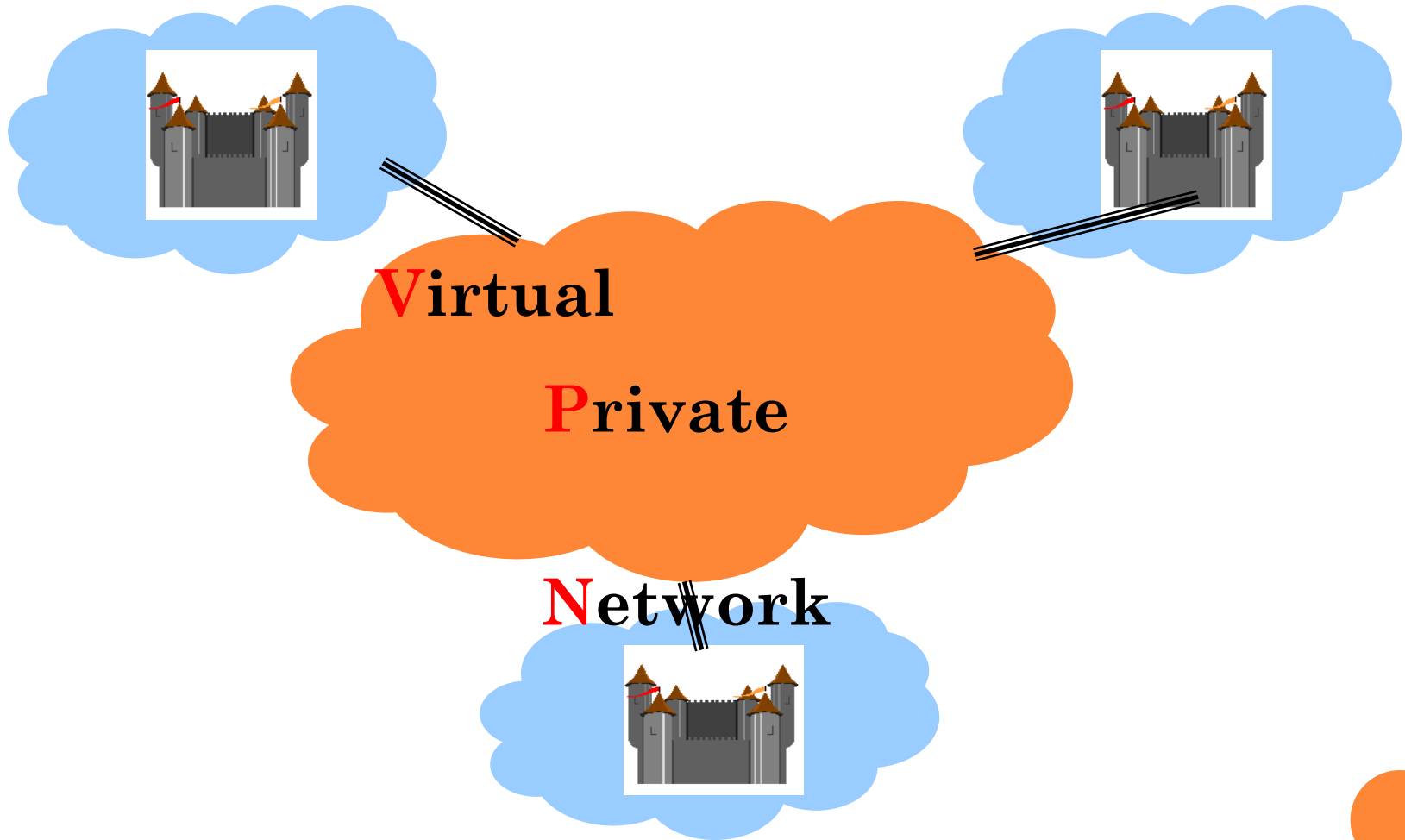
امنیت ارتباطات و حفاظت از شبکه

حفاظت از شبکه خودی :

ارتباط امن بین شبکه‌ای :



امنیت ارتباطات و حفاظت شبکه



امنیت ارتباطات و حفاظت شبکه

امنیت ارتباطات

SET,
PEM, S-HTTP
Kerberos,...



SSL,TLS



IPSec



PPTP



Application

Presentation

Session

Transport

Network

Datalink

Physical

حفاظت از شبکه

Application Proxy



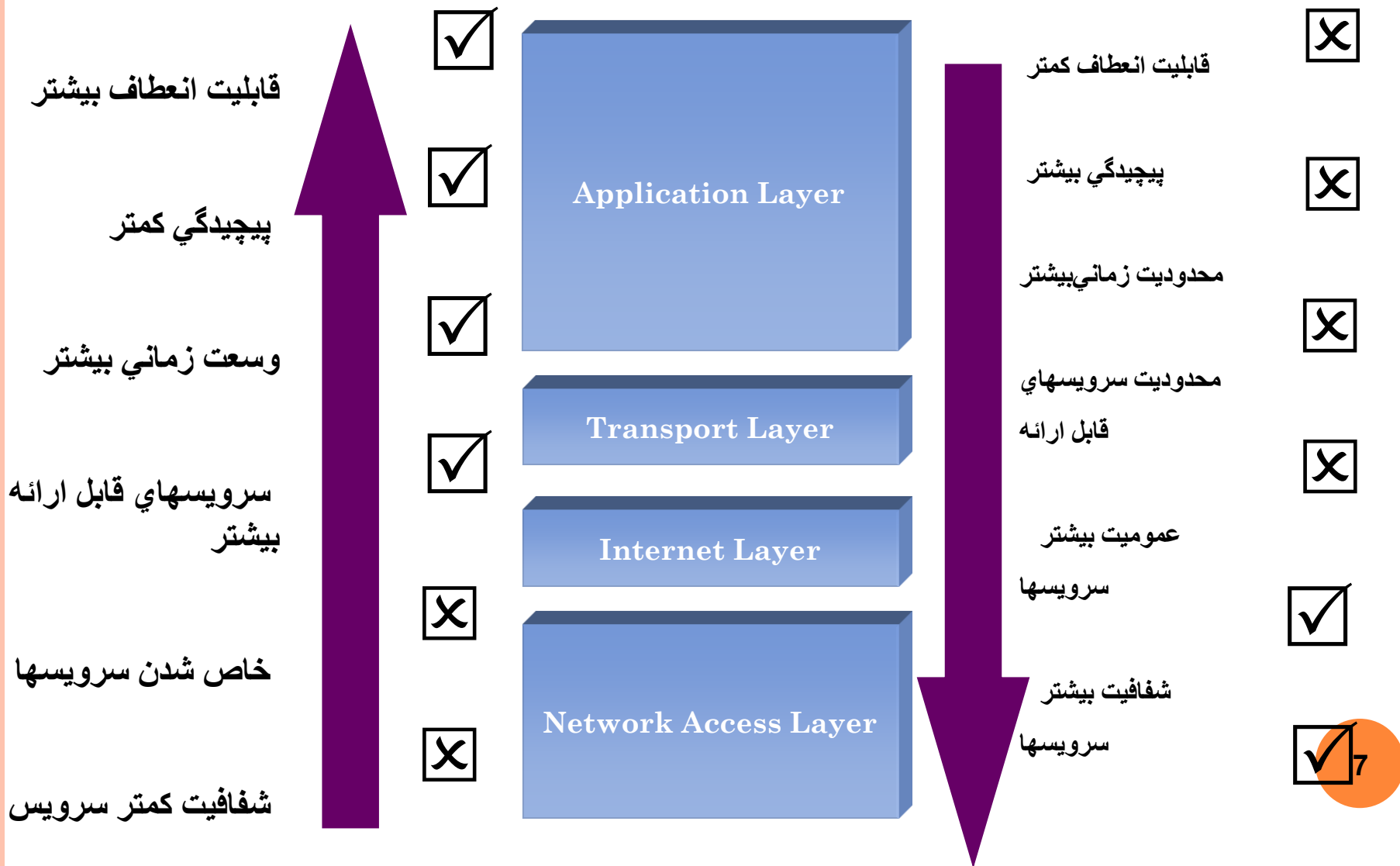
Circuit Proxy



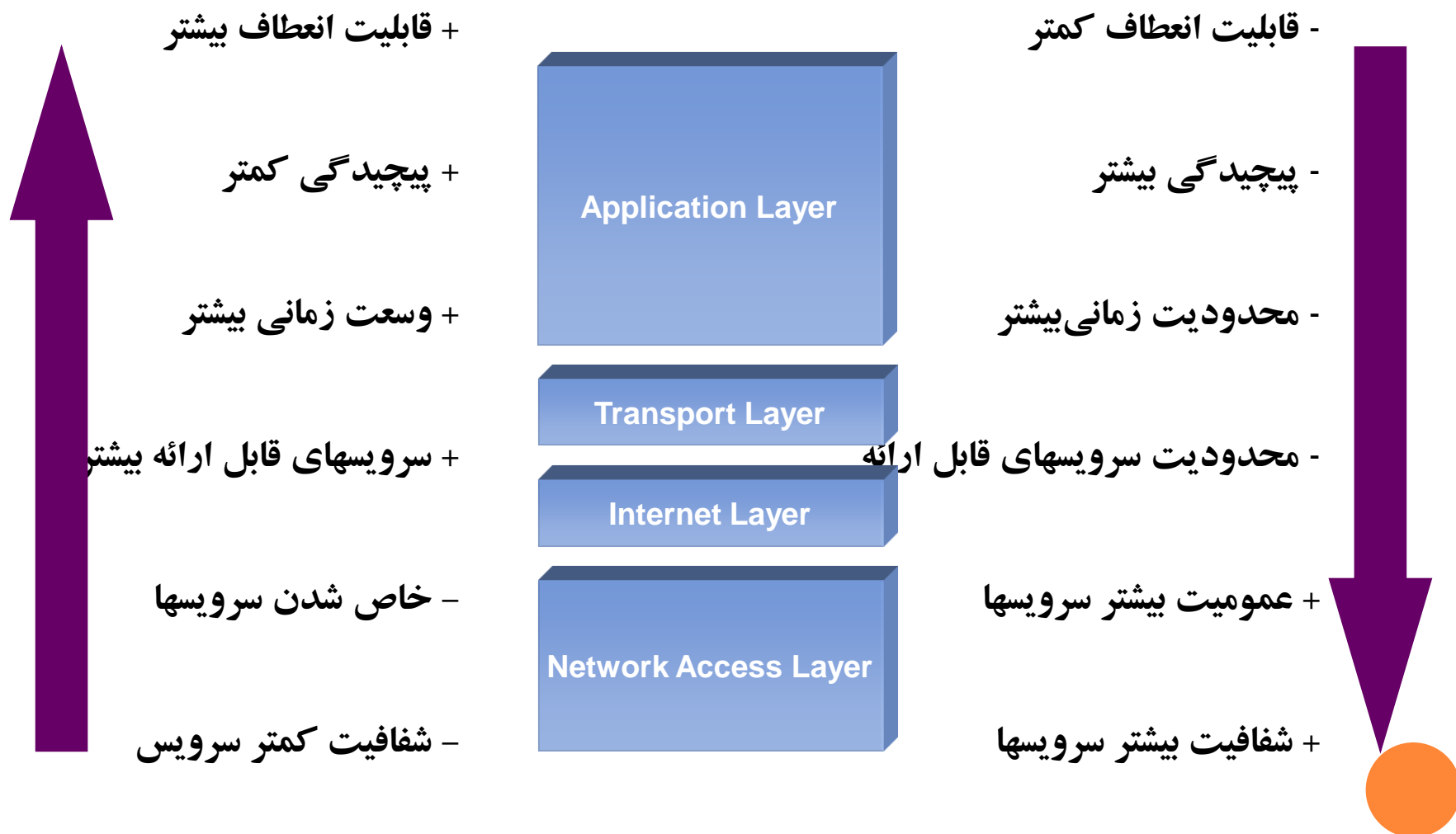
Packet Filtering



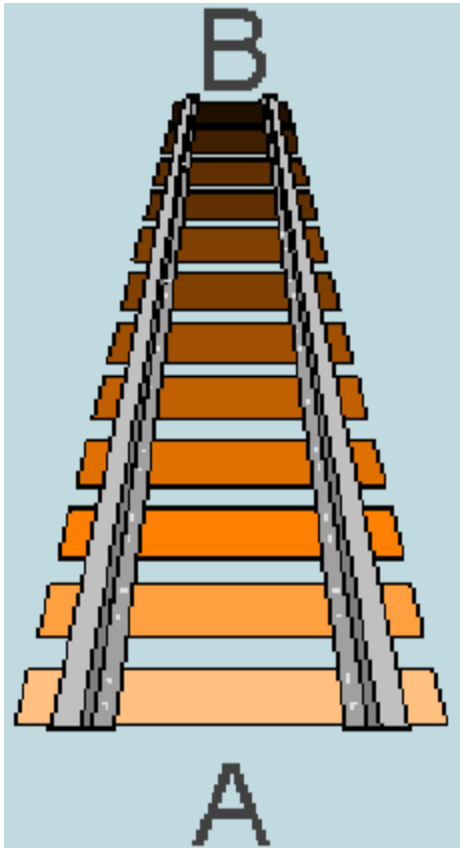
انواع امن سازی ارتباط بین شبکه‌ای



تفاوت امن سازی در لایه های مختلف



تشبیه



بسته‌بندی اجناس

امن سازی در لایه کاربرد

بسته‌بندی پستی

امن سازی در لایه حمل

چینش در اتاقکهای
مخصوص ترابری

امن سازی در لایه اینترنت

Security Services and, OSI, Layers, Mechanisms

Table 1.6 Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

THREATS ON THE WEB

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none">•Modification of user data•Trojan horse browser•Modification of memory•Modification of message traffic in transit	<ul style="list-style-type: none">•Loss of information•Compromise of machine•Vulnerability to all other threats	Cryptographic checksums
Confidentiality	<ul style="list-style-type: none">•Eavesdropping on the Net•Theft of info from server•Theft of data from client•Info about network configuration•Info about which client talks to server	<ul style="list-style-type: none">•Loss of information•Loss of privacy	Encryption, web proxies
Denial of Service	<ul style="list-style-type: none">•Killing of user threads•Flooding machine with bogus requests•Filling up disk or memory•Isolating machine by DNS attacks	<ul style="list-style-type: none">•Disruptive•Annoying•Prevent user from getting work done	Difficult to prevent
Authentication	<ul style="list-style-type: none">•Impersonation of legitimate users•Data forgery	<ul style="list-style-type: none">•Misrepresentation of user•Belief that false information is valid	Cryptographic techniques

روشهای مختلف تامین امنیت وب

○ استفاده از IPSec . مزایا :

- همه منظوره
- شفاف از دید کاربران لایه بالاتر
- سربار استفاده از IPSec با استفاده از فیلترینگ قابل حل است

○ استفاده از SSL/TLS

- شفاف از دید Application ها
- پشتیبانی مرورگرهایی مانند Netscape و IE و نیز بسیاری از وب سرورها

○ سرویسهای امنیتی وابسته به کاربرد خاص

• SET

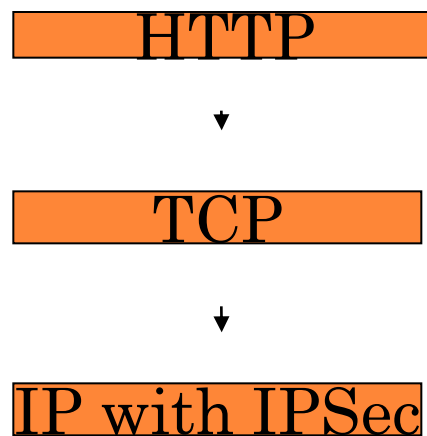
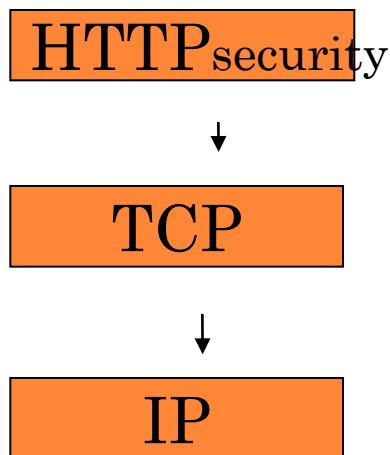


معماری های جایگزین

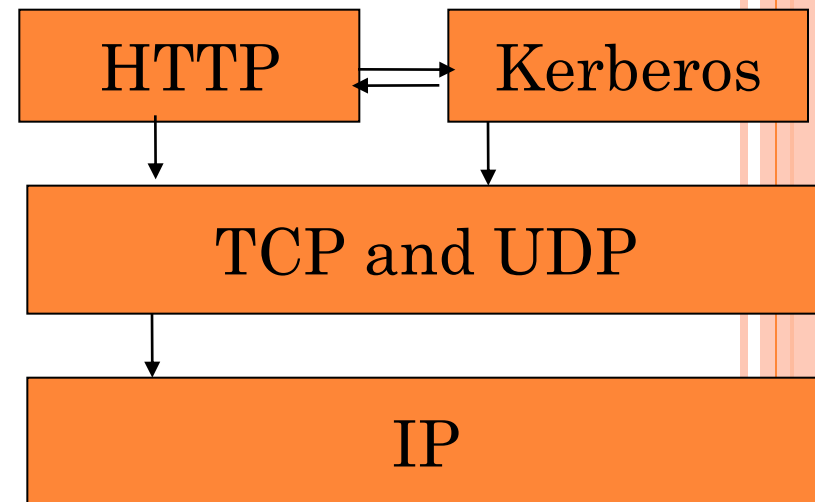
- Separate Layer
 - Over TCP: SSL
 - Over IP: IPSec
- Application-Specific
 - SHTTP
- Parallel
 - Kerberos; Kerberos with TLS?



معماری های جایگزین



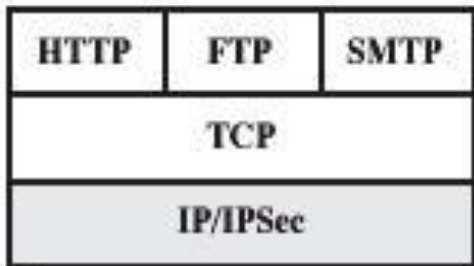
Integrated with Core
network level



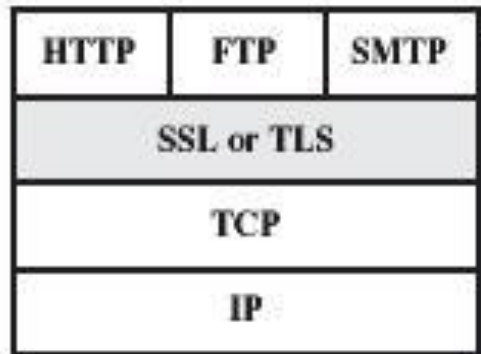
Parallel Security Protocol
application level



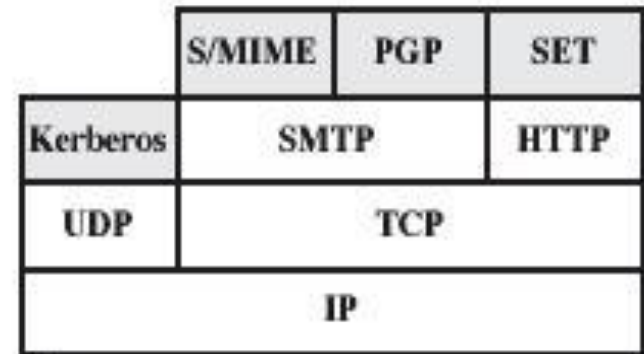
WEB SECURITY APPROACHES



(a) Network Level



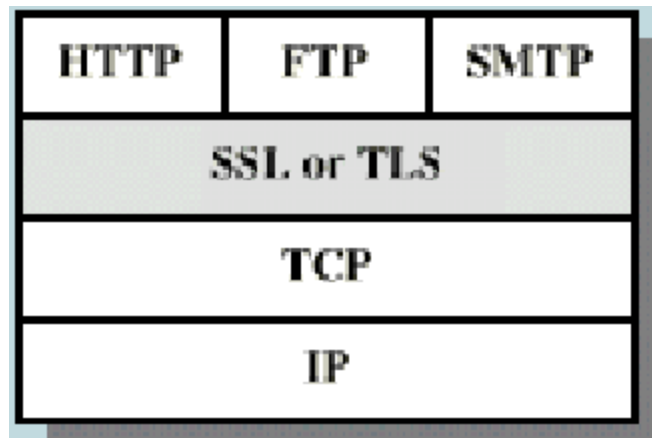
(b) Transport Level



(c) Application Level



ایجاد امنیت در لایه انتقال



+ سرویسهای امنیتی برای کاربردهای مورد نظر قابل اعمالند

لایه انتقال

- باید در کاربردها اصلاحات مورد نیاز را اعمال نمود

پروتکل SSL

- پروتکل SSL (Secure Socket Layer) توسط شرکت Netscape ارائه شد.
- SSL به عنوان واسط بین لایه انتقال و لایه کاربرد عمل می کند.
- از SSL می توان برای امن کردن سرویس های ارتباطی مبتنی بر TCP و پروتکل های لایه کاربرد (مثل FTP و HTTP) استفاده کرد.

SSL تاریخچه

○ **SSL1.0** اولین طراحی شرکت Netscape * سال ۱۹۹۴ میلادی.
این نسخه هیچگاه منتشر نشد!

○ **SSL2.0** توسط شرکت Netscape طراحی و منتشر شد * اوایل سال ۱۹۹۵ میلادی.

○ **SSL3.0** توسط شرکت Netscape طراحی و منتشر شد * اوایل سال ۱۹۹۶ میلادی.

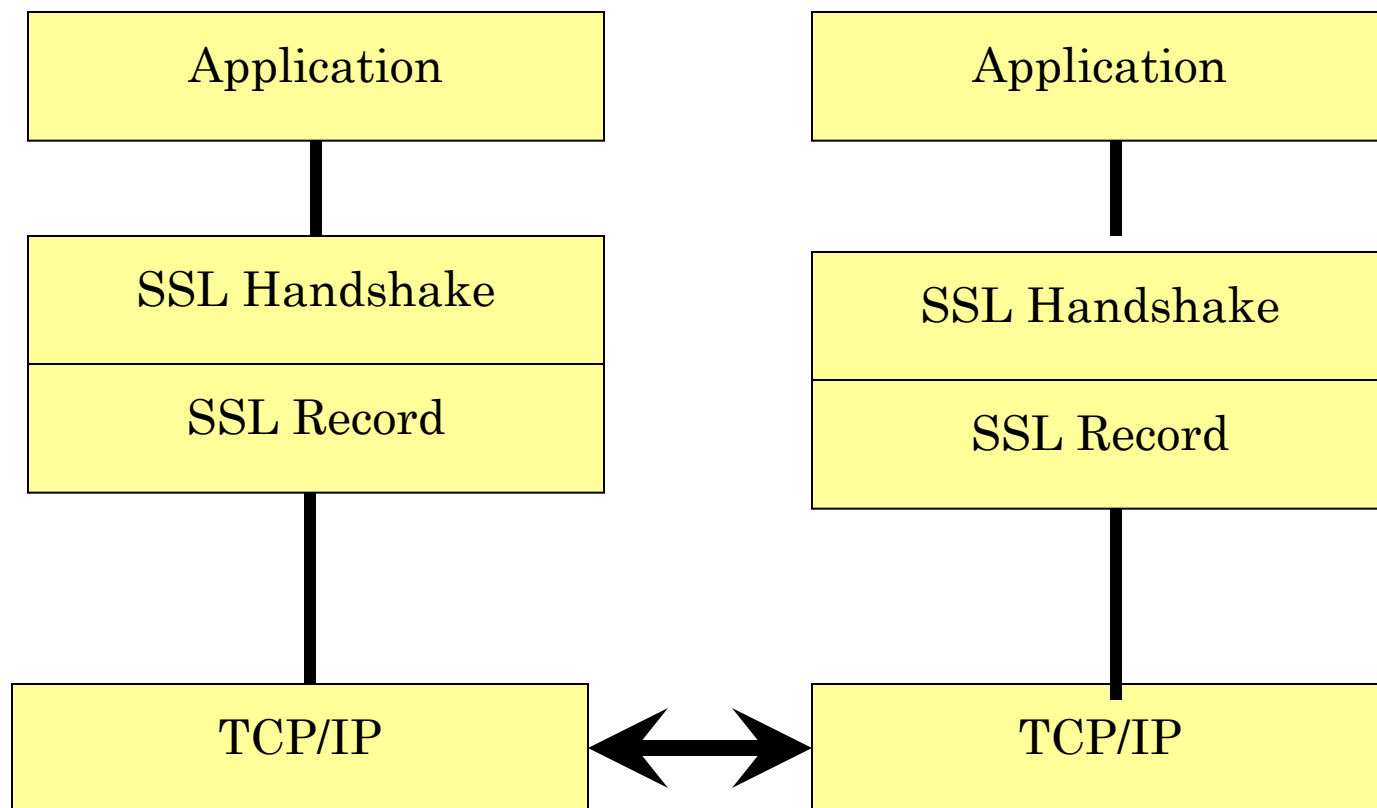
در ابتدای ماه می سال ۱۹۹۶ میلادی، توسعه SSL تحت مسئولیت IETF در آمد.

○ **TLS1.0** اولین نسخه استاندارد پروتکل SSL * اوایل سال ۱۹۹۹ میلادی.

○ **TLS1.1** برای رفع ضعفهای TLS1.0 منتشر شد.
این نسخه، استاندارد نشده است.

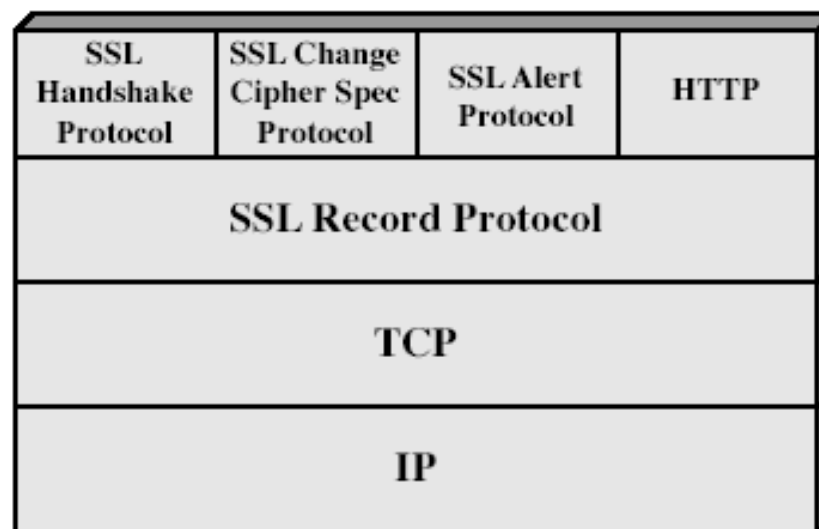
تلاش برای ارتقای پروتکل SSL ادامه دارد.

معماری SSL

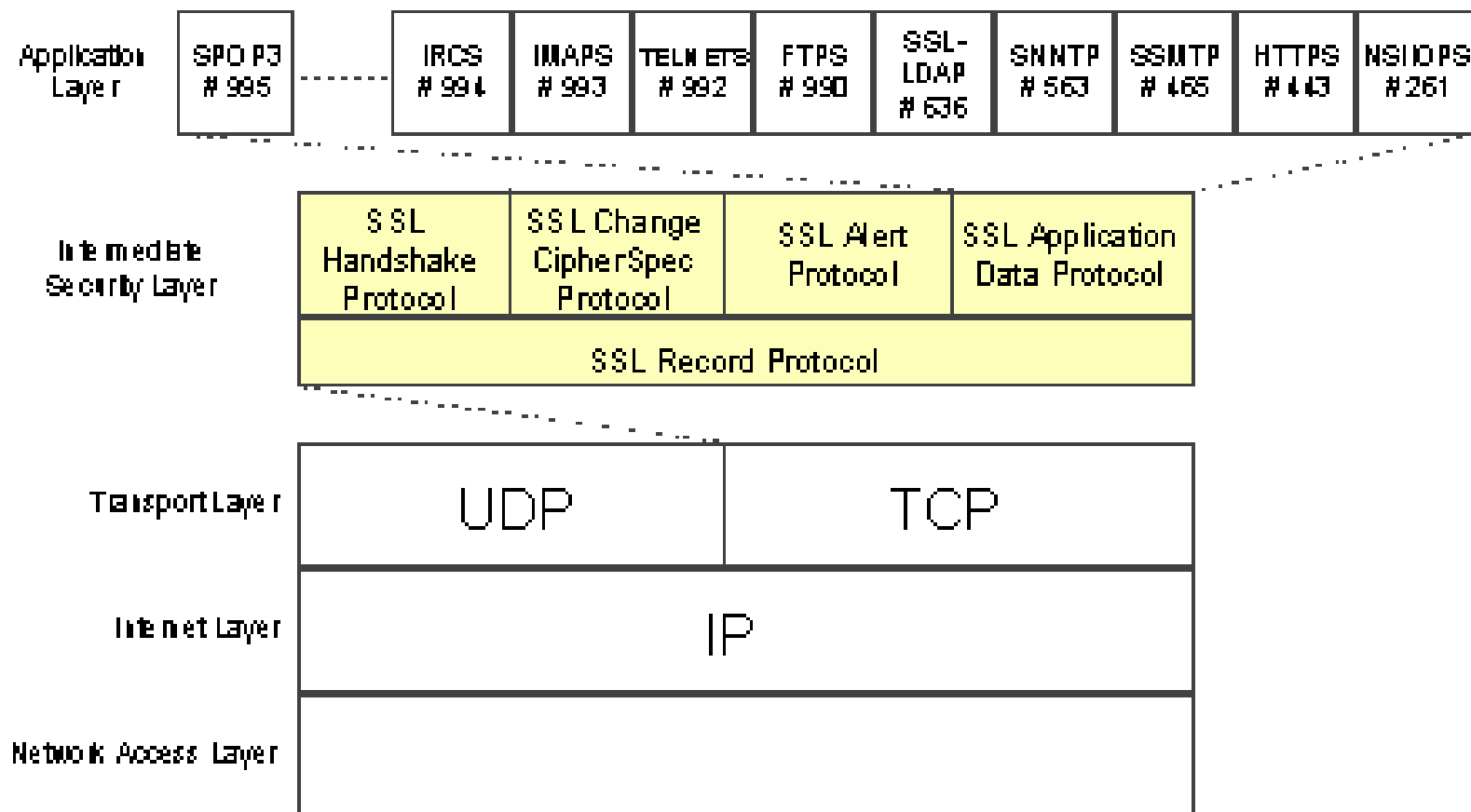


SSL - معماری

- لایه اول بالای لایه انتقال و لایه دوم در لایه کاربرد
- لایه اول شامل پروتکل Record و لایه دوم مربوط به سرویسهای مدیریتی بوده و شامل پروتکلهای زیر می شود



معماری SSL



SSL - مفاهيم

SSL connection

- ❑ Server & client random
- ❑ Server write MAC secret
- ❑ Client write MAC secret
- ❑ Server write key
- ❑ Client write key
- ❑ Initialization Vector
- ❑ Sequence numbers

SSL session

- Session identifier
- Peer certificate
- Compression method
- Cipher spec
- Master secret
- Is resumable



SSL – پروتکلها

○ SSL Record Protocol : دو سرویس برای SSL فراهم می کند:

• محرمانگی :

○ با استفاده از یک کلید متقارن مخفی که در پروتکل Handshake به اشتراک گذاشته شده است.

○ استفاده از یکی از الگوریتمهای IDEA، RC2-40، RC4-40، RC4-128، Fortezza، DES، DES-40، 3DES

• جامعیت پیغام

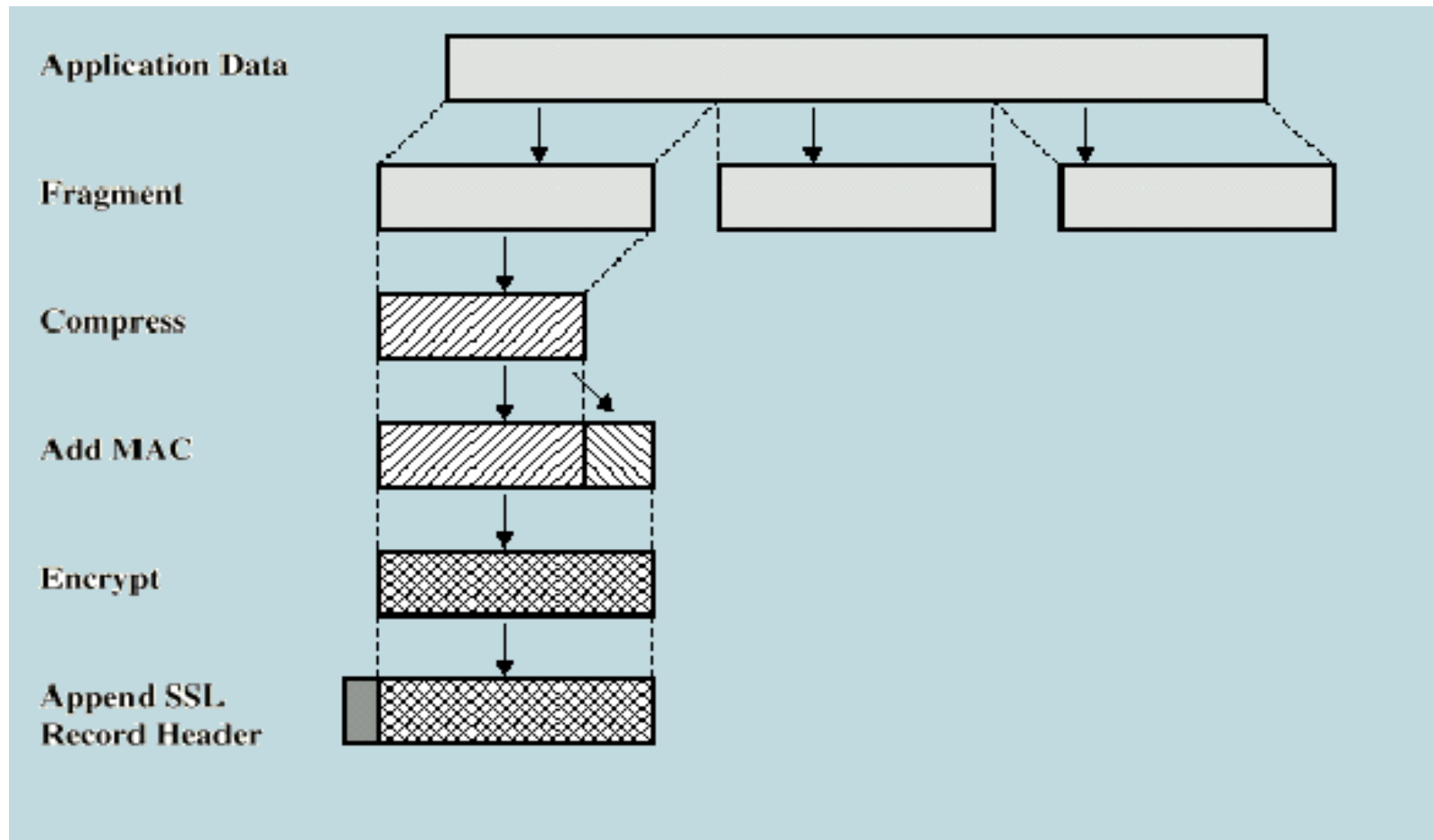
○ تولید MAC با استفاده از کلید متقارن مخفی

○ استفاده از SHA-1 یا MD5

○ پروتکل handshake وظیفه تولید و توزیع کلیدهای متقارن برای انجام رمزگذاری مرسوم و نیز محاسبه MAC را برعهده دارد



عملکرد پروتکل Record



SSL – پروتکلها

اعمال انجام شده در پروتکل Record

- قطعه بندی: تولید بلاکهای به طول 2^{14} یا کمتر .
- فشرده سازی : اختیاری و بدون از دست رفتن داده.
- تولید MAC : مشابه HMAC و روی ورودی زیر انجام می گیرد:
`Hash(MAC_write_secret || pad_2 || hash(MAC_write_secret || pad_1 || seq_num || SSLCompressed.type || SSLCompressed.length || SSLCompressed.fragment))`
- الگوریتم hash ، MD5 یا SHA-1 می باشد.
- رمزنگاری : استفاده از رمز بلاکی یا نهی. باعث افزایش حداقل 1024 بایت میشود.
- اضافه کردن سرآیند : به ابتدای بلاک رمز شده می چسبد و شامل موارد زیر است:
(نوع محتوا، نسخه اصلی SSL، نسخه فرعی SSL، طول داده فشرده شده)
نوع محتوا(Content Type) بیان کننده پروتکل استفاده کننده از این سرویس در لایه دوم می باشد

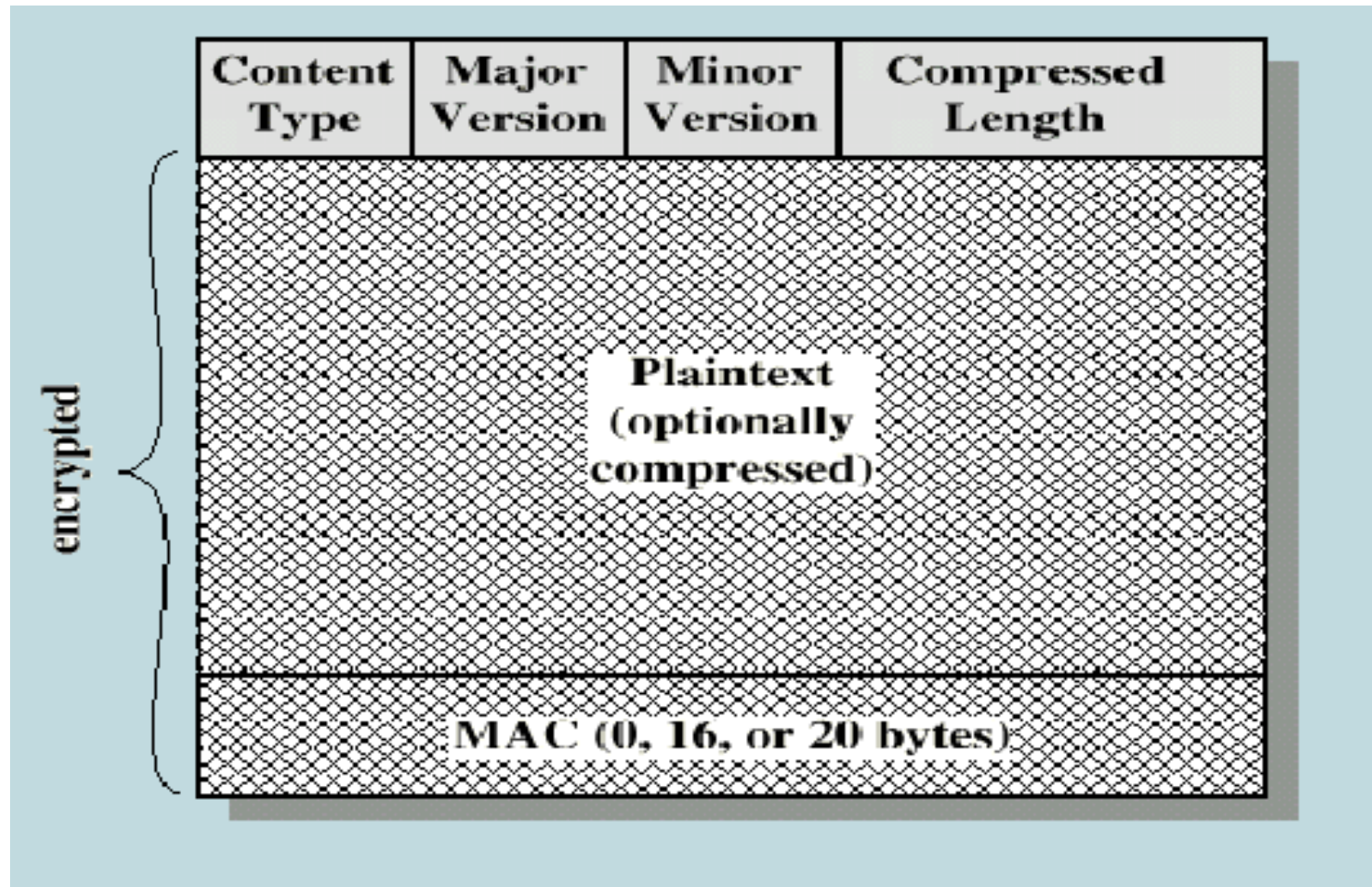


RECORD - رمزنگاری

Block Cipher		Stream Cipher	
Algorithm	Key Size	Algorithm	Key Size
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		



SSL Record Format



SSL Handshake Protocol

• Client و Server با کمک پروتکل Handshake :

✓ روی نسخه پروتکل موافقت می کنند.

✓ الگوریتمهای رمزنگاری را انتخاب می کنند.

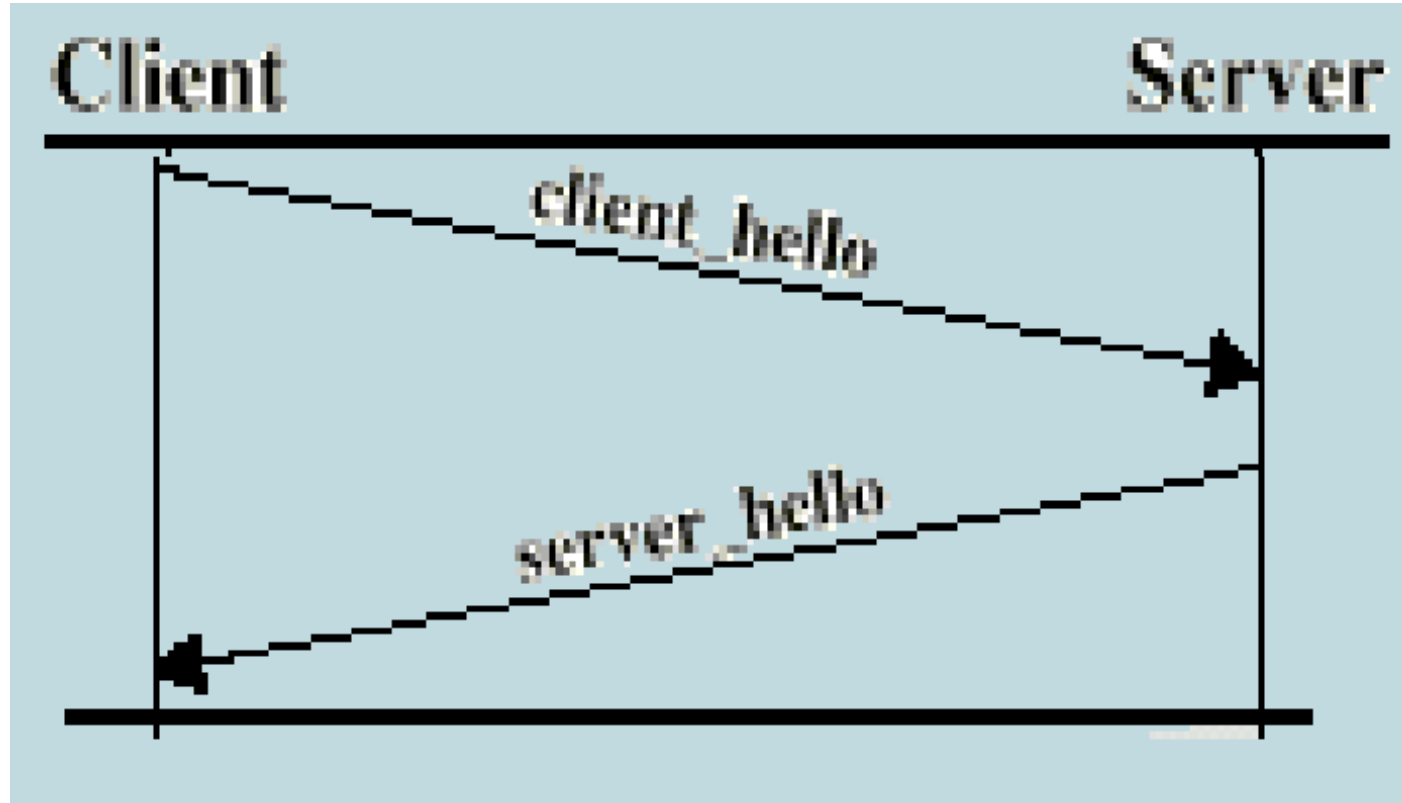
✓ همدیگر را احراز اصالت می کنند (انتخابی).

✓ کلید های مخفی را تولید می کنند.

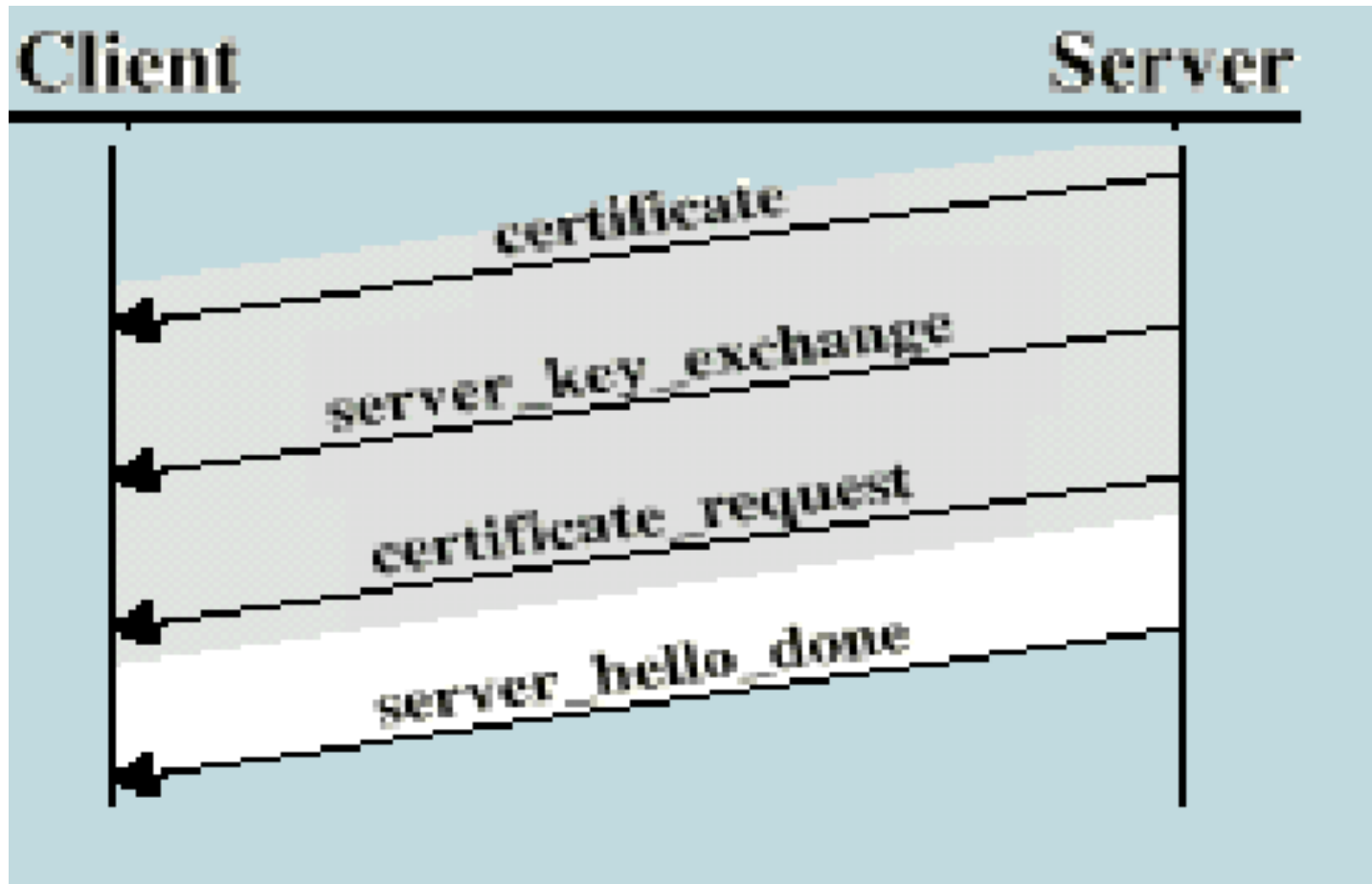
• اگر یک نشست SSL قبلاً ایجاد شده باشد می توان باتوافق طرفین از همان نشست استفاده کرد.



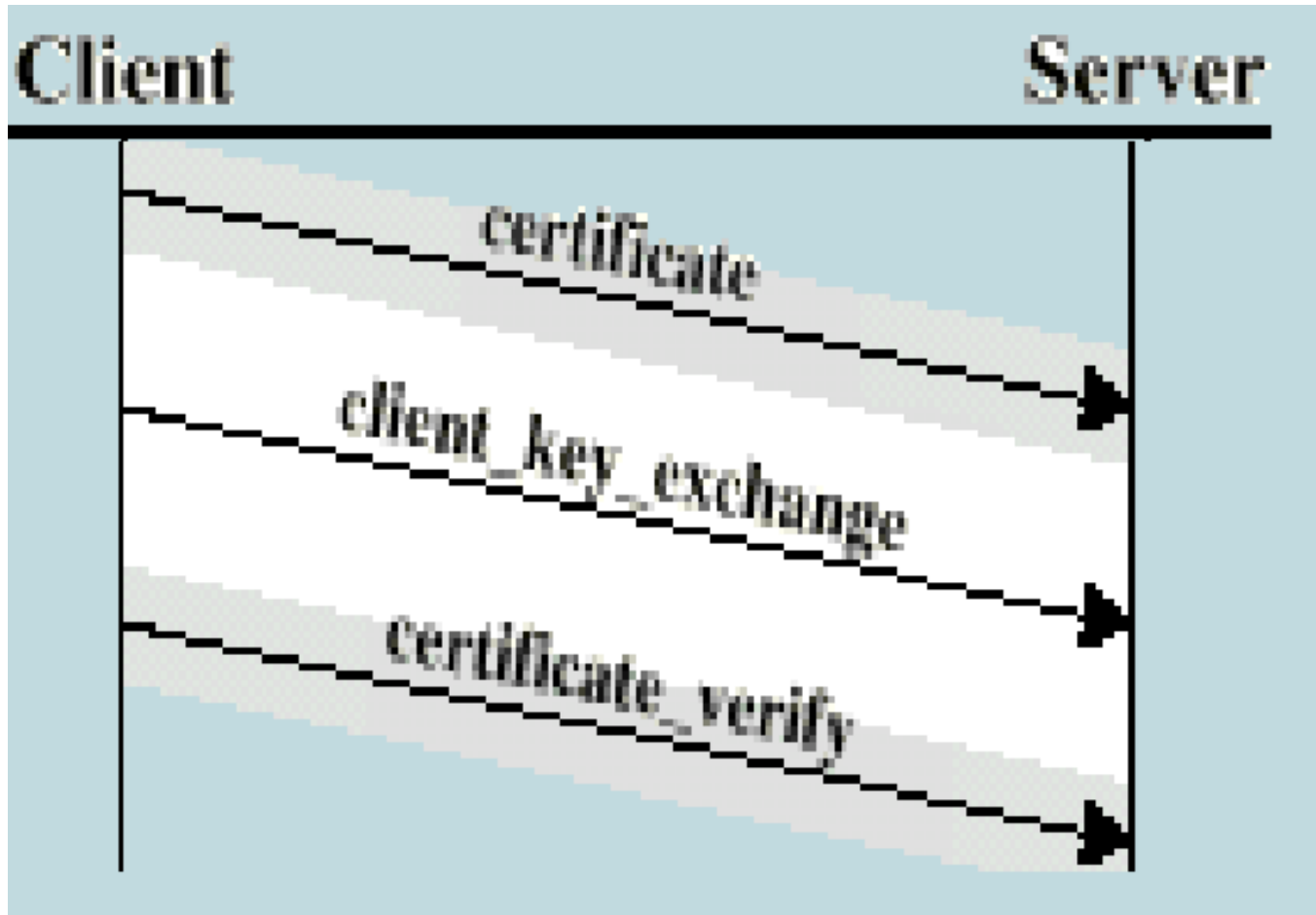
مراحل انجام پروتکل Handshake



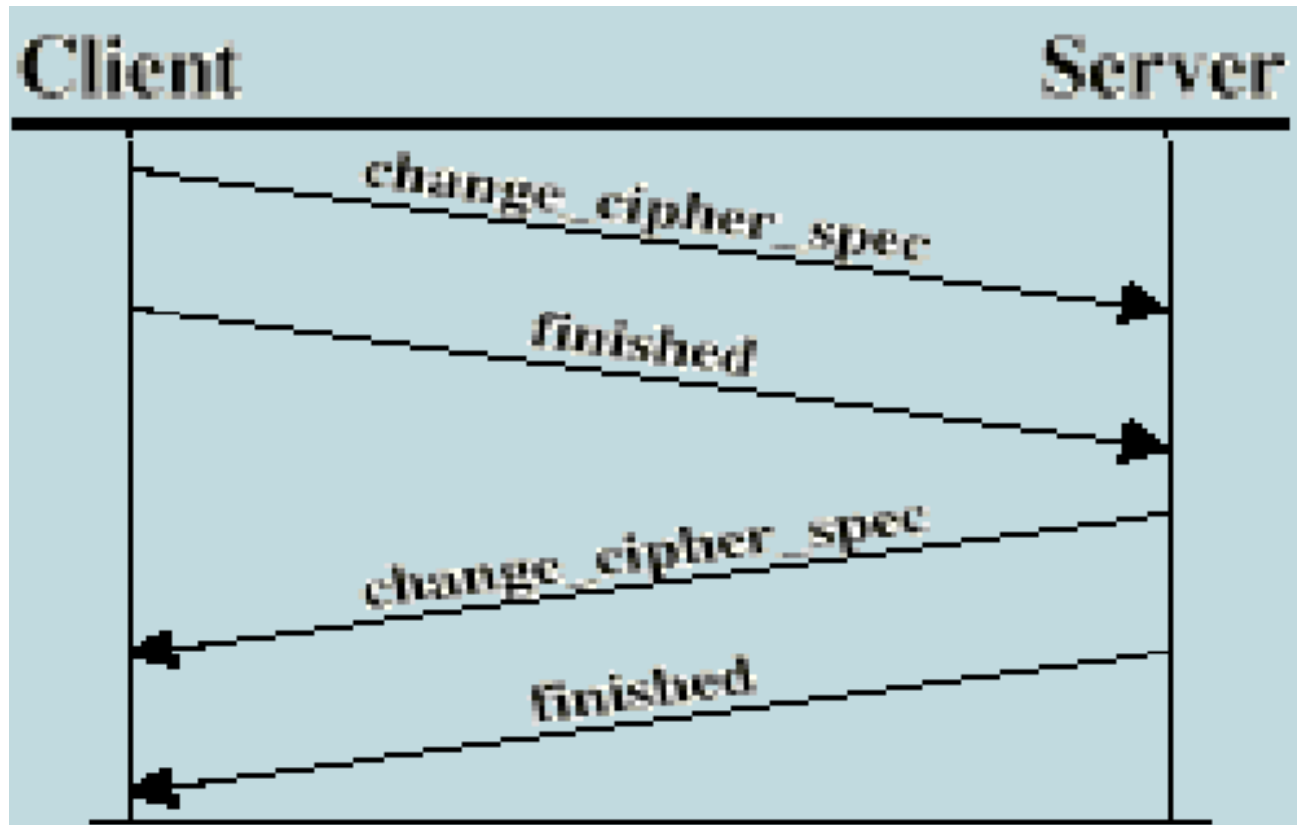
Handshake مراحل انجام پروتکل



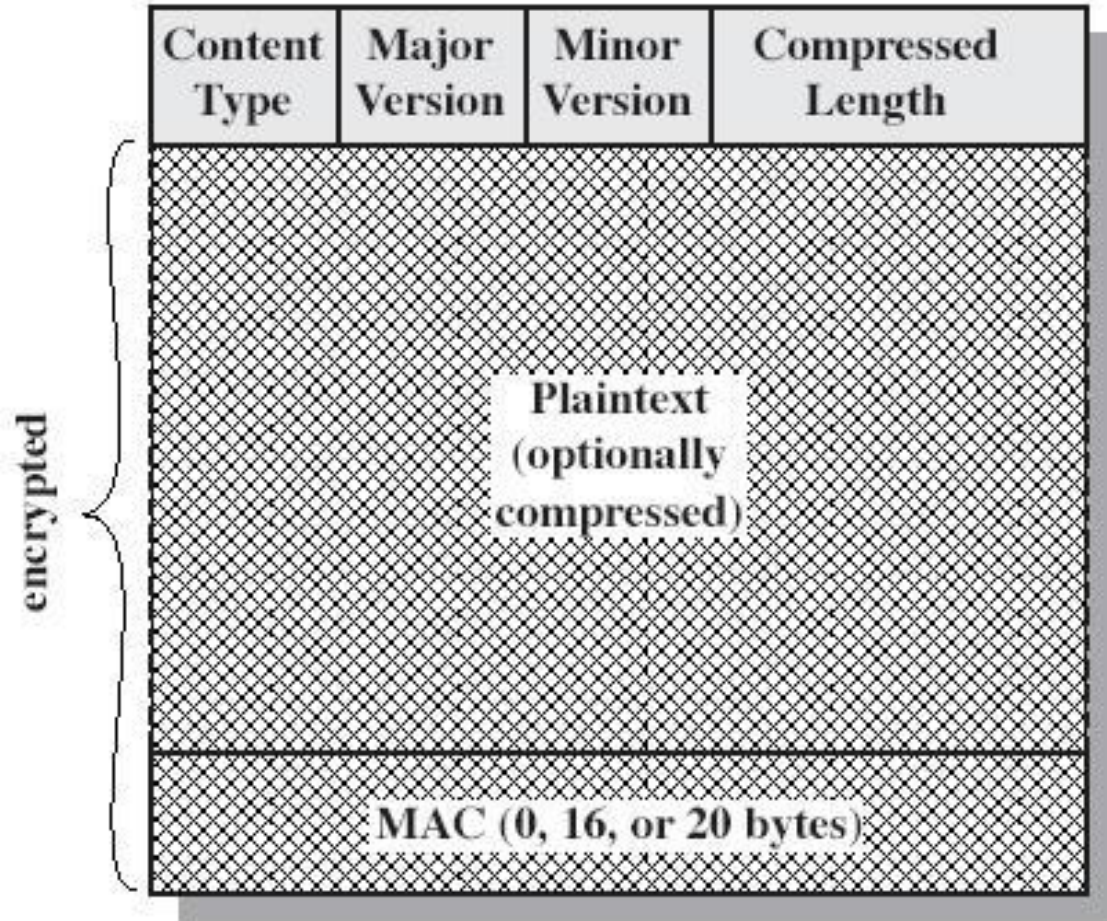
مراحل انجام پروتکل Handshake



مراحل انجام پروتکل Handshake



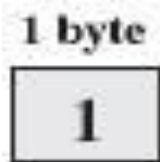
SSL RECORD FORMAT



SSL – پروتکلها

پروتکل Change Cipher Spec:

- یکی از ۳ پروتکل لایه دوم SSL که از پروتکل Record استفاده می کنند.
- شامل ۱ بایت می باشد
- منجر به نوشته شدن مشخصات رمزنگاری معلق (pending) بجای مشخصات فعلی می شود.



SSL – پروتکلها

پروتکل SSL Alert:

- هشدارها و خطاهای مربوط به SSL را به طرف مقابل منتقل می کند
- شدت خطای پیش آمده : Warning or Fatal
- مانند بقیه داده های SSL فشرده سازی و رمزنگاری می شود.
- نمونه خطاها :

unexpected message, bad record mac,
decompression failure, handshake failure

1 byte 1 byte

Level	Alert
-------	-------



SSL – پروتکلها

پروتکل SSL Handshake

- پیش از انتقال هر نوع داده ای تحت SSL انجام می شود.
- با استفاده از آن کارفرما و کارگزار می توانند :
 - همدیگر را شناسایی کنند
 - الگوریتم های رمزنگاری و MAC را رد و بدل کنند
 - کلیدهای متقارن و نامتقارن را رد و بدل کنند



قرارداد توافق

پروتکل SSL Handshake

شامل ۴ فاز اصلی زیر می باشد

- مشخص کردن قابلیت‌های رمزنگاری دو طرف
- احراز هویت کارگزار به کارفرما و مبادله کلیدهای آن
- احراز هویت کارفرما به کارگزار و مبادله کلیدهای آن
- جایگزینی پارامترهای رمزنگاری جدید به جای قبلی و خاتمه توافق



قرارداد توافق – فاز HELLO

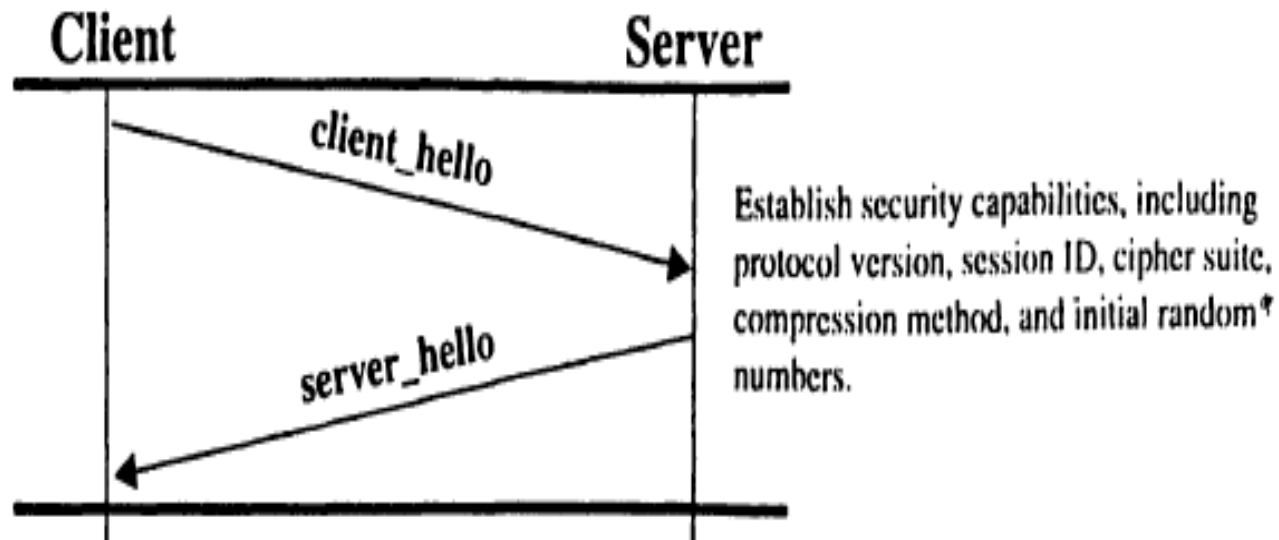
ارسال پیام Hello توسط کارفرما (آغازگر جلسه)

- پیشنهاد نسخه قرارداد
- پیشنهاد الگوریتم های مناسب
- پیشنهاد مکانیسم فشرده سازی مناسب
- انتخاب نسخه و الگوریتم های مورد قبول کارگزار
- کارگزار بررسی می کند که آیا این پیشنهاد قابل قبول است یا نه؟



PHASE 1: ESTABLISH SECURITY CAPABILITIES

- Client hello(Version,Random,Session ID,CipherSuite,Compression Method)

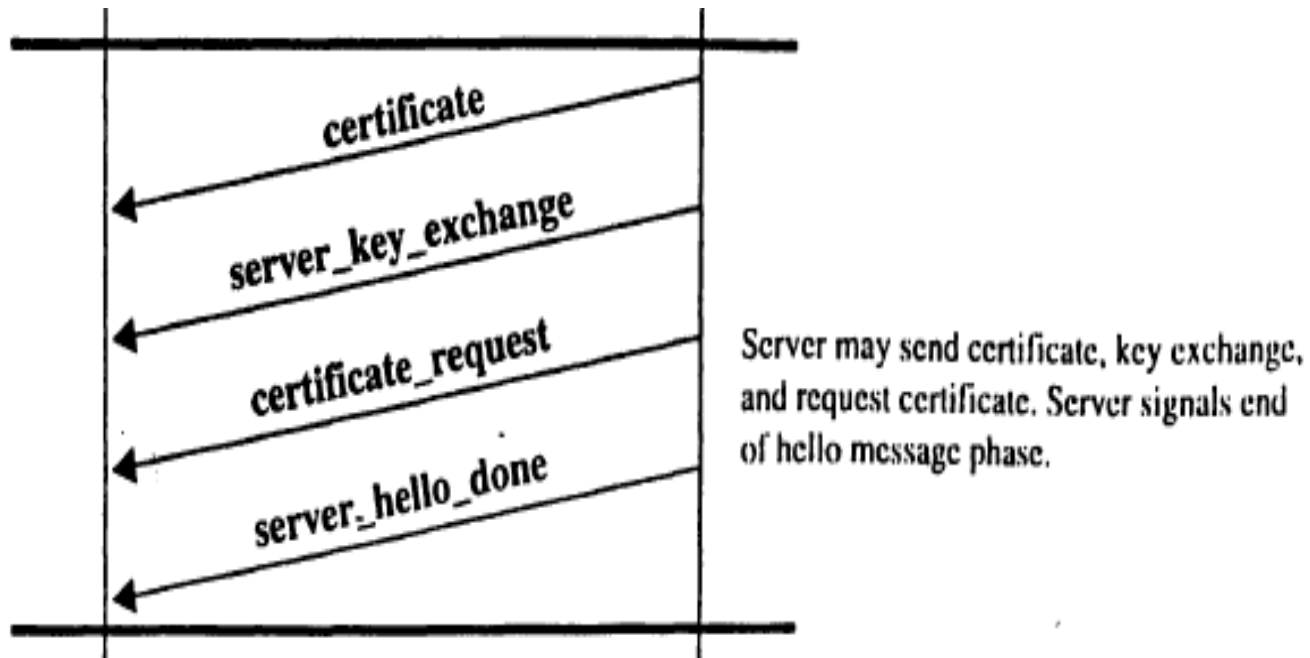


قرارداد توافق – فاز تبادل کلید

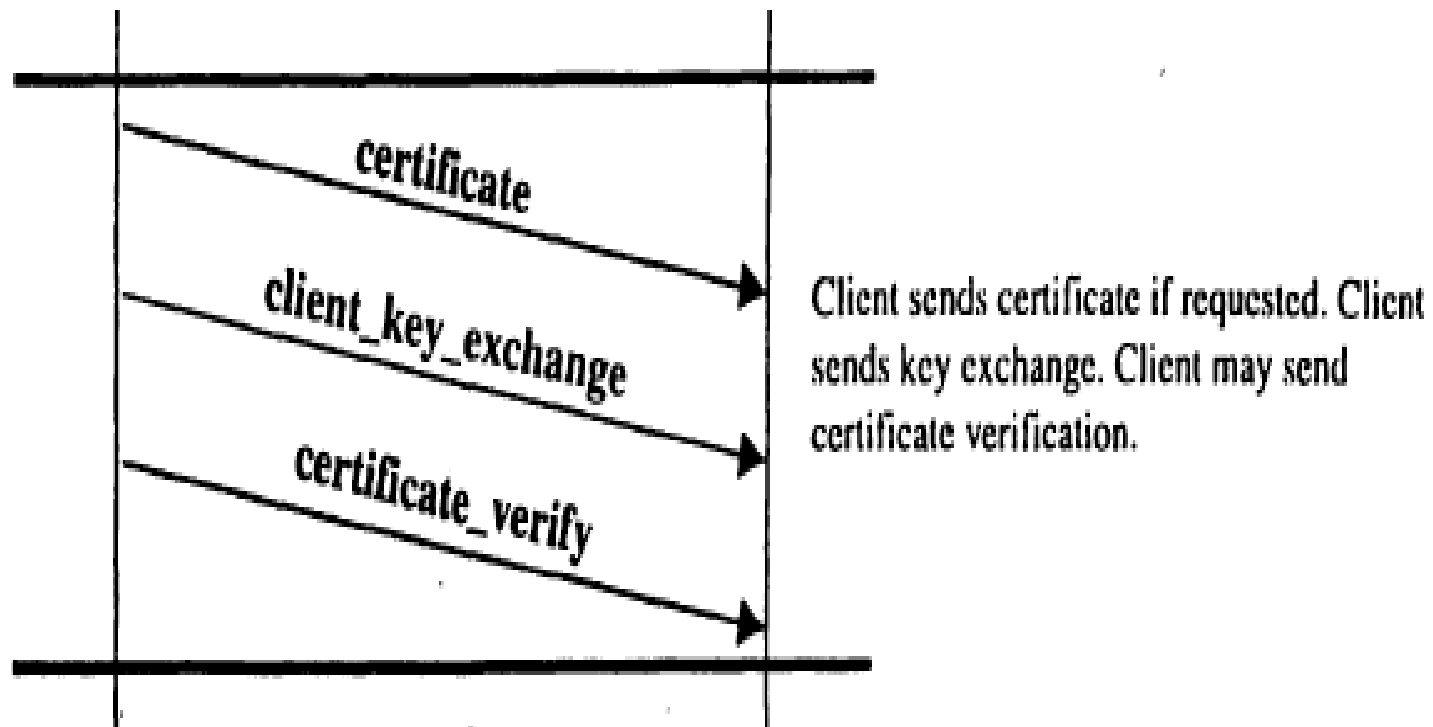
- ارسال گواهی کارگزار برای کارفرما
 - همراه با کلید عمومی (RSA) یا پارامترهای DH
- تولید و ارسال سری کلید
 - کارفرما کلید سری را تولید کرده و برای کارگزار می فرستد
 - یا اینکه هر دو با استفاده از پارامترهای DH کلید سری را محاسبه می کنند.



PHASE 2: SERVER AUTHENTICATION & KEY EXCHANGE



PHASE 3: CLIENT AUTHENTICATION & KEY EXCHANGE



قرارداد توافق – فاز خاتمه

○ فعال کردن قرارداد تغییر مشخصات رمز

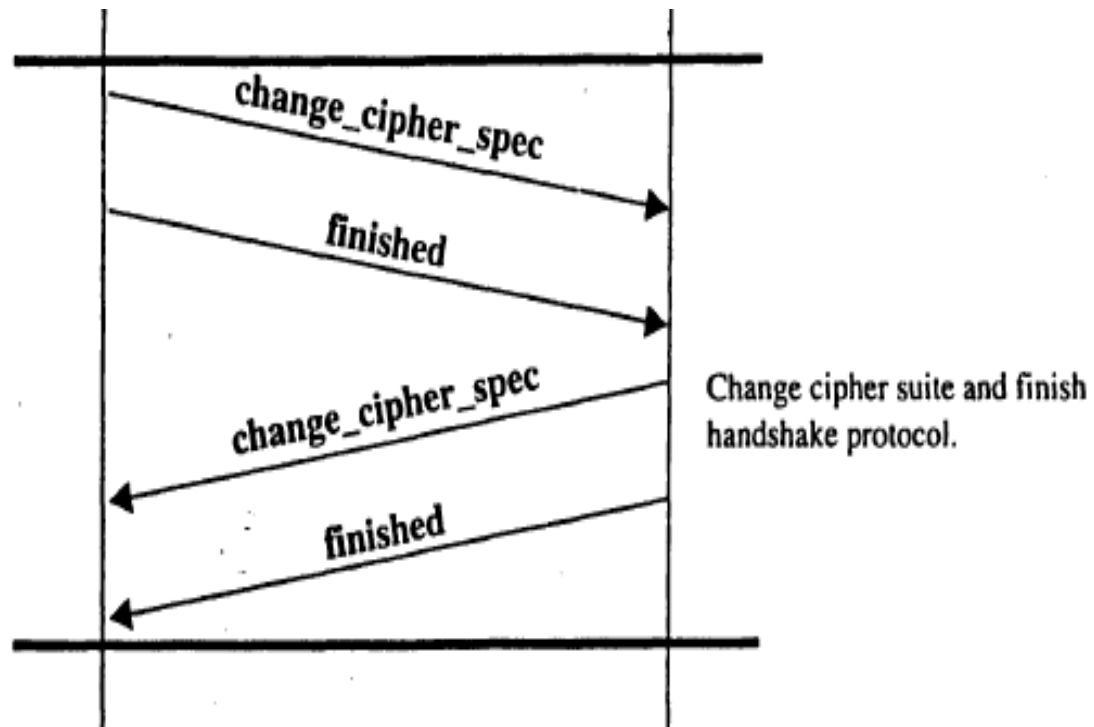
- کارفرما قرارداد تغییر مشخصات رمز را فعال کرده و برای کارگزار می فرستد.
- کارگزار نیز قرارداد مشخصات رمز را فعال کرده و ارسال می کند.

○ پایان

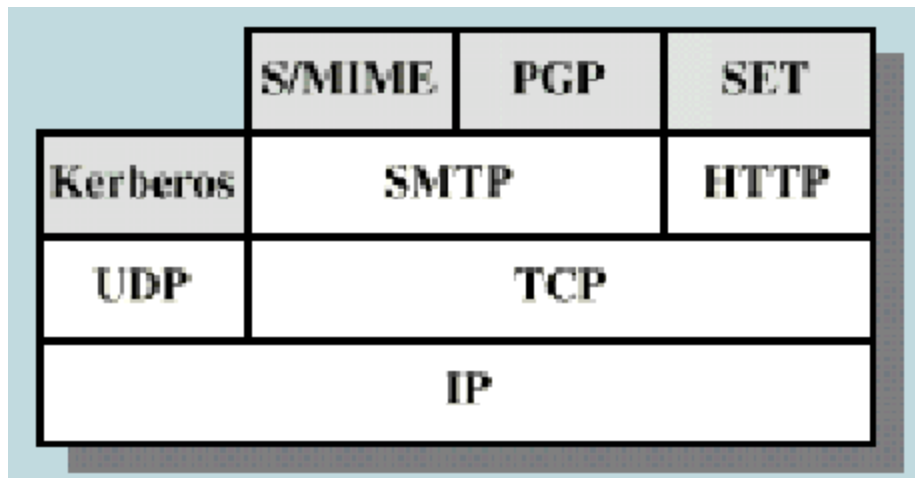
- ارسال پیغام پایانی
- آغاز تبادل اطلاعات بصورت محرمانه و با پارامترهای جدید



PHASE 4: FINISH



ایجاد امنیت در لایه کاربرد



+ سرویسهای امنیتی از دید شبکه شفاف هستند
- لایه کاربرد - سرویسهای امنیتی برای هر کاربر بایستی بطور مجزا طراحی و پیاده شوند

امنیت داده ها

امنیت در لایه انتقال و کاربرد فصل پانزدهم :

دکتر یعقوب فرجامی

عضو هیات علمی دانشکده فنی قم

مفاهیم

- امنیت می تواند در لایه های مختلف شبکه تعریف شود
- با اینکه امنیت در لایه های پایین تر وجود دارد، متخصصین و خبرگان به امنیت کمتر از «انتها به انتها» راضی نمی شوند (End to End Security)

○ مفهوم امنیت در لایه انتقال

SSL(Security Sockets Layer)

TSL(Transport Layer Security)

○ مفهوم امنیت در لایه کاربرد

PGP(Pretty Good Privacy)



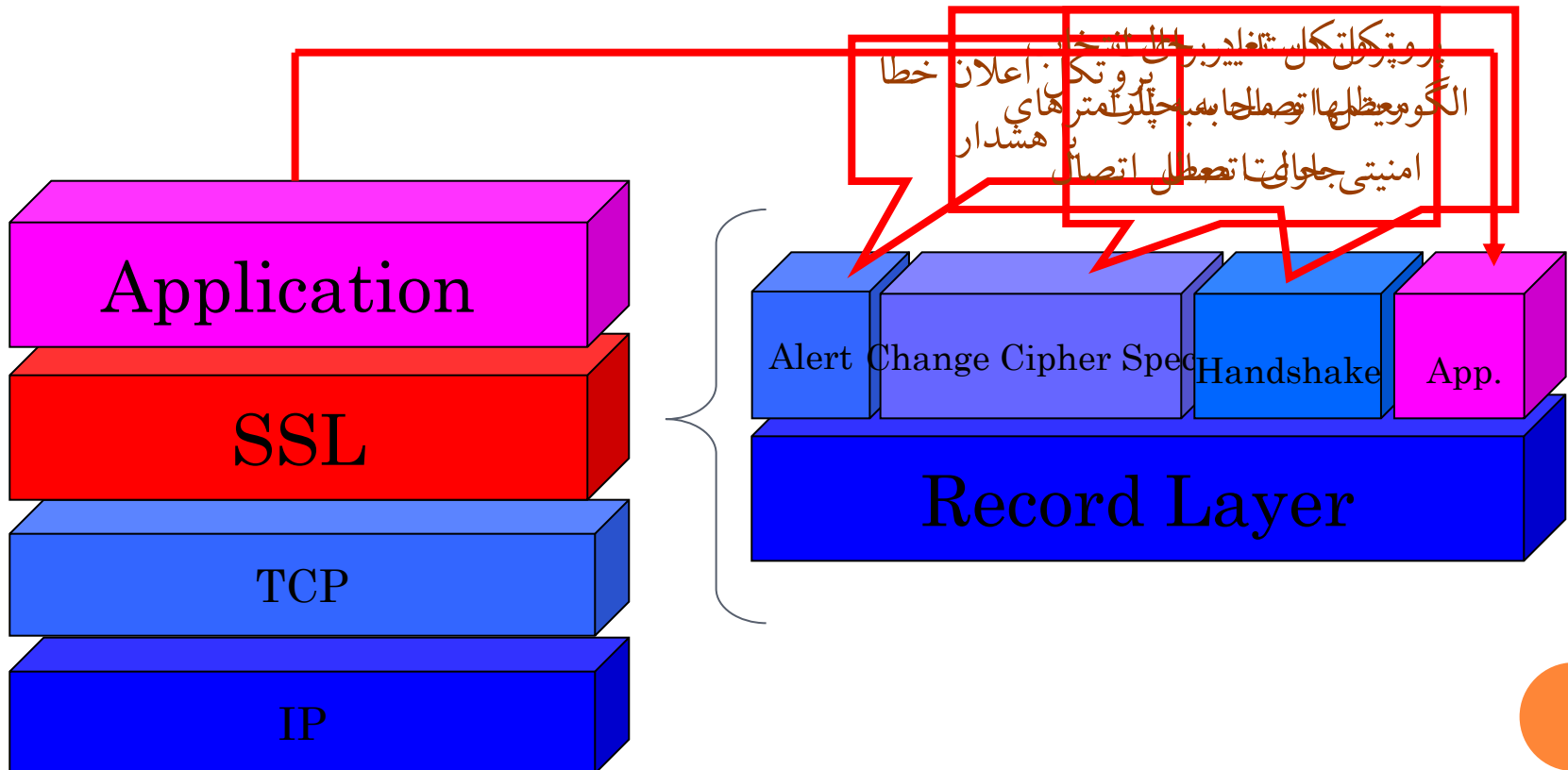
SSL ○

- لایه ای امنیتی بر روی لایه انتقال
- تلاشی برای پر کردن جای خالی لایه نمایش (Presentation) مدل هفت لایه ای OSI (نبود این لایه در مدل TCP/IP)
- اگر برنامه ای نیاز به اتصالی امن داشته باشد باید از طریق SSL، سوکتی ایجاد کرده تا شامل خدمات زیر شود :
 - مذاکره مقدماتی و توافق بر سر پارامترها و الگوریتم های امنیتی
 - احراز هویت سرور و مشتری به صورت کامل و مجزا
 - تبادل اطلاعات به صورت رمزنگاری شده
 - بررسی صحت و اصالت داده ها
 - فشرده سازی داده ها (اختیاری)
- نکته : جایگاه دقیق SSL بین برنامه کاربردی و لایه TCP است



SSL

SSL یک لایه مجزا است که تنها برای برقراری امنیت به معماری اینترنت اضافه می شود.



SSL



SSL فرآیند دست تکانی در

- این فرآیند برای مذاکره بر سر گزینه های امنیتی و مبادله کلید است
- انواع پیام ها :

1. Client Hello
2. Server Hello
3. Server Authentication
4. Certificate Request
5. Certificate
6. Client Key Exchange
7. Client Change Cipher
8. Client Finished
9. Server Change Cipher
10. Server Finished



SSL فرآیند دست تکانی در

Client Hello : مشتری با ارسال این پیام تمایل خود را برای ایجاد یک نشست امن اعلام می کند که دارای فیلدهای زیر است :

1. Protocol Version Supported : شماره نسخه ای از SSL که توسط مشتری حمایت می شود

2. Session ID : برای احیاء نشست که قبلاً وجود داشته است

3. Cipher Suite : فهرستی از الگوریتم های مورد حمایت مشتری

4. Compression Method : فهرستی از روش های فشرده سازی مورد حمایت مشتری

5. Nonce : عددی تصادفی برای جلوگیری از حمله تکرار



SSL فرآیند دست تکانی در

Server Hello : در پاسخ سلام مشتری خواهد بود و شامل فیلدهای زیر :

1. Approved Protocol Version : شماره نسخه مورد پذیرش سرور برای SSL

2. Session ID : شناسه نشست جاری به پیشنهاد سرور

3. Approved Cipher Suite : پذیرش یکی از الگوریتم های پیشنهادی مشتری برای الگوریتم نامتقارن به منظور تبادل کلید (متقارن) نشست، مانند RSA

4. Approved Compression Method : پذیرش یکی از روش های پیشنهادی مشتری برای فشرده سازی

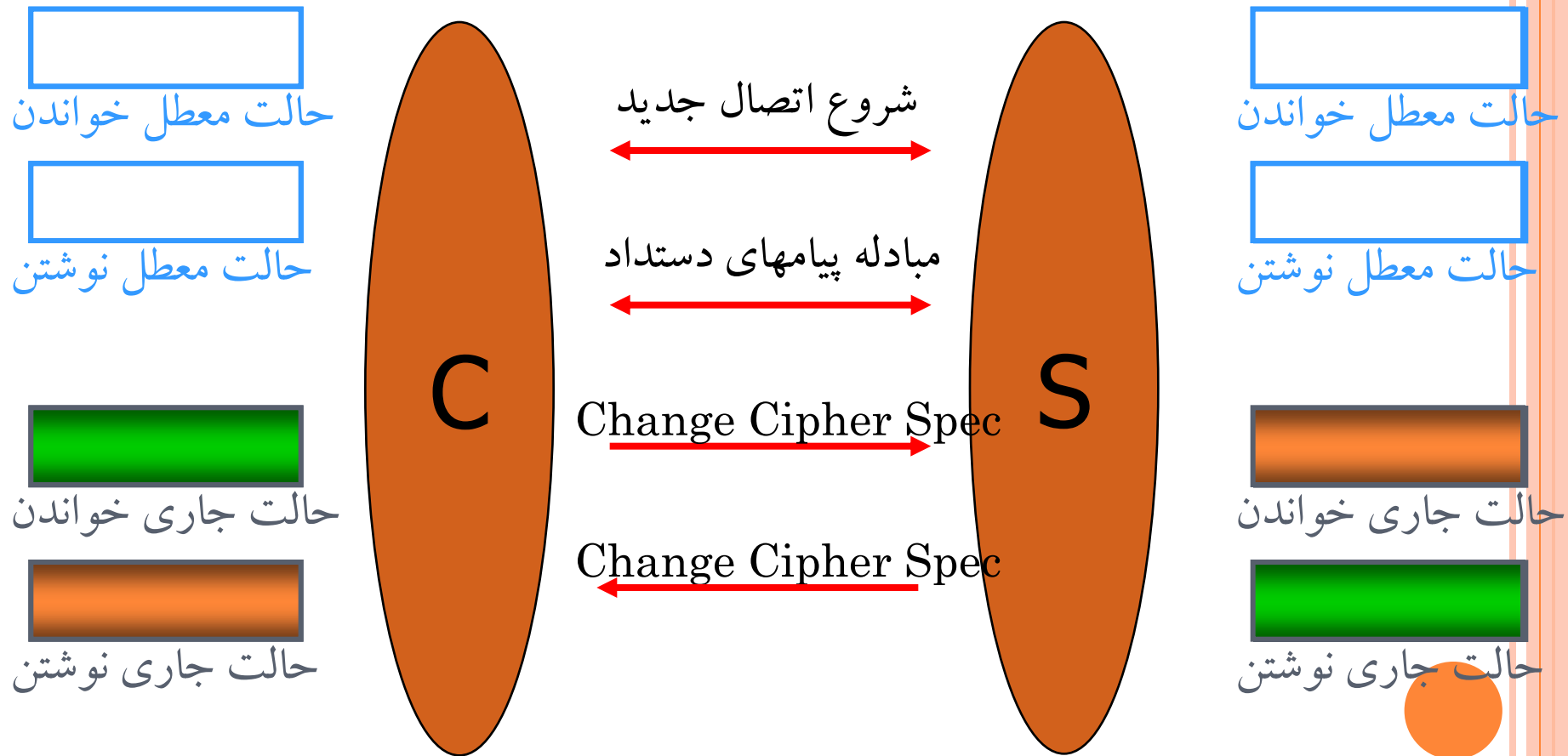


SSL فرآیند دست تکانی در

- Server Authentication : ارسال گواهینامه x.509 سرور برای مشتری
- Certificate Request : مطالبه گواهینامه مشتری از طرف سرور (اختیاری)
- Certificate : پاسخی به پیام قبلی از طرف مشتری به سرور (گواهینامه مشتری)
- Client Key Exchange : انتخاب کلید اولیه توسط مشتری که با کلید عمومی سرور رمز شده و ارسال می گردد
- Client Change Cipher : مشتری خواستار تغییر روش رمزنگاری به الگوریتم توافقی از سرور است
- Client Finished : ختم فرآیند دست تکانی از سمت مشتری
- Server Change Cipher : موافقت سرور برای تغییر روش رمزنگاری
- Server Finished : موافقت سرور با ختم فرآیند دست تکانی



حالات چهارگانه اتصال



فرآیند دست تکانی در SSL

Client Hello

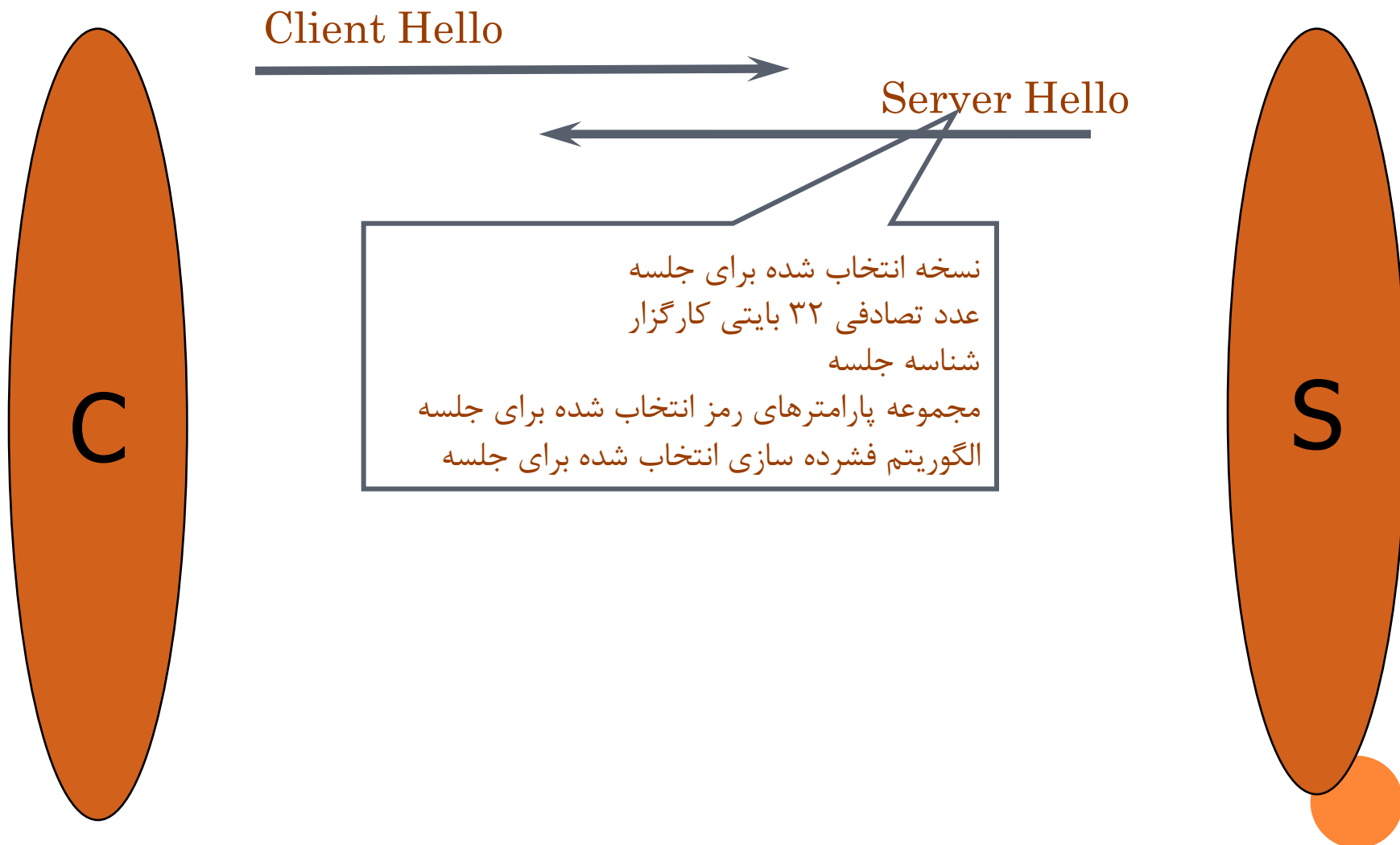


بالاترین نسخه قابل حمایت کارفرما
عدد تصادفی ۳۲ بیتی کارفرما
شناسه جلسه
لیست مجموعه پارامترهای رمز قابل حمایت کارفرما
لیست روشهای فشرده سازی قابل حمایت کارفرما

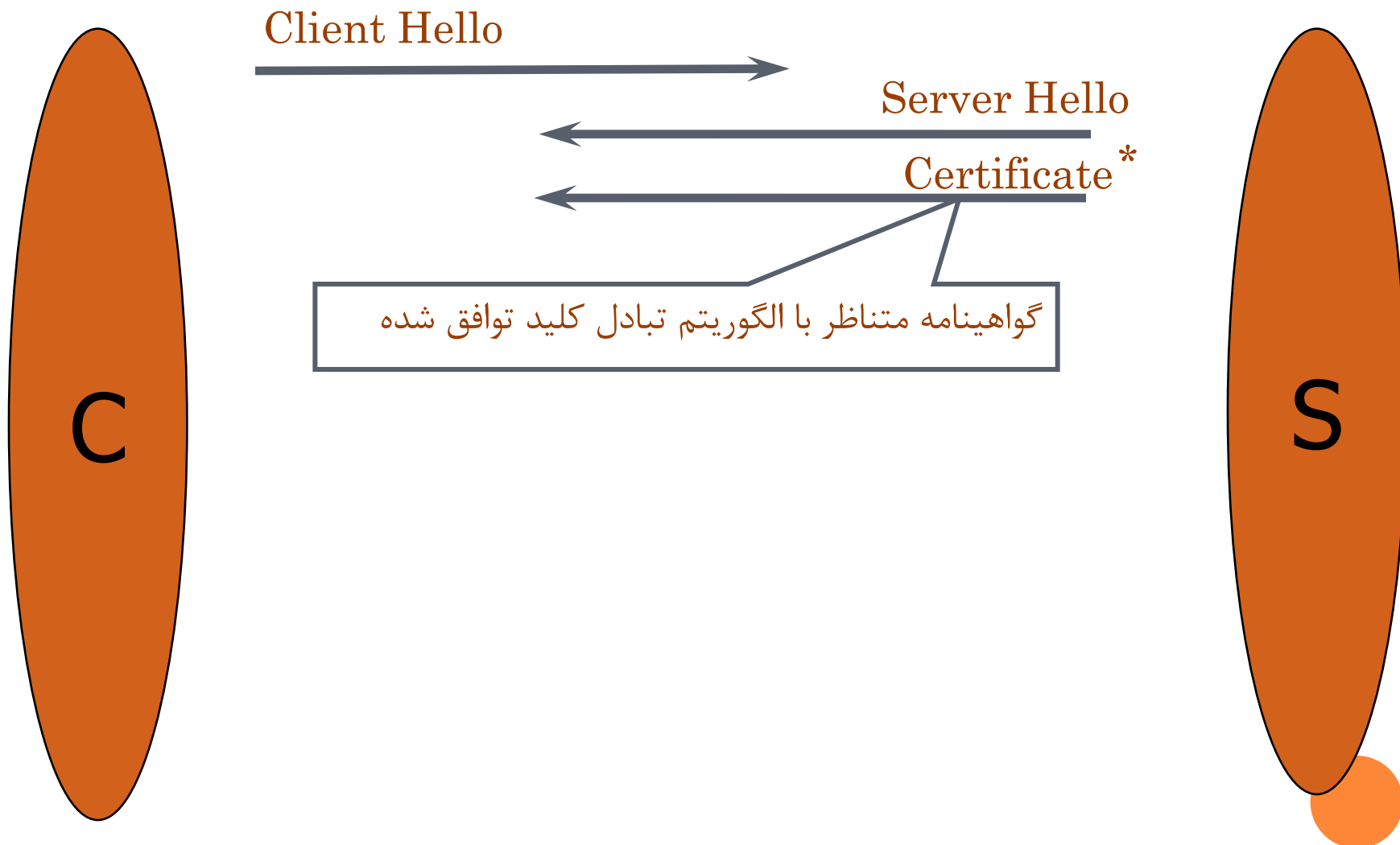
S

مجموعه پارامترهای رمز شامل الگوریتم تبادل کلید، الگوریتم رمز گذاری،
الگوریتم احراز اصالت و همچنین طول کلیدها می باشد.

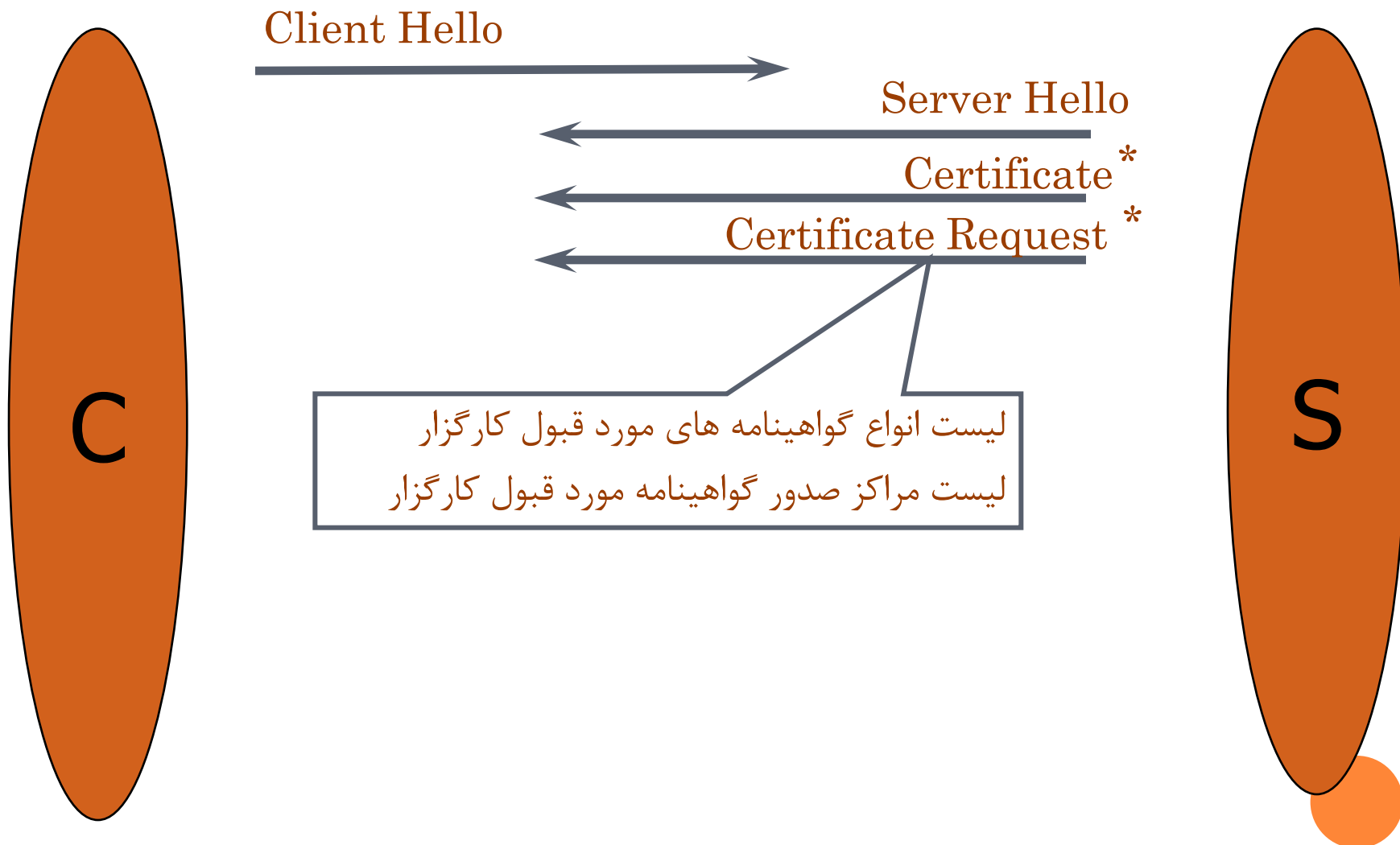
فرآیند دست تکانی در SSL



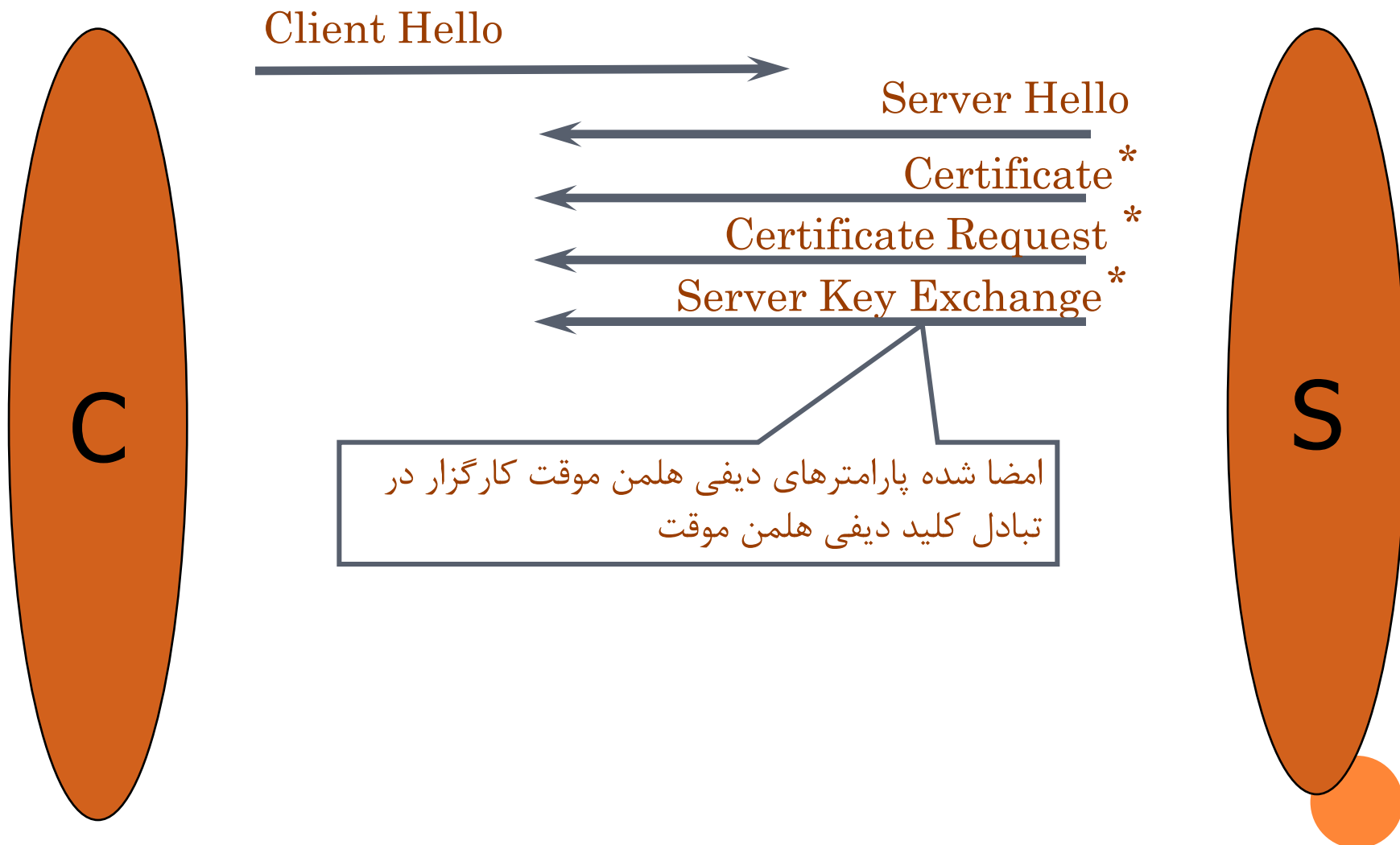
فرآیند دست تکانی در SSL



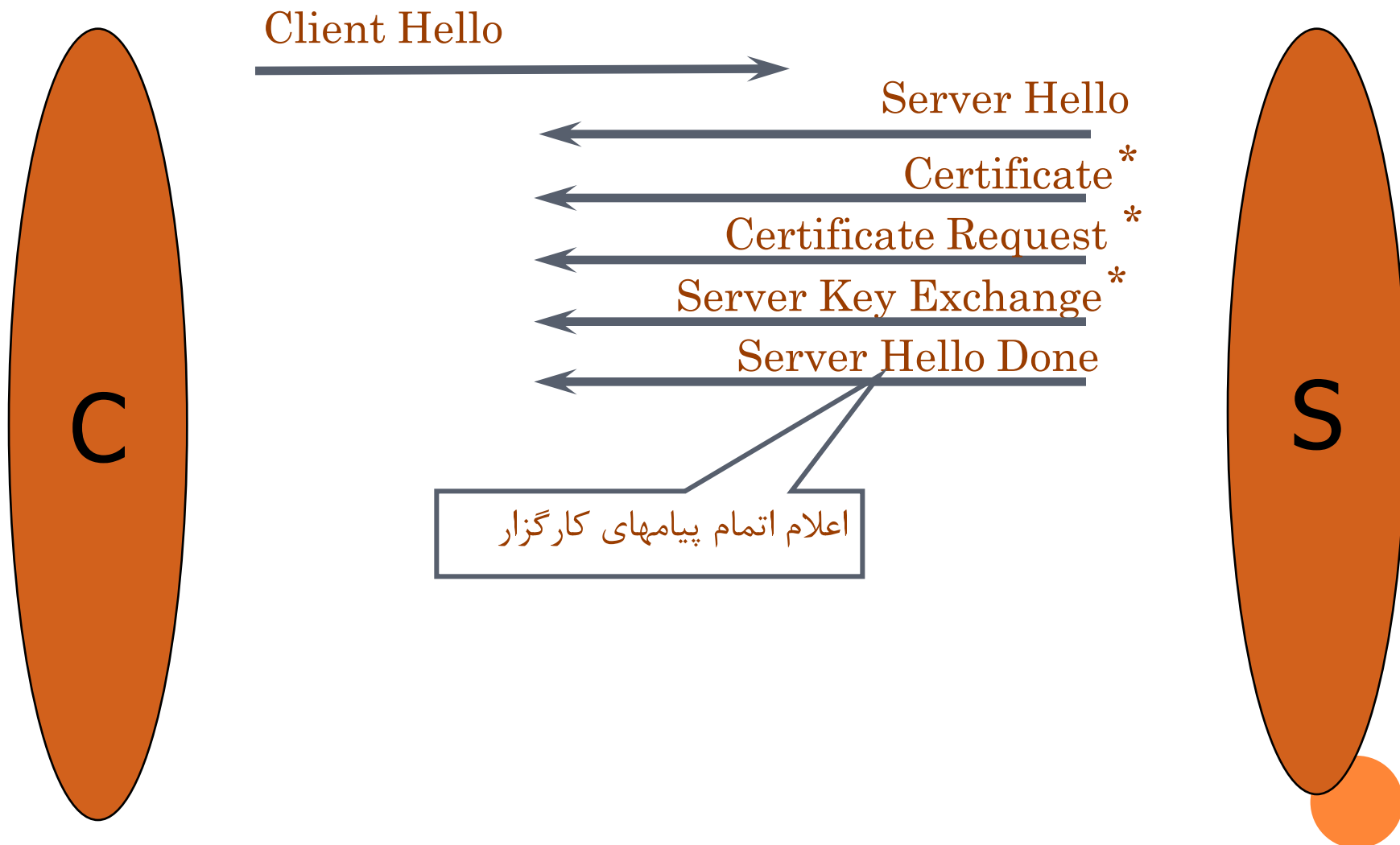
فرآیند دست تکانی در SSL



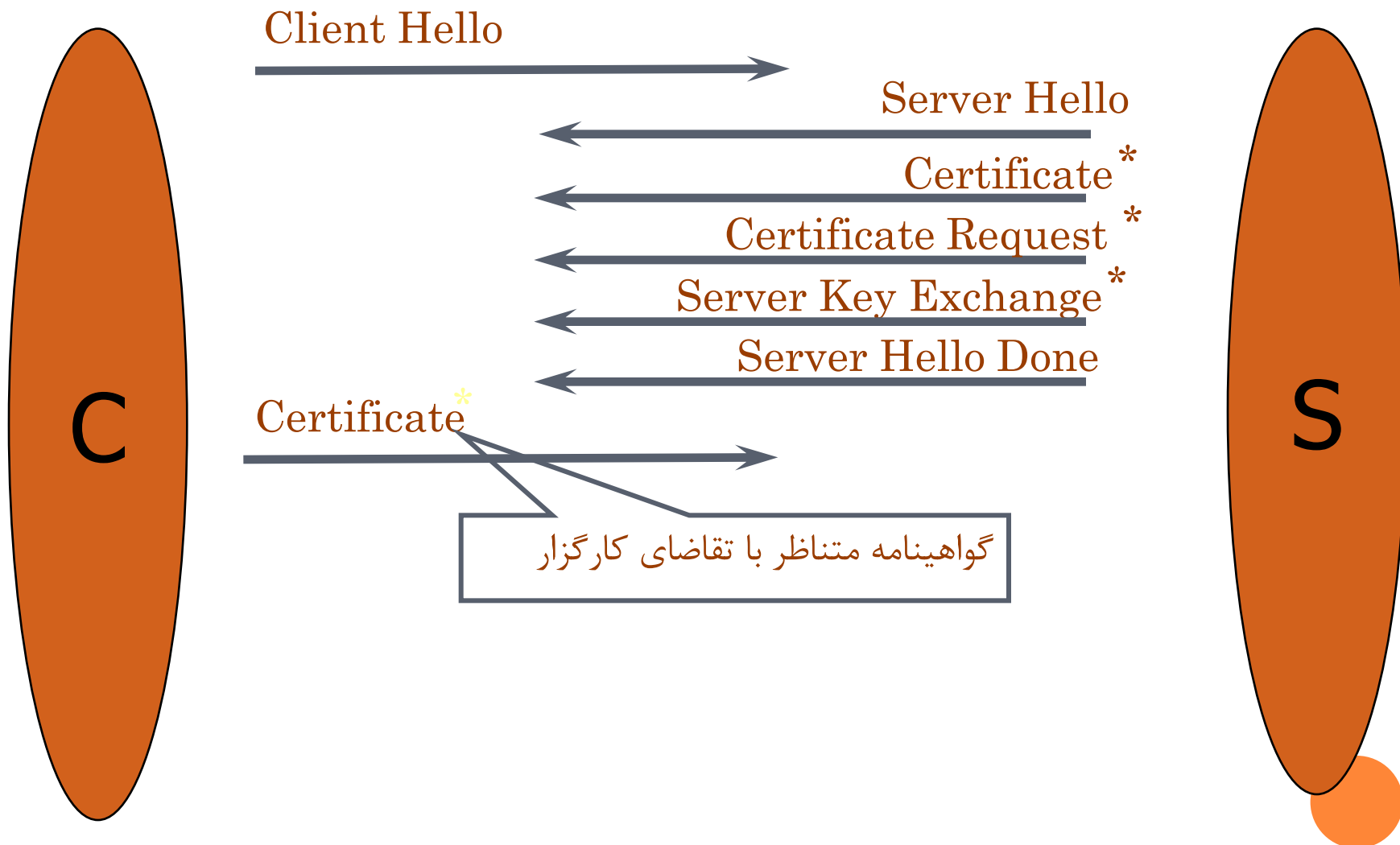
فرآیند دست تکانی در SSL



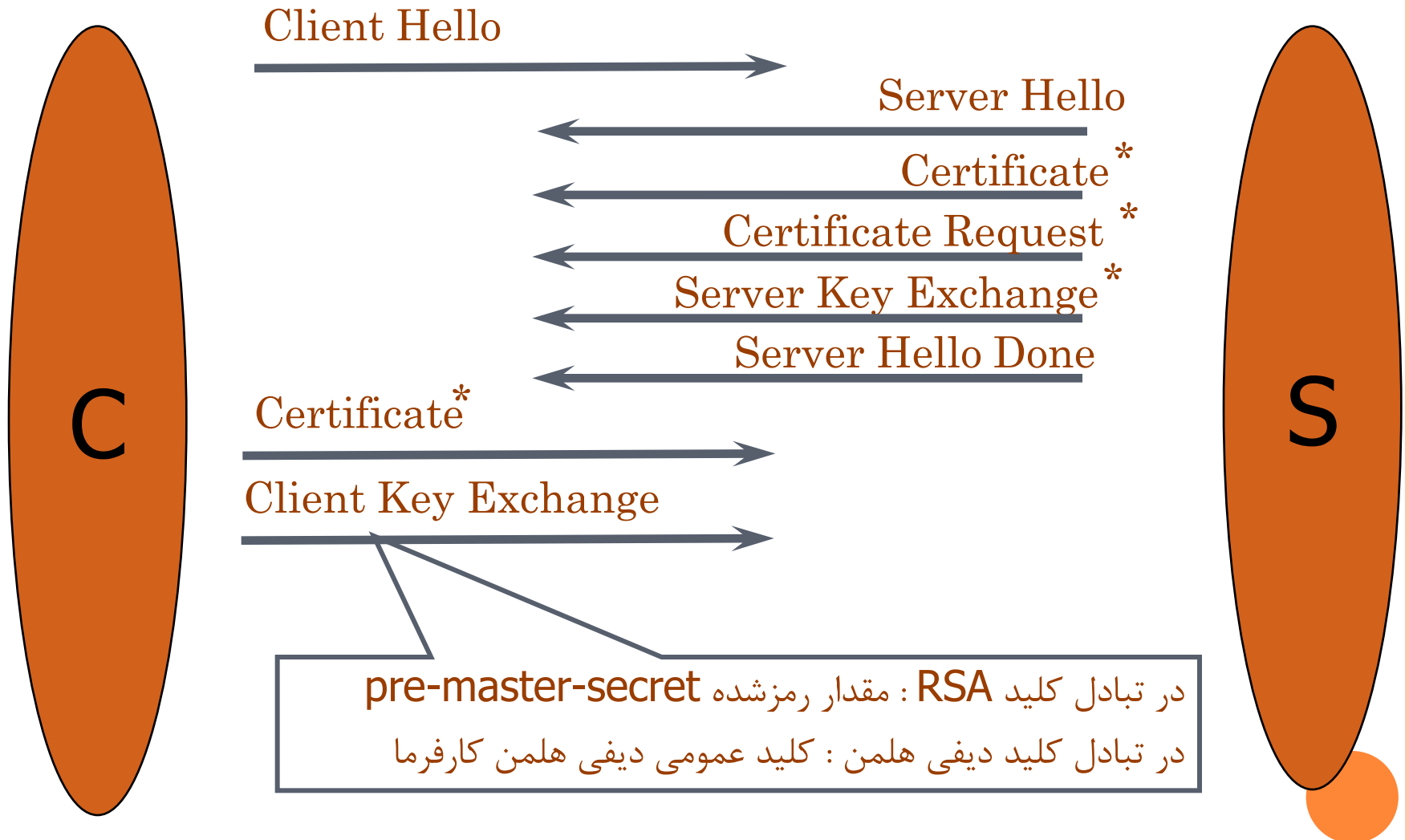
فرآیند دست تکانی در SSL



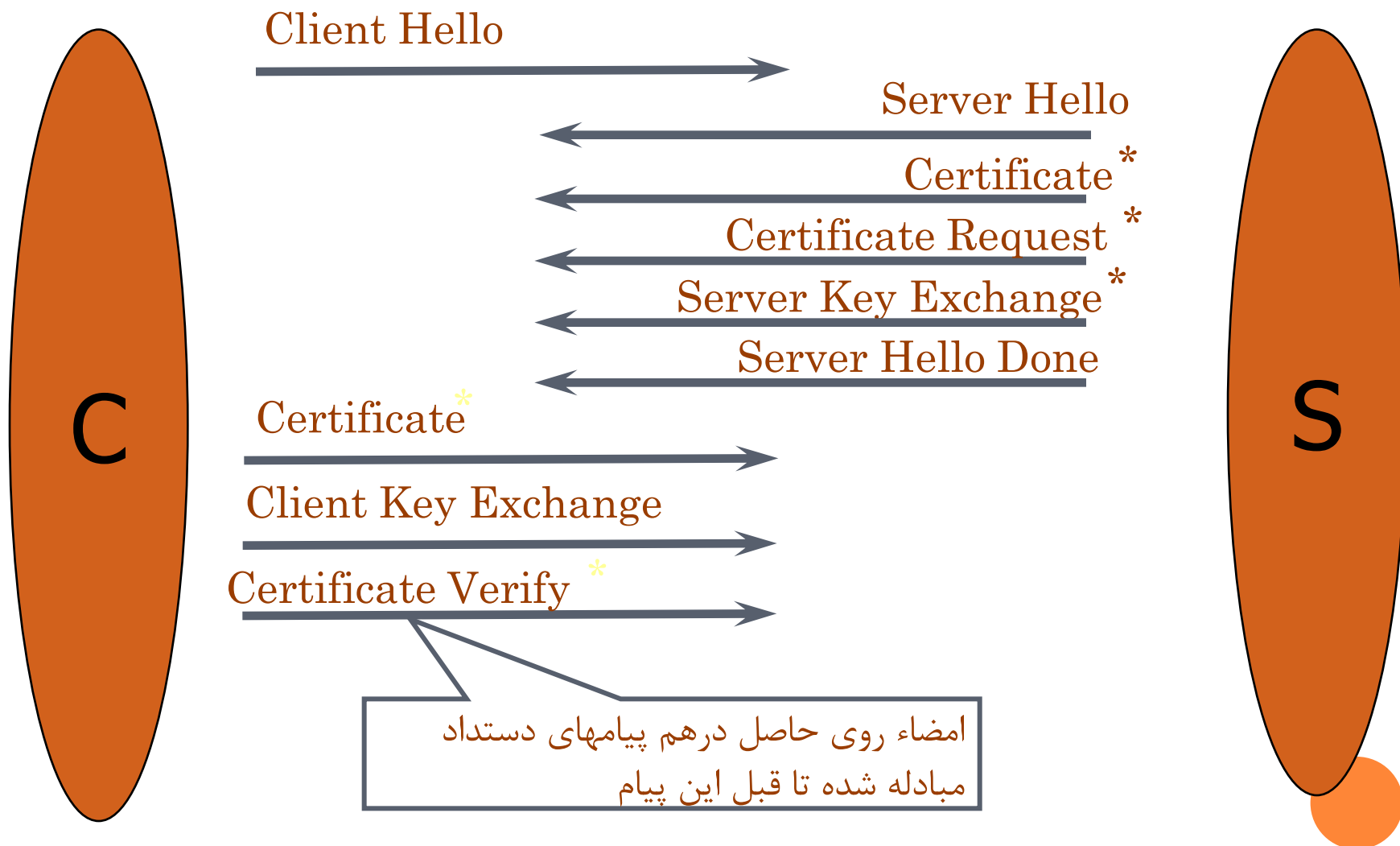
فرآیند دست تکانی در SSL



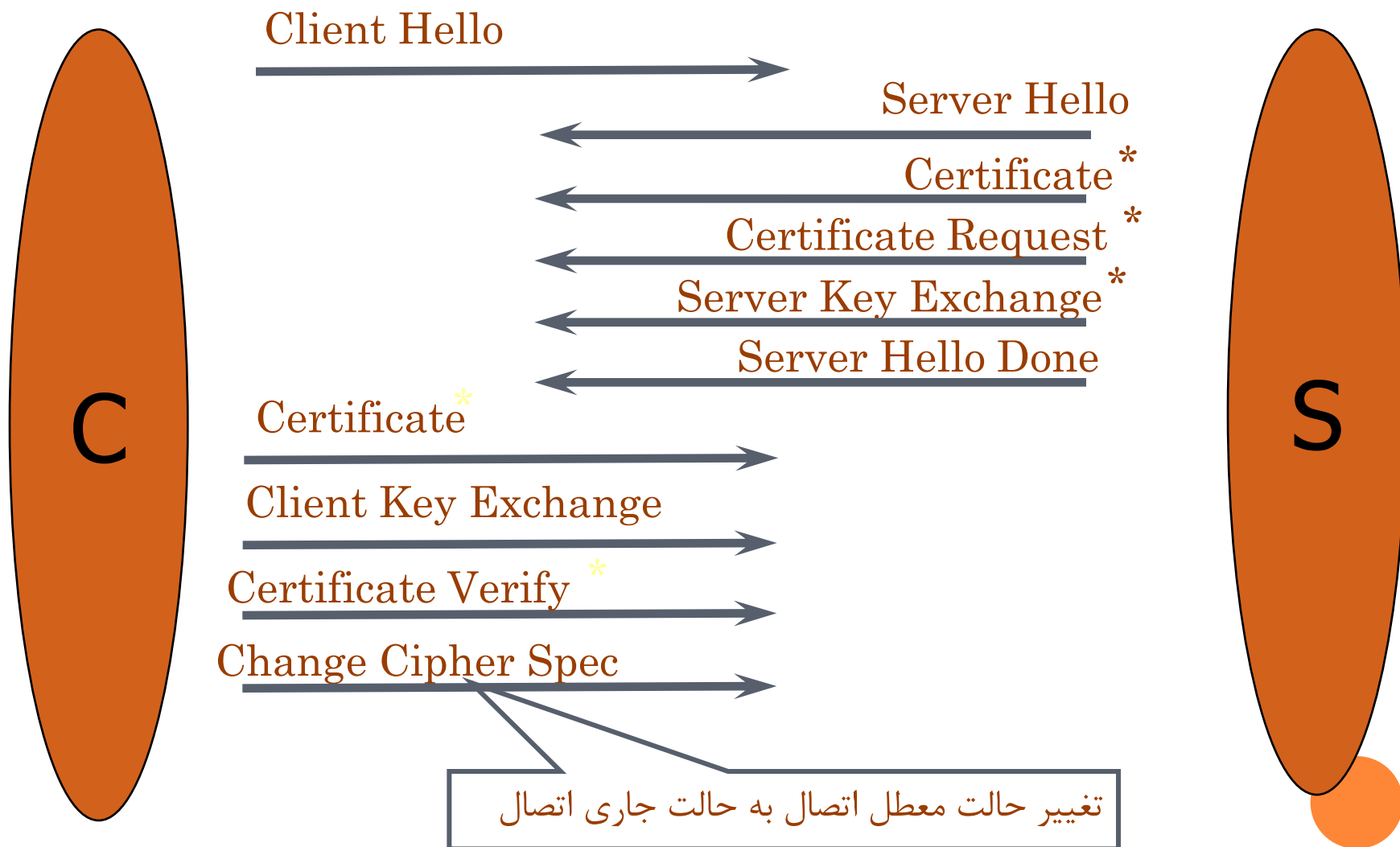
فرآیند دست تکانی در SSL



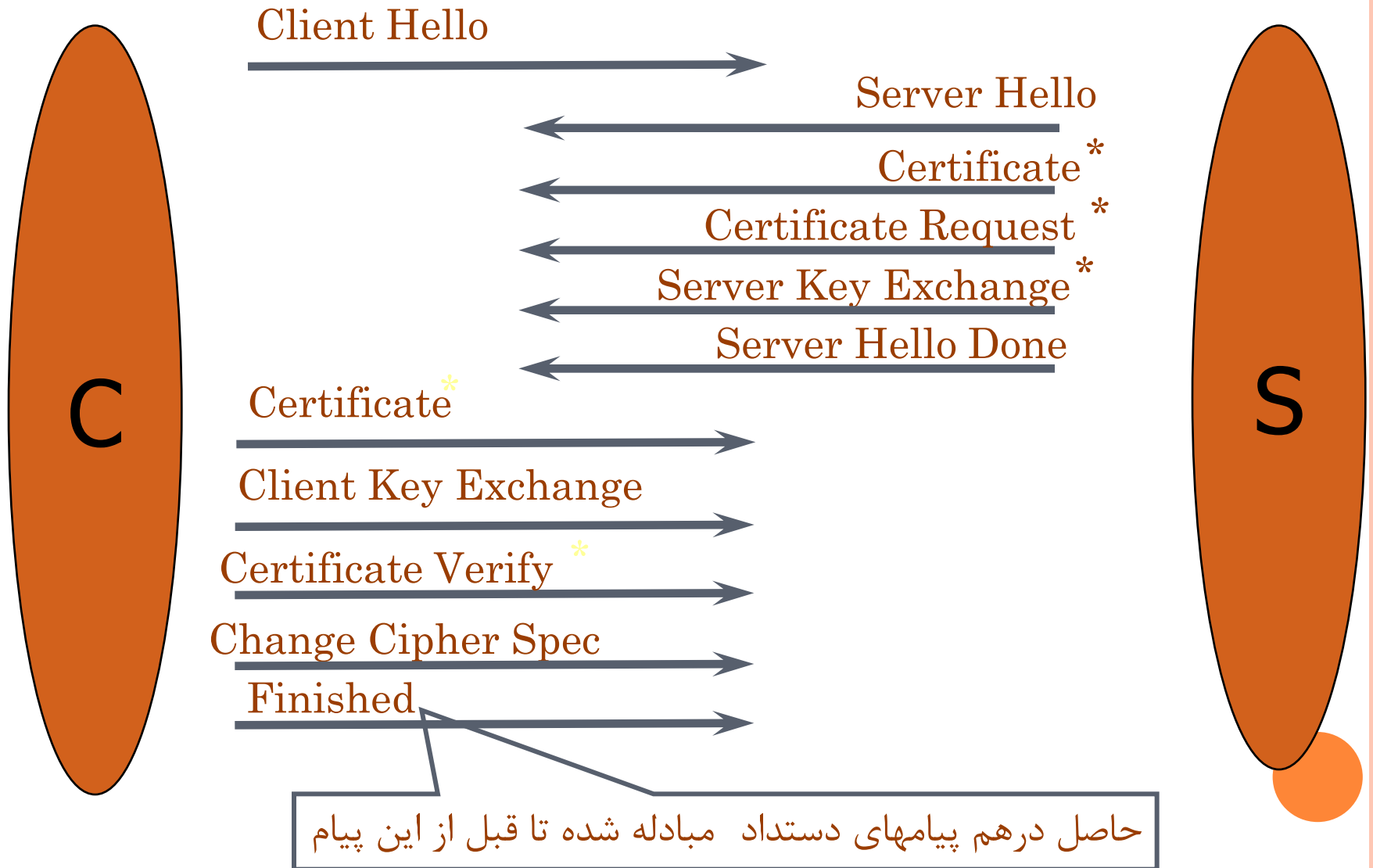
فرآیند دست تکانی در SSL



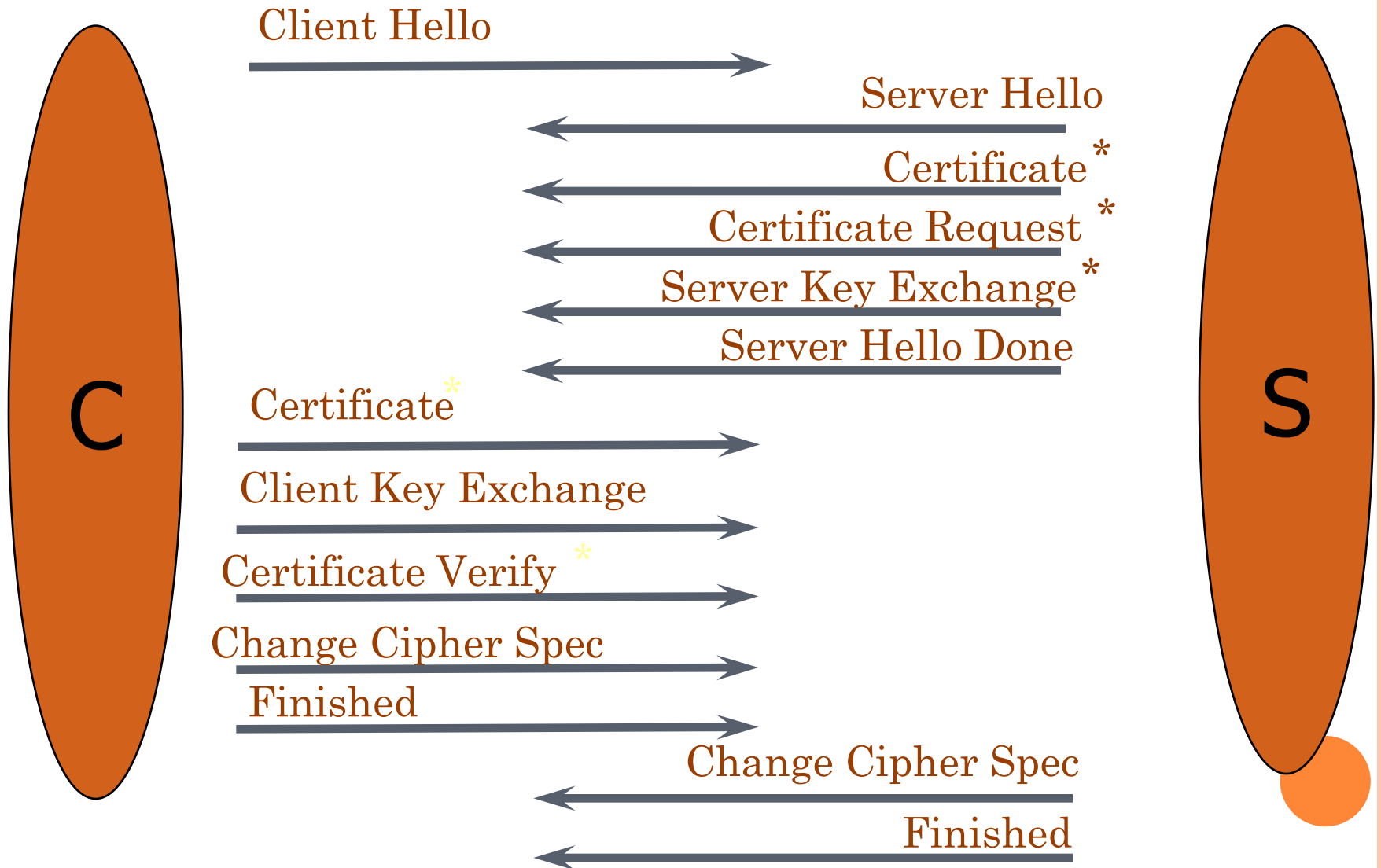
فرآیند دست تکانی در SSL



فرآیند دست تکانی در SSL



فرآیند دست تکانی در SSL



SSL فرآیند دست تکانی در

○ موارد رمزنگاری در SSL

- RSA و دیفی_هلمن برای مبادله کلید
- DES، 3DES، RC2 و RC4 برای بدنه داده ها
- MD5 و SHA-1 برای امضاء دیجیتال



SSL فرآیند تبادل داده در

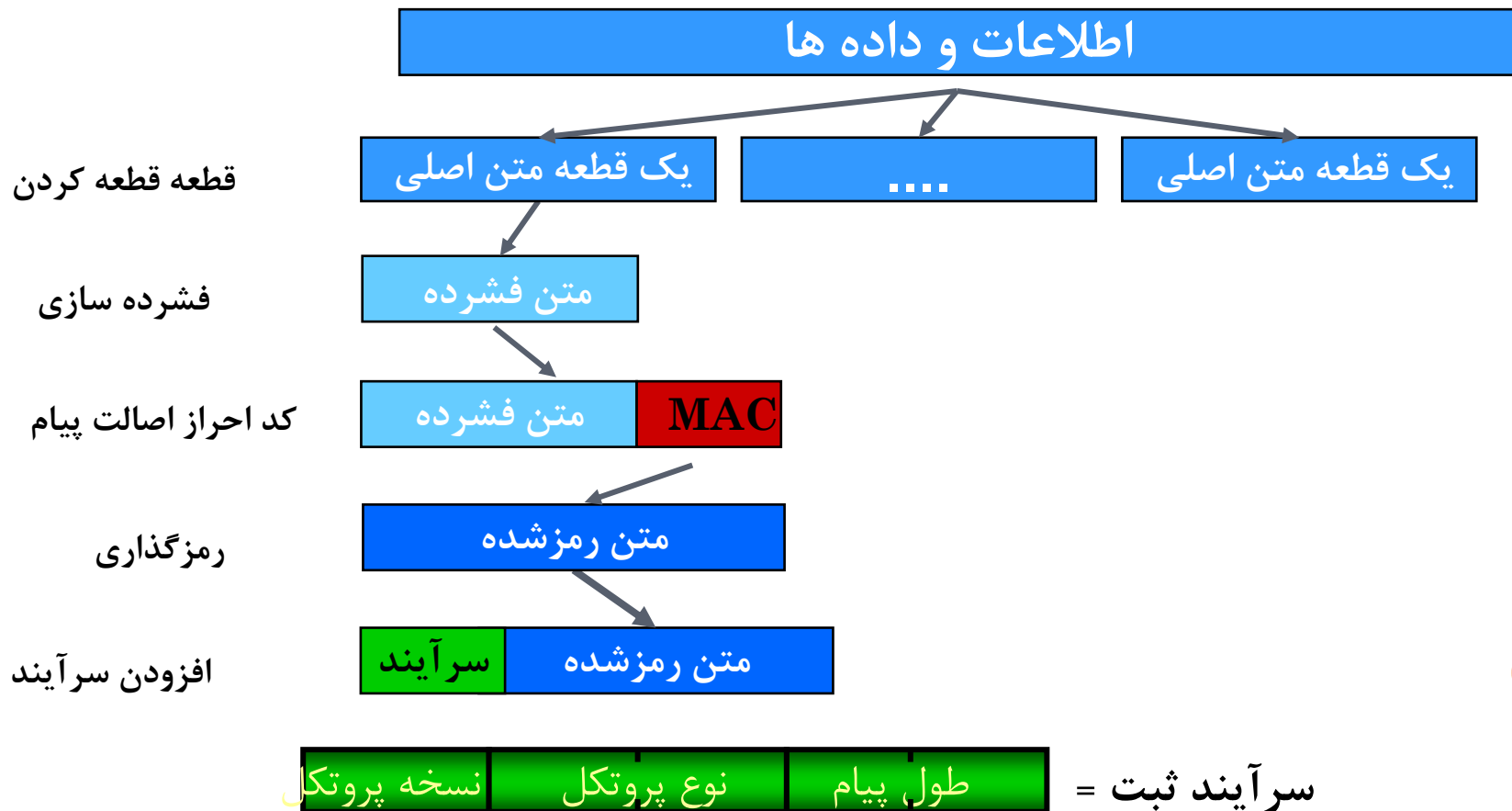
روال های پردازش و ارسال داده ها در SSL

1. Fragmentation : قطعه قطعه کردن داده های دریافتی
2. Compression : فشرده سازی قطعات
3. Message Authentication : اضافه شدن کد MAC برای اطمینان از دست نخوردگی داده ها
4. Encryption : شروع رمزنگاری با کلید توافق شده و سپس پیاده سازی یکی از روشهای زنجیره سازی بلوک ها
5. Addition of Header : اضافه کردن هدر به حاصل مرحله قبل که شامل «شماره نسخه پروتکل»، «طول داده فشرده» و «نوع محتوا» است



روال های پردازش و ارسال داده ها در SSL

- اطلاعات از چهار پروتکل لایه بالایی وارد لایه ثبت می شوند تا به شکل مناسب در آمده و به لایه انتقال فرستاده شوند.
- عملیات فشرده سازی، احراز اصالت و رمزگذاری طبق حالت جاری اتصال انجام می شوند.



SSL فرآیند تبادل داده در

انواع پیام های اخطار در SSL

1. عدم وجود گواهینامه
2. نامعتبر بودن گواهینامه
3. عدم پشتیبانی از نوع گواهینامه
4. گزارش ابطال گواهینامه
5. گزارش دریافت گواهینامه تاریخ گذشته
6. گزارش گواهینامه ناشناخته یا نامفهوم

نکته : در SSL این امتیاز اضافی برای کاربر وجود دارد که اگر گواهی توسط SSL تایید نشد اختیار را به مشتری بدهد



امنیت وب



SSL

SSL – تاریخچه

74

❖ SSL 1.0

July, 1994: در شرکت Netscape طراحی شد.

❖ SSL 2.0

Dec, 1994: مرورگر Netscape همراه با SSL 2.0 به بازار عرضه شد.

July, 1995: مایکروسافت نسخه جدیدی از IE را به بازار عرضه کرد که از SSL پشتیبانی می کرد.

❖ SSL 3.0

Nov, 1995: شرکت Netscape توصیف SSL 3.0 را منتشر کرد

May, 1996: IETF مسئولیت پاسخگویی به مشکلات قرارداد SSL را برعهده گرفت.

SSL – تاریخچه (...ادامه)

75

❖ TLS 1.0

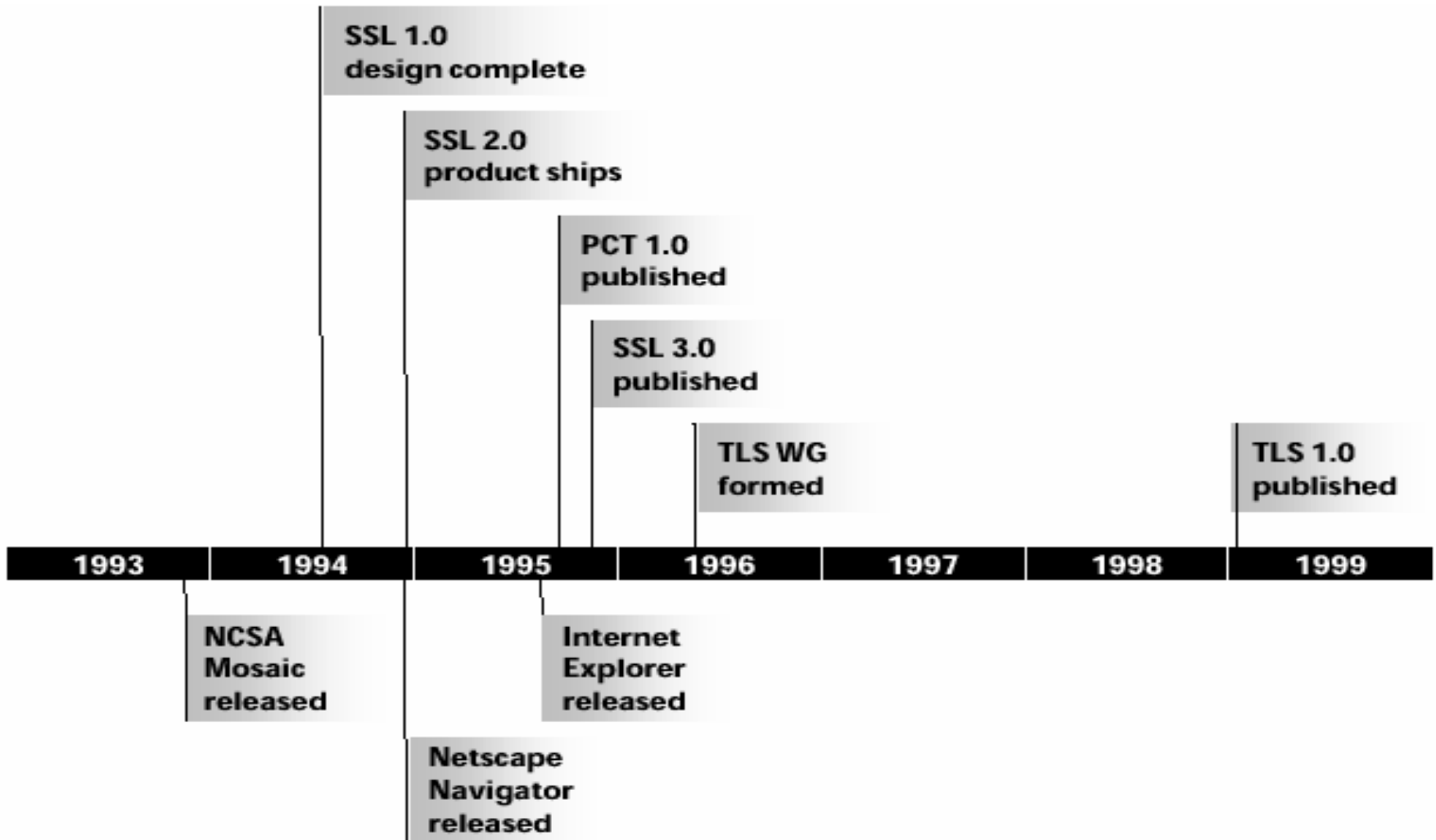
IETF: Apr, 1996 گروه کاری TLS را تشکیل داد.
Jan, 1999: TLS 1.0 بطور رسمی همراه با RFC 2246 به بازار عرضه شد.

❖ TLS1.1

Now: برای رفع ضعفهای TLS1.0 منتشر شده. این نسخه، هنوز استاندارد نشده است.

SSL – تاریخچه (...ادامه)

76



SSL و TLS در دنیای واقعی

77

Wells Fargo Account Summary - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Favorites Print Home

Address https://online.wellsfargo.com/mn1_aa1_on/cgi-bin/session.cgi?sessargs=coAn76ax52xtPX8uoCT8rRBfMMdJldx Go Links Yahoo maps Mapblast Dictionary

Home | Help Center | Contact Us | Locations | Site Map | Apply | **Sign Off**

Account Summary

Last Log On: January 06, 2004

Wells Fargo Accounts **OneLook Accounts**

> Account Summary

- Brokerage
- Bill Pay
- Transfer
- Account Services
- My Message Center

Tip: Select an account's balance to access the Account History.

NEW [Enroll for Online Statements](#) [My Message Center](#)

Cash Accounts

Account	Account Number	Available Balance
Checking Add Bill Pay		
Total		

To end your session, be sure to Sign Off.

Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off
Home | Help Center | Contact Us | Locations | Site Map | Apply

© 1995 - 2003 Wells Fargo. All rights reserved.

Stay organized with FREE 24/7 access to Online Statements. Sign up today.

Sign up for the Wells Fargo Rewards® program and get 2,500 points. [Learn More.](#)


Internet


SSL و TLS در دنیای واقعی

78

Google Gmail: ایمیل از zero and one - سیستم پایگاه داده - Tal

← → ↻ <https://ebanking.bankmellat.ir/ebanking/>

 **ebanking.bankmellat.ir**
The identity of this website has been verified by TÜRKTRUST Elektronik Sunucu Sertifikası Hizmetleri.
[Certificate information](#)


 Your connection to ebanking.bankmellat.ir is encrypted with 256-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.

The connection is not compressed.

The server does not support the TLS renegotiation extension.

 **Site information**
You first visited this site on Sep 14, 2011.
[What do these mean?](#)

English

نمایند :
مدت الکترونیک) هستید ولی تاکنون خدمات ویژه اینترنتی
مشتری و کلمه عبور خود را دریافت نمایید.
نسبت به تغییر کلمه عبور خود اقدام نمایید .

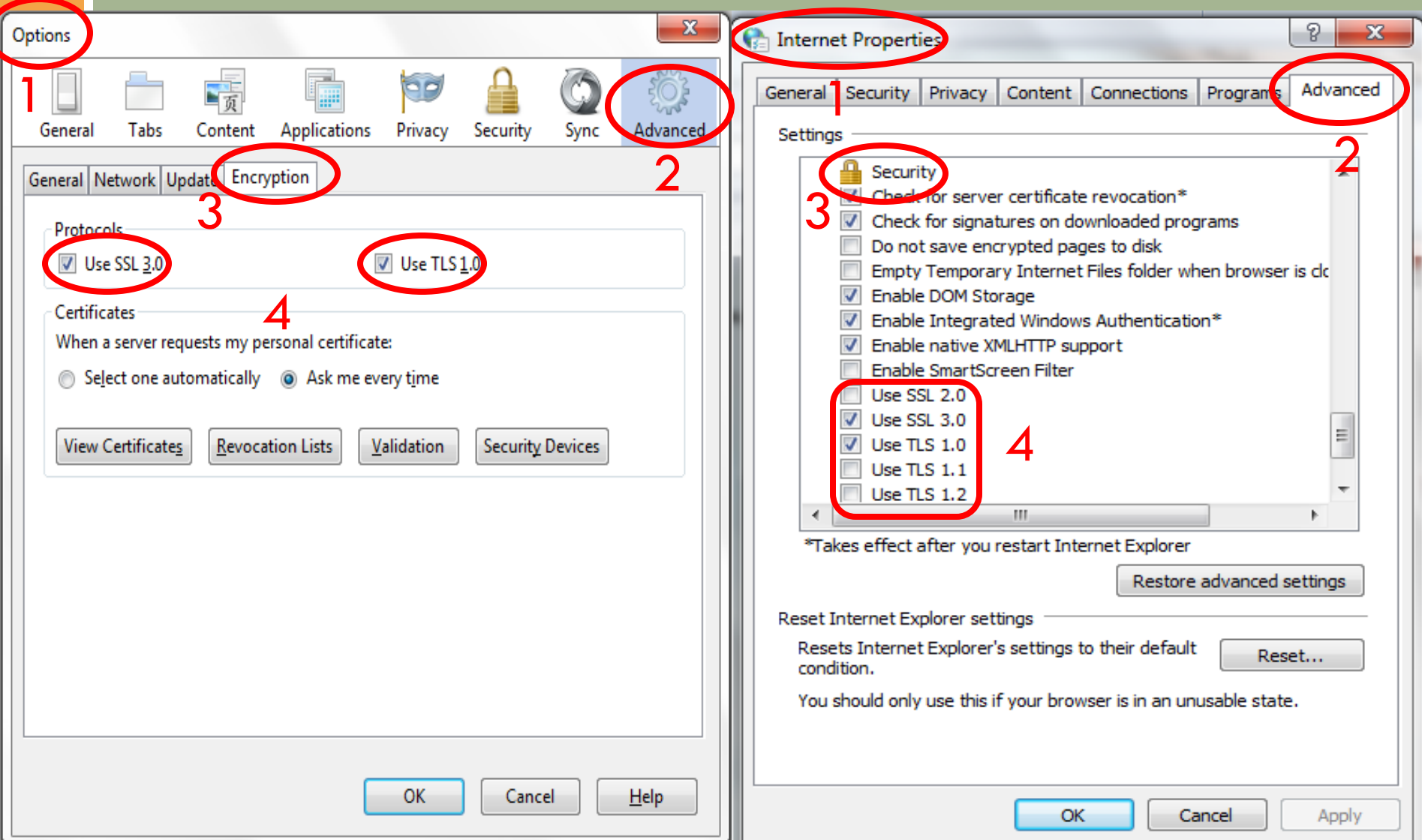
اطلاعات شخصی، جهت وارد کردن کلمه عبور از صفحه کل

اینترنتی بانک ملت

- افتتاح حساب الکترونیک
- پرداخت قبوض
- گزارش قبوض پرداختی

به کارگیری در مرورگر ها

79



Authentication

80

Trapdoor One-way Permutation

که در پیاده سازی امضای دیجیتالی می تواند استفاده شود.

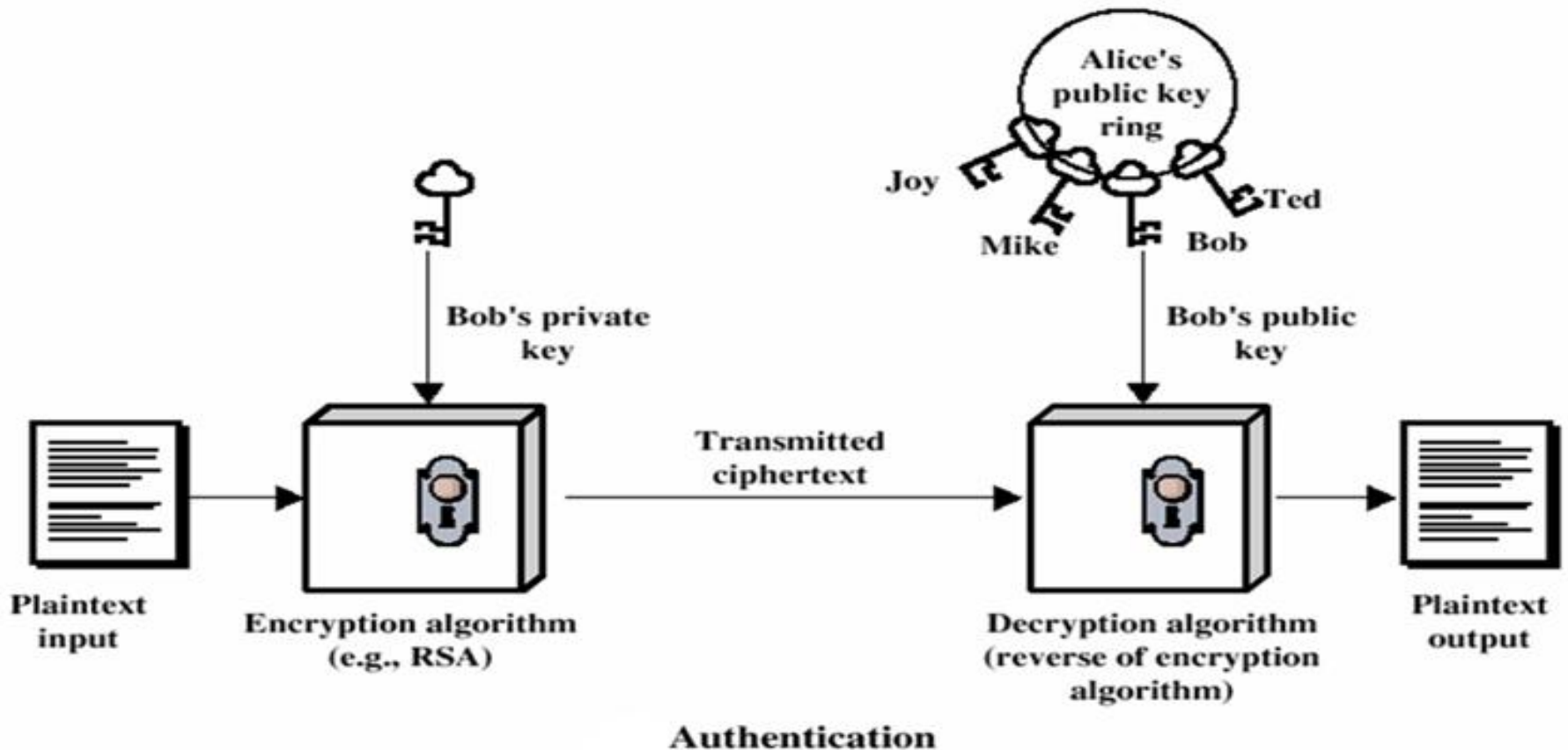
اگر **Alice** پیامی را دریافت کند که نشان از این دارد که **Bob** آن را فرستاده است، **Alice** نیازمند ابزاری برای سنجش اعتبار پیام است.

یک راه این است که **Bob** با استفاده از کلید خصوصی خود پیام را قبل از ارسال رمز کند.

Authentication

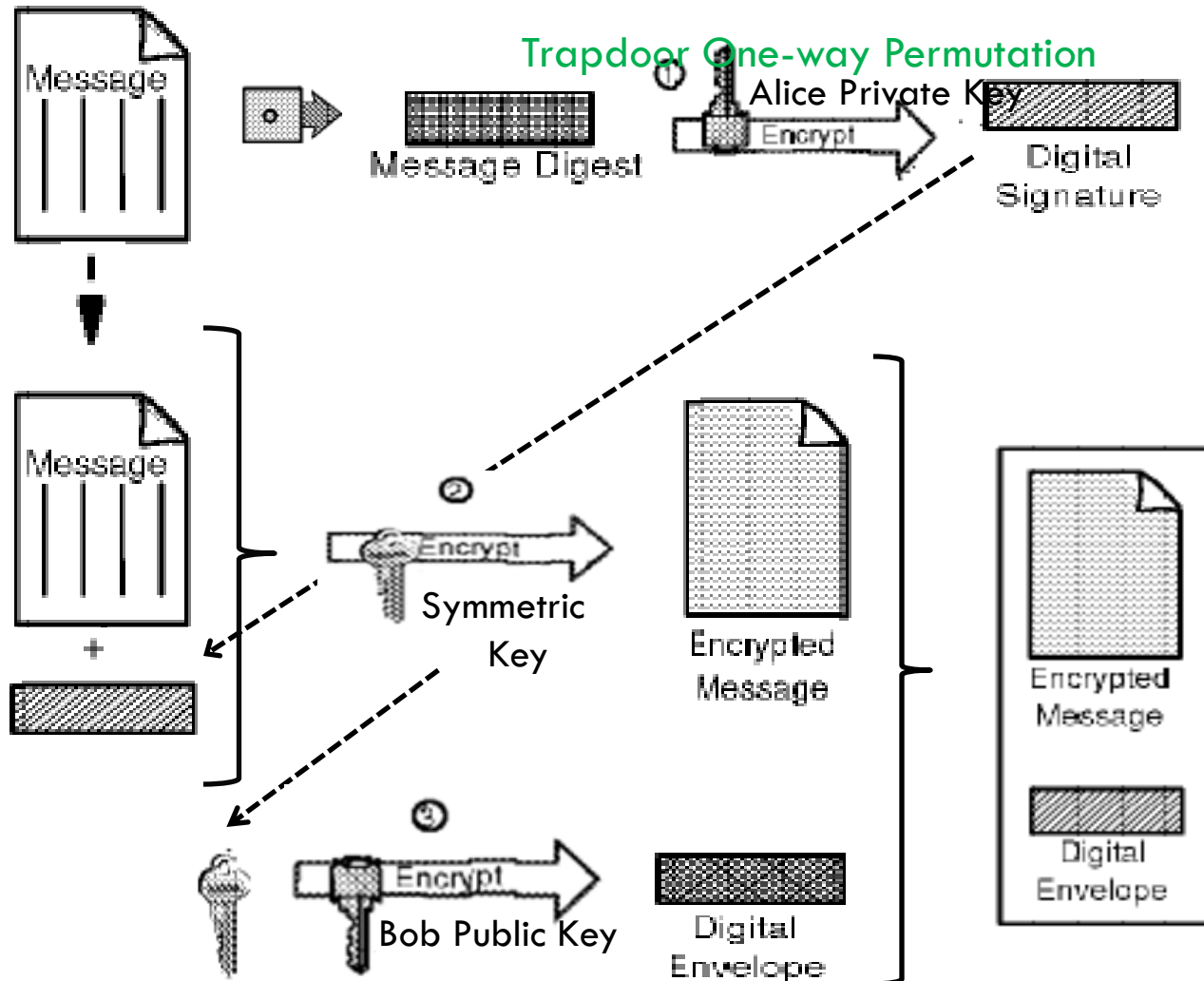
81

Trapdoor One-way Permutation



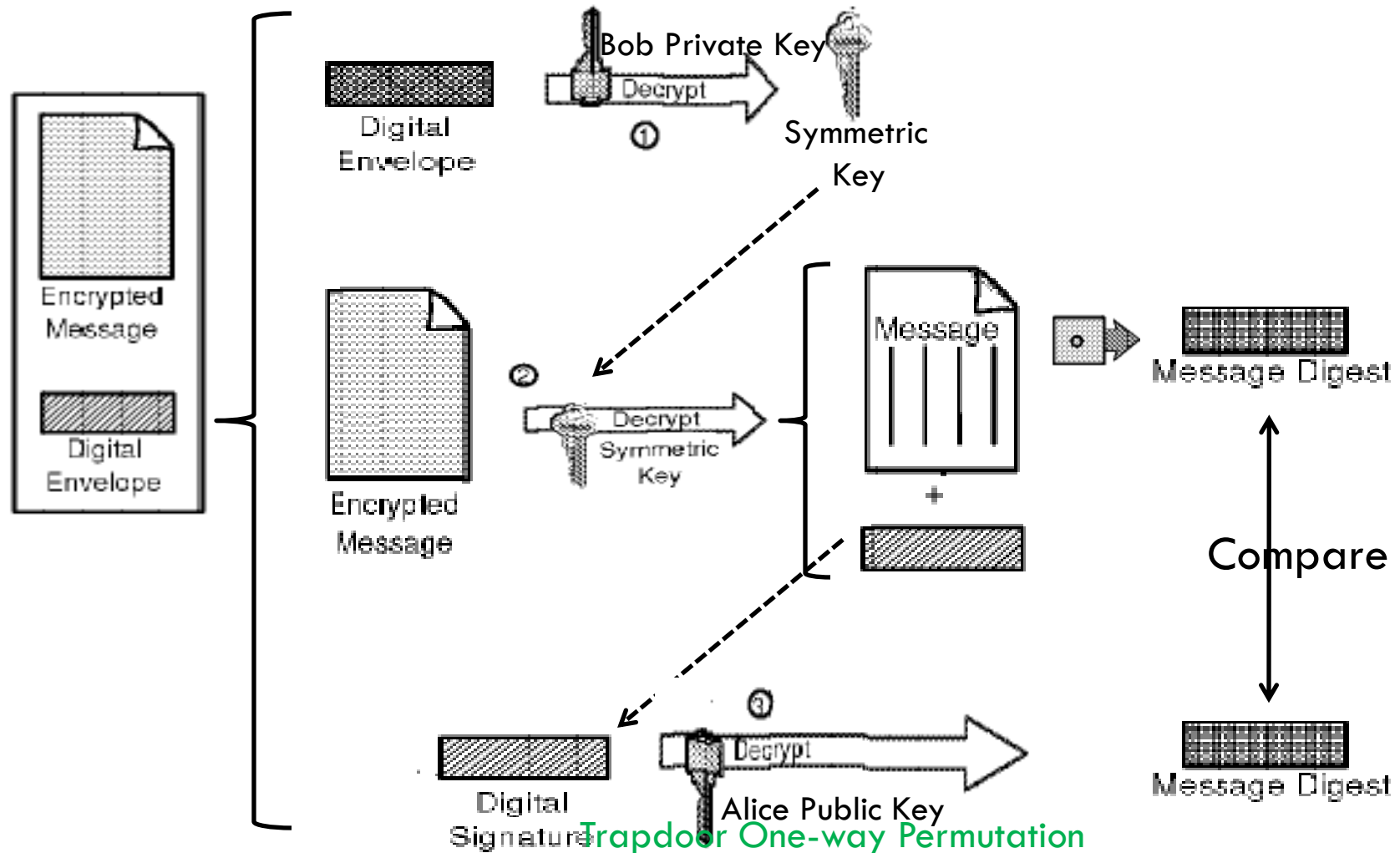
Digital Signature

82



Digital Signature

83



نحوه به دست آوردن کلید عمومی طرف مقابل در SSL

84

کلید عمومی را از چه کسی باید بپرسیم؟

اگر یک حمله کننده بتواند کاربری را متقاعد کند که یک کلید عمومی جعلی به هویتی با ارزش (شخص موثق) مربوط است، در نتیجه مهاجم می تواند خود را به جای **صاحب آن هویت** معرفی کند. سادگی این حمله نشان می دهد که رمزنگاری بر اساس کلید عمومی وقتی کار می کند که کاربران بتوانند از مرتبط بودن یک کلید به یک هویت اطمینان حاصل کنند.

راه حل: لزوم وجود یک Trusted Third Party یا TTP

نحوه به دست آوردن کلید عمومی طرف مقابل در SSL

85

:Certificates

✓ توسط یک Trusted Third Party (TTP) ایجاد می شوند.

✓ پیامی شامل چندین فیلد که مهمترین آنها هویت یک کاربر و کلید عمومی مربوط به اوست.

✓ با کلید خصوصی TTP امضا می شود.

✓ تمامی کاربران سیستم، کلید عمومی TTP را می دانند. (موجود در مرورگرها)

سلسله مراتب CA ها

86

:Certification Authority

✓ به TTP ای که گواهینامه دیجیتالی صادر می کند Certification Authority یا CA گفته می شود.

✓ با زیاد شدن تعداد کاربران یک CA به تنهایی پاسخگو نخواهد بود و در نتیجه سلسله مراتبی از CA ها وجود دارد.

✓ CA ریشه برای CA های دیگر گواهینامه صادر می کند.

✓ کاربران سیستم فقط کلید عمومی CA ریشه (اولین CA) را نگهداری می کنند. (در مرورگر خود)

نحوه به دست آوردن کلید عمومی طرف مقابل در SSL

87

- در لیست گواهینامه های مرورگر شما این شرکتهای صادر کننده Certificate وجود دارند. در واقع اگر شرکت اعطاکننده ناشناخته باشد مرورگر شما اخطار می دهد و کاربر متوجه یک مشکل در روند کار می شود.



سلسله مراتب CA ها

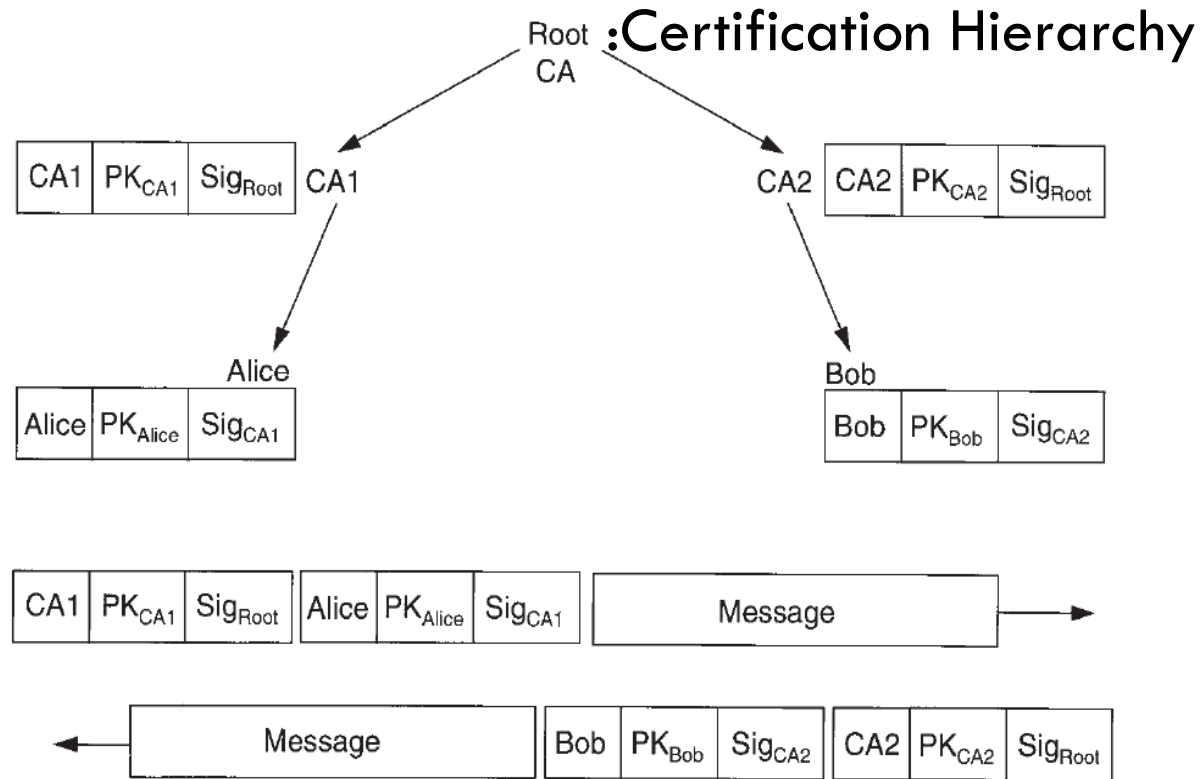
88

• Alice توسط CA1 تایید شده است.

• Bob توسط CA2 تایید شده اند.

• CA1 و CA2 توسط CA تایید شده اند.

• همه کاربران سیستم کلید عمومی CA را می دانند.

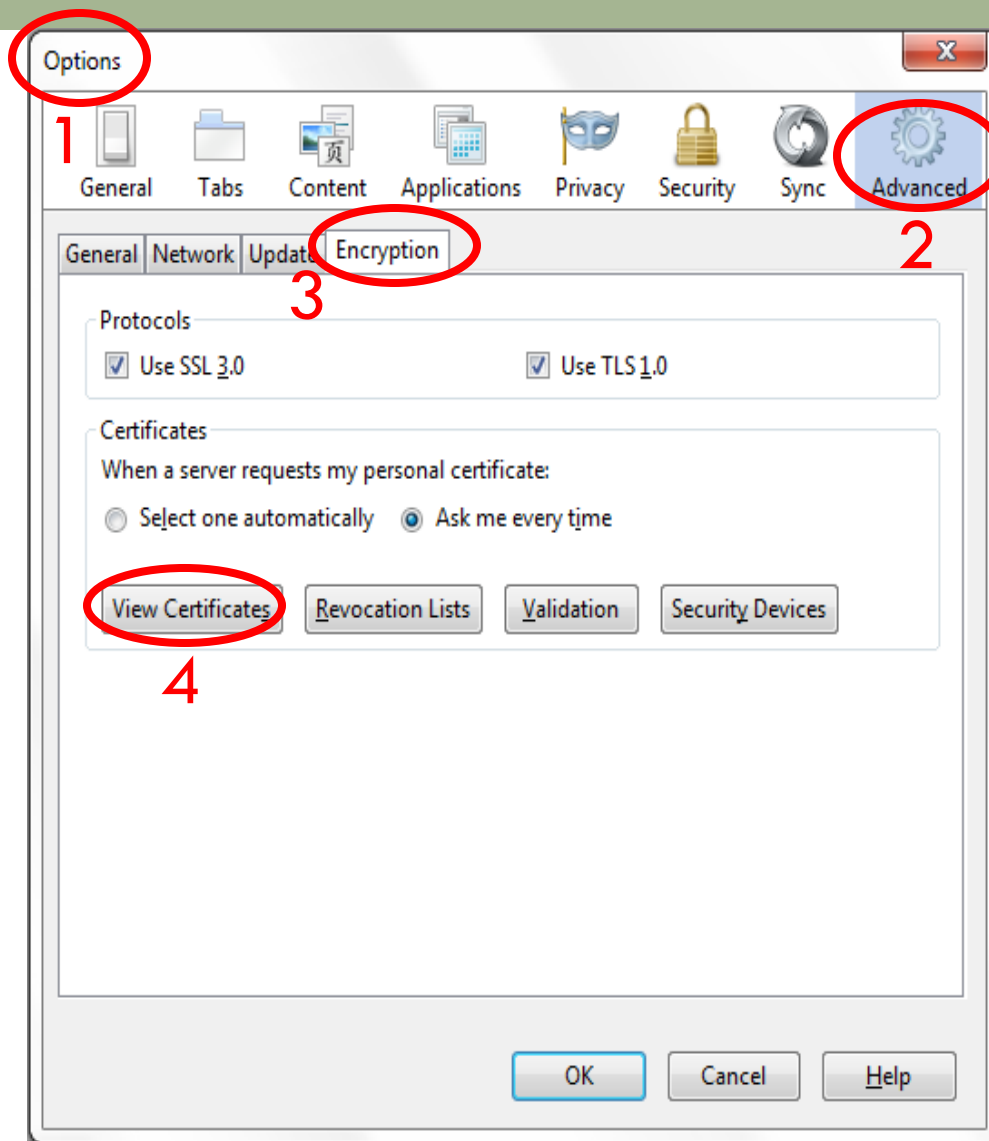


• Alice در هنگام فرستادن پیام گواهینامه خود (تایید توسط CA1) و گواهینامه CA1 (تایید توسط CA) را همراه پیام می فرستد.

• Bob با PK_{Root} : Message Authentication → PK_{Alice} → PK_{CA1} → PK_{Root}

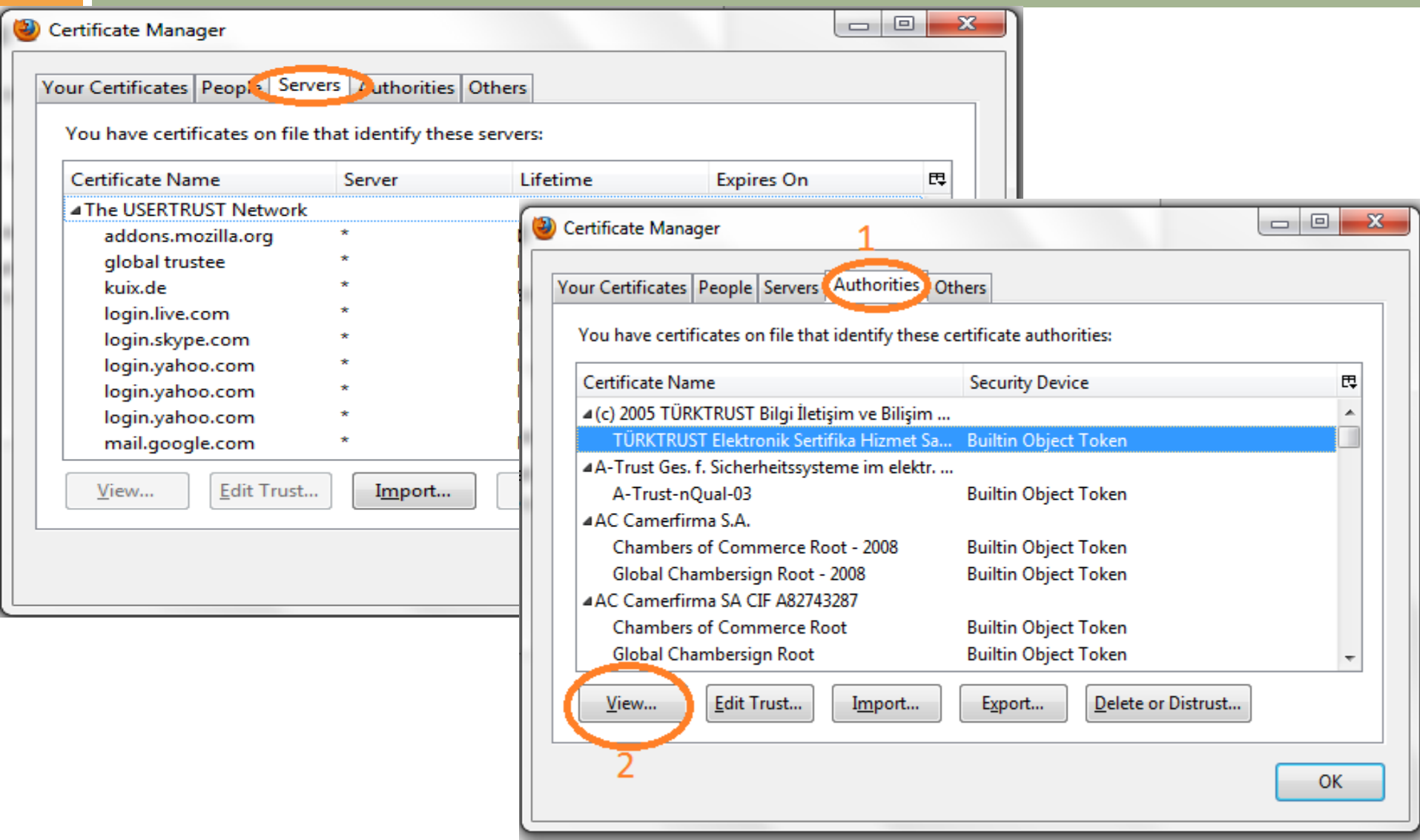
نمونه ای از Certificate ها

89



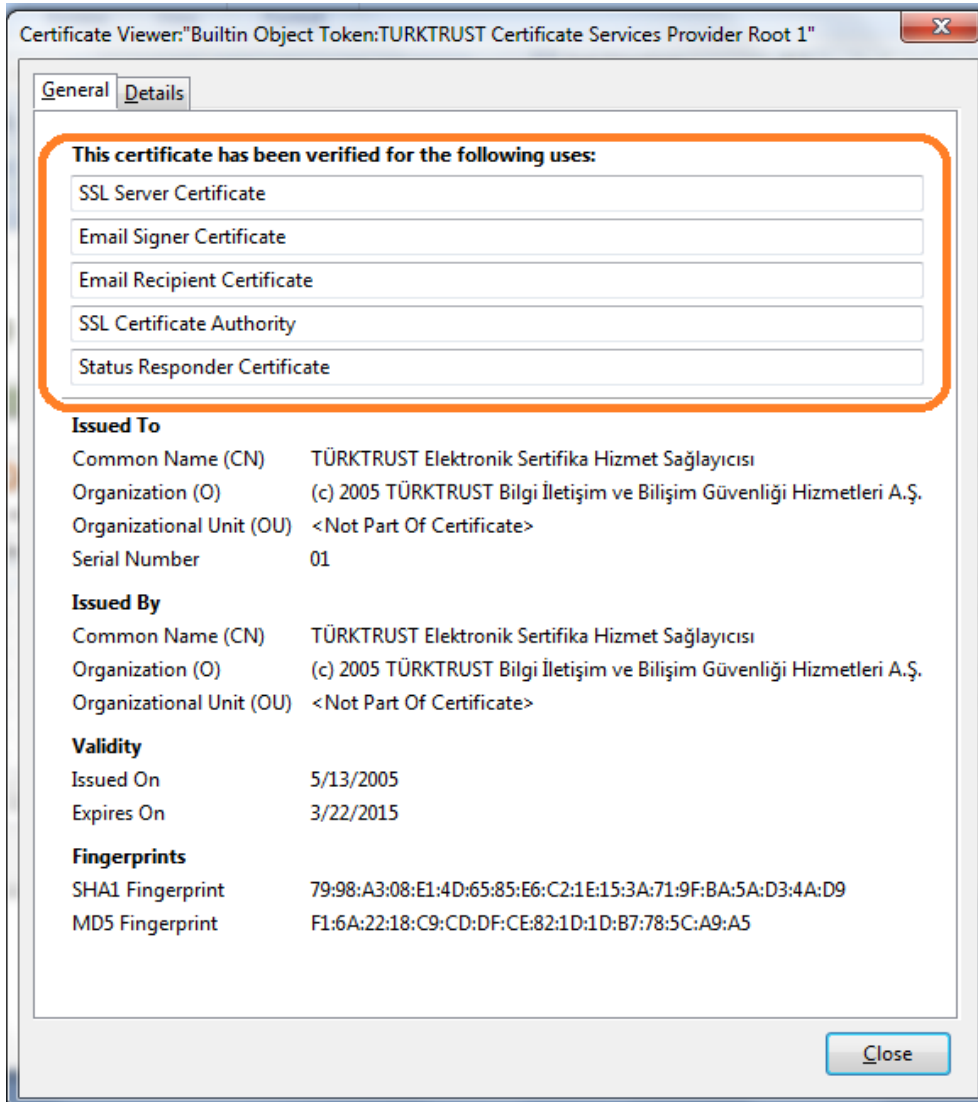
نمونه ای از Certificate ها

90



نمونه ای از Certificate ها

91



نمونه ای از Certificate ها

92



SSL خدمات زیر را ارائه میدهد :

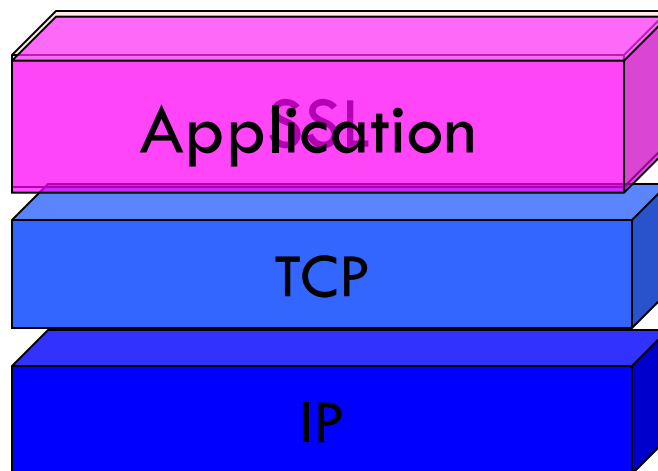
93

- ✓ مذاکره مقدماتی و توافق پارامترها و الگوریتم های امنیتی بین سرویس دهنده و مشتری
- ✓ احراز هویت سرویس دهنده و مشتری به صورت کاملاً مجزا و مستقل
- ✓ فشرده سازی داده ها در صورت تمایل
- ✓ تبادل اطلاعات به صورت رمزنگاری شده
- ✓ بررسی صحت و اصالت داده ها
- ✓ سرویس قابل اطمینان انتها به انتها (end to end) و مبتنی بر TCP/IP

SSL Architecture

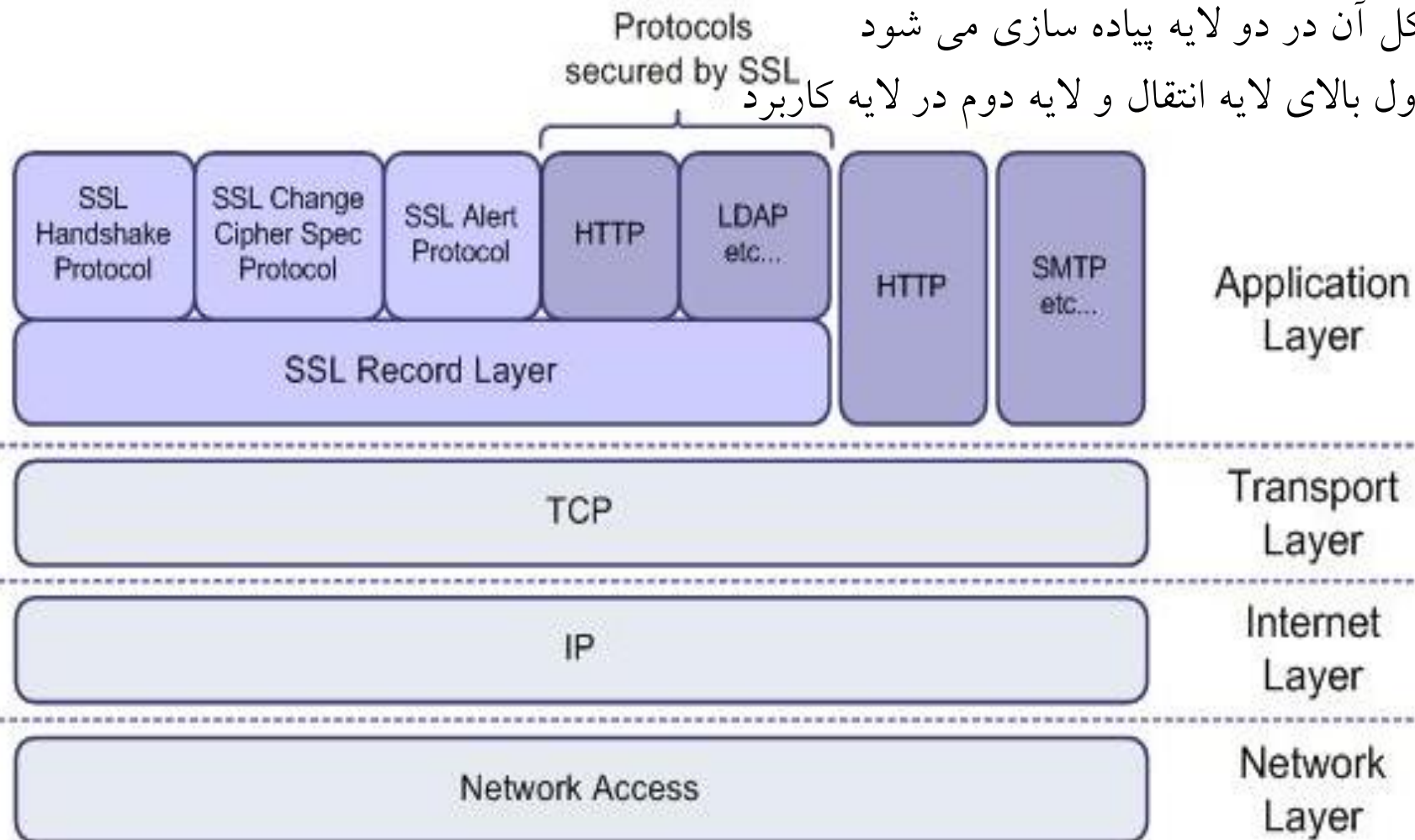
94

✓ SSL و TLS بین لایه TCP و لایه Application قرار می گیرند.



SSL Architecture

95



✓ پروتکل آن در دو لایه پیاده سازی می شود

✓ لایه اول بالای لایه انتقال و لایه دوم در لایه کاربرد

SSL Record Layer

96

□ SSL Record Layer : دو سرویس برای SSL فراهم می کند:

۱- محرمانگی :

- با استفاده از یک کلید متقارن مخفی که در پروتکل Handshake به دست آمده است.

- استفاده از یکی از الگوریتمهای IDEA، RC2-40، DES، DES-40، RC4-128، RC4-40، Fortezza، 3DES

۲- احراز هویت فرستنده :

- استفاده از MAC تولید شده در فاز Handshake

- استفاده از SHA-1 یا MD5

SSL Record Layer

97

اعمال انجام شده در پروتکل Record

۱- قطعه بندی: تولید بلاکهای به طول 2^{14} (16 KB) یا کمتر .

۲- فشرده سازی: اختیاری و بدون از دست رفتن داده.

۳- تولید MAC: مشابه HMAC و روی دو فیلد MAC که در فاز Handshake محاسبه می شود، انجام می گیرد.

۴- رمزنگاری: استفاده از رمز بلوکی یا رشته ای.

۵- اضافه کردن سرآیند: به ابتدای بلاک رمز شده که شامل موارد زیر است:

نوع محتوا ، نسخه اصلی SSL ، نسخه فرعی SSL ، طول داده فشرده شده

نوع محتوا (Content Type) بیان کننده پروتکل استفاده کننده از این سرویس در لایه دوم می باشد

Record Protocol Operation

98

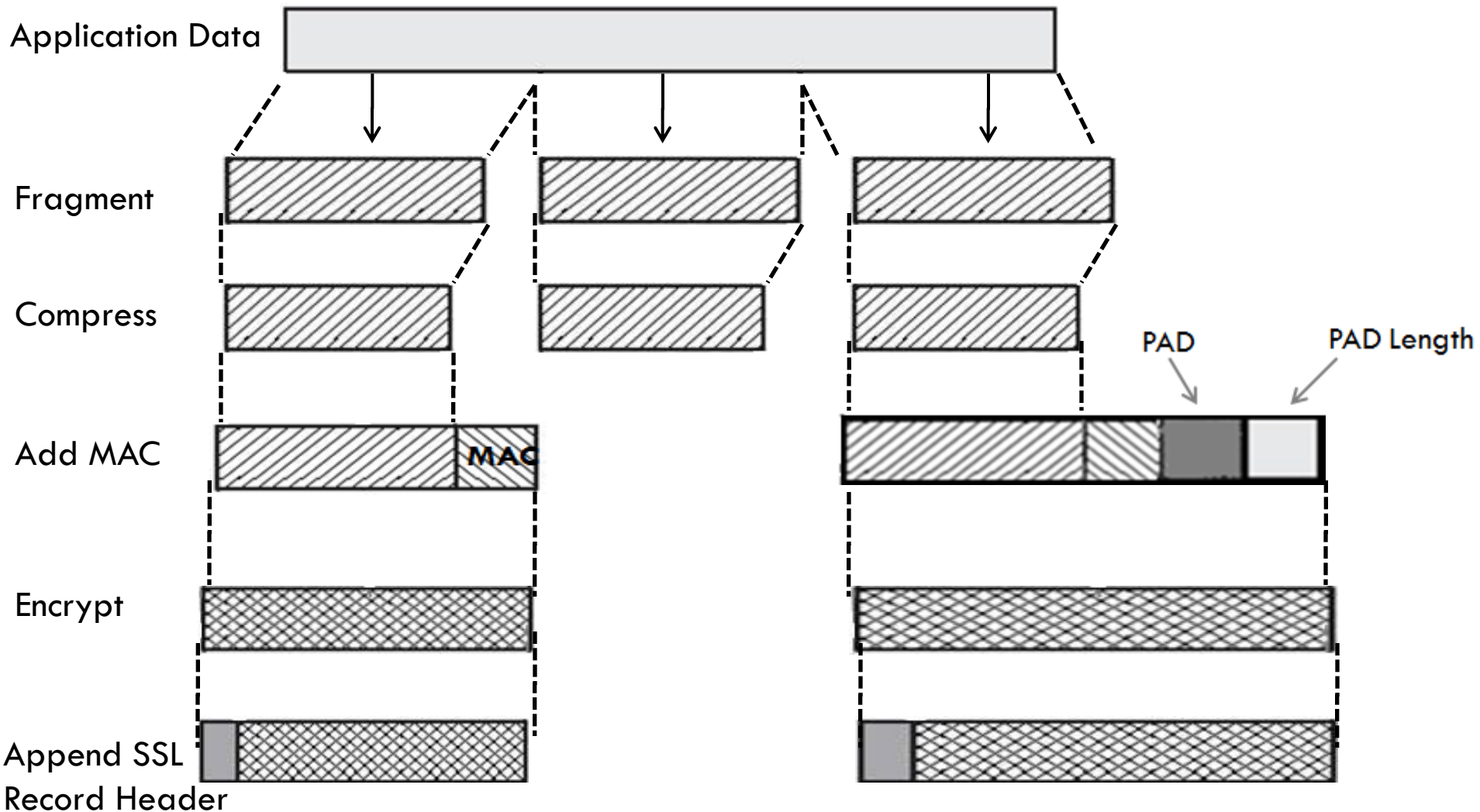
در مبادله داده های لایه Application توسط لایه Record، یکی از دو روش زیر به کار می رود:

۱- **Generic Stream Cipher**: ممکن است که بخواهد یک دنباله رمز شده کلی با MAC ای که به آن الحاق شده بفرستد

۲- **Generic Block Cipher**: که داده ها به صورت بلوک های جدا رمز شده و یک MAC نیز به آن ها الحاق شده است. این روش شامل فیلد دیگری به نام PAD نیز می باشد که برای تغییر طول داده ها به حاصلضربی از طول بلوک های روش رمز نگاری به کار می رود. (PAD فقط در این مد استفاده می شود).

Record Protocol Operation

99



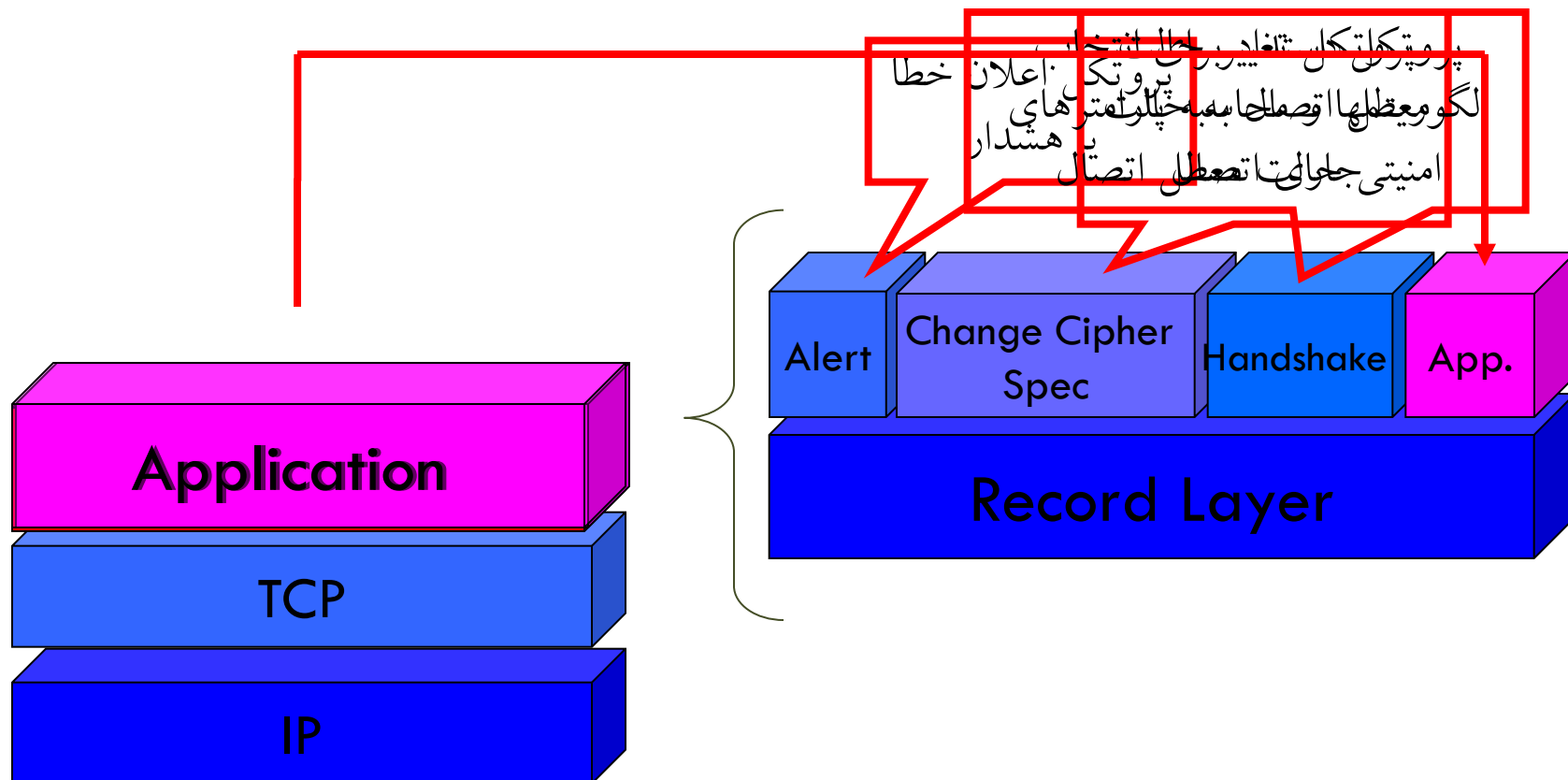
روش های رمزنگاری Record

100

Block Cipher		Stream Cipher	
Algorithm	Key Size	Algorithm	Key Size
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

اجزای SSL

101



پروتکل SSL Handshake:

- ✓ پیش از انتقال هر نوع داده ای تحت SSL، انجام می شود.
- ✓ با استفاده از آن Client و Server برخی کارهای ابتدائی به منظور مذاکره در مورد پارامترهای رمزنگاری نشست SSL و احراز هویت طرفین را انجام می دهند.

1 byte

1

پروتکل Change Cipher Spec:

- ✓ تغییر پارامترهای رمزنگاری در وسط نشست.
- ✓ شامل ۱ بایت می باشد.

اجزای SSL

10
3

1 byte 1 byte

Level	Alert
-------	-------

پروتکل SSL Alert:

- ✓ هر مشکلی که پیش بیاید توسط **Alert** به آن رسیدگی می شود.
- ✓ هشدارها و خطاهای مربوط به **SSL** را به طرف مقابل منتقل می کند.
- ✓ مانند بقیه داده های **SSL** فشرده سازی و رمزنگاری می شود.
- ✓ شامل دو بایت می شود.

نمونه خطاها :

unexpected message, bad record MAC, decompression failure, handshake failure

Handshake

104

✓ ارسال پیام **Client_Hello** توسط کاربر (آغازگر نشست)

Client

Client_Hello

Server • ۲۸ بایت داده تولید شده توسط یک مولد عدد
(تصادفی)

- شماره نشست یکتا (ID)
- لیستی از روش های فشرده سازی و رمزنگاری
که توسط کاربر پشتیبانی می شود.

Client_hello (Version, Client Random ,Session
ID ,Cipher Suite, Compression Method)

Handshake

105

✓ ارسال پیام **Server_Hello** توسط کارگزار

- یک مقدار عددی تصادفی دیگر متفاوت و

مستقل از مقدار **Client_Hello**

- روش های فشرده سازی و رمزنگاری انتخاب شده توسط کارگزار

✓ ارسال پیام **Certificate**

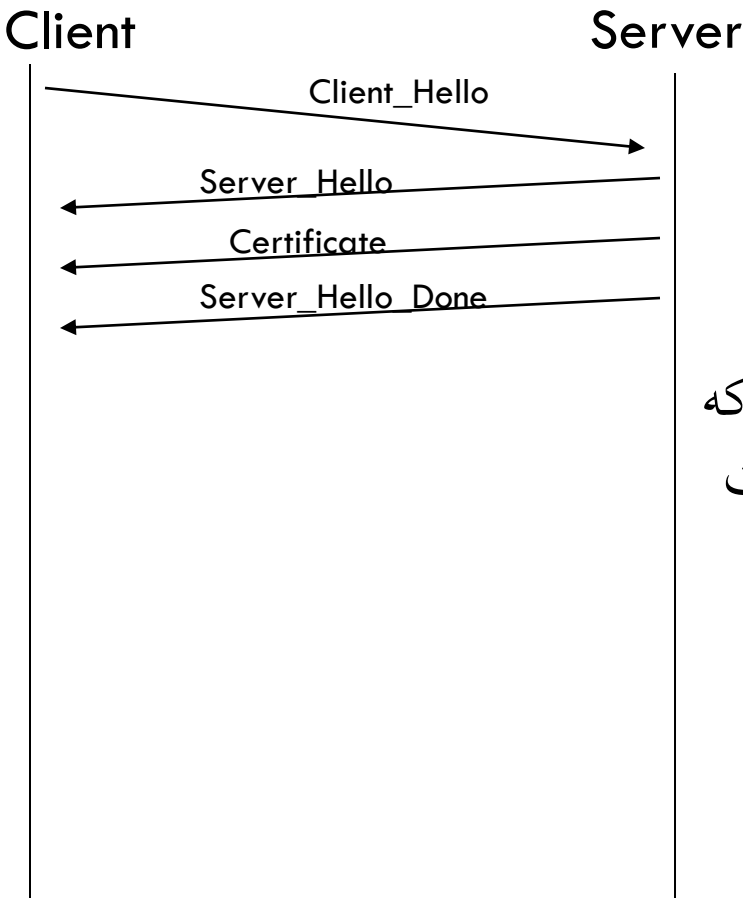
- لیستی از گواهینامه های **X.509 version 3** که

شامل همه گواهینامه ها (خودش تا ریشه) است

که با کمک آن ها اکنون کاربر می تواند کلید

عمومی کارگزار را بدست آورد.

✓ ارسال پیام **Server_Hello_Done**



Handshake

106

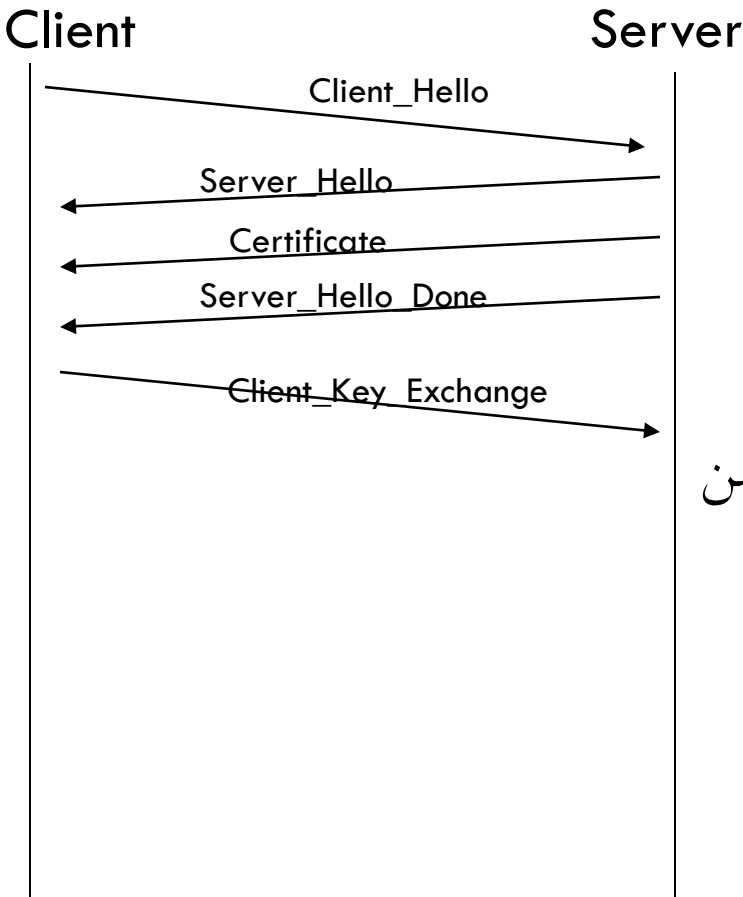
✓ ارسال پیام **Client_Key_Exchange** توسط کاربر

- کمیتی به نام **PreMasterSecret** به طول 48 Bytes محاسبه می شود.

(2 Bytes نسخه پروتکل و 46 Bytes داده تصادفی)

- قبل از ارسال با کلید عمومی سرور رمز می شود.

(**PreMasterSecret** همه اطلاعات لازم برای ایمن کردن نشست SSL را در بر دارد.)

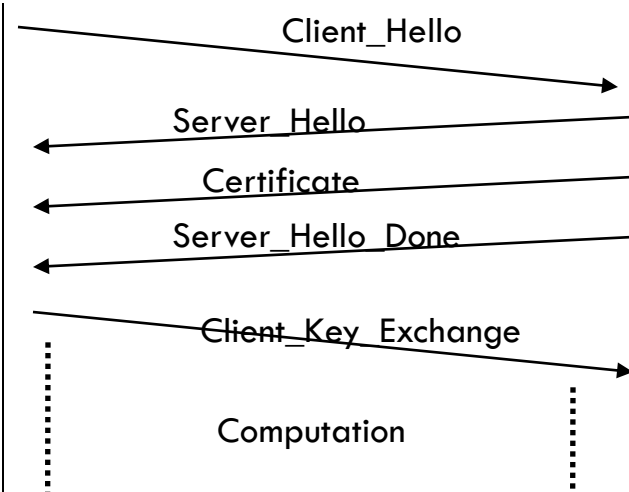


Handshake

107

- پس از ارسال **PreMasterSecret** توسط کاربر هر دو طرف شروع به محاسبه **MasterSecret** از روی آن می نمایند.

Client Server



- از روی **MasterSecret** رشته ای به نام **KeyBlock** در هر دو طرف ساخته شده و در ادامه نشست از مقادیر موجود در آن استفاده می شود.

KeyBlock

Client_Write_MAC_Secret
Server_Write_MAC_Secret
Client_Write_Key
Server_Write_Key
Client_Write_IV
Server_Write_IV

Handshake

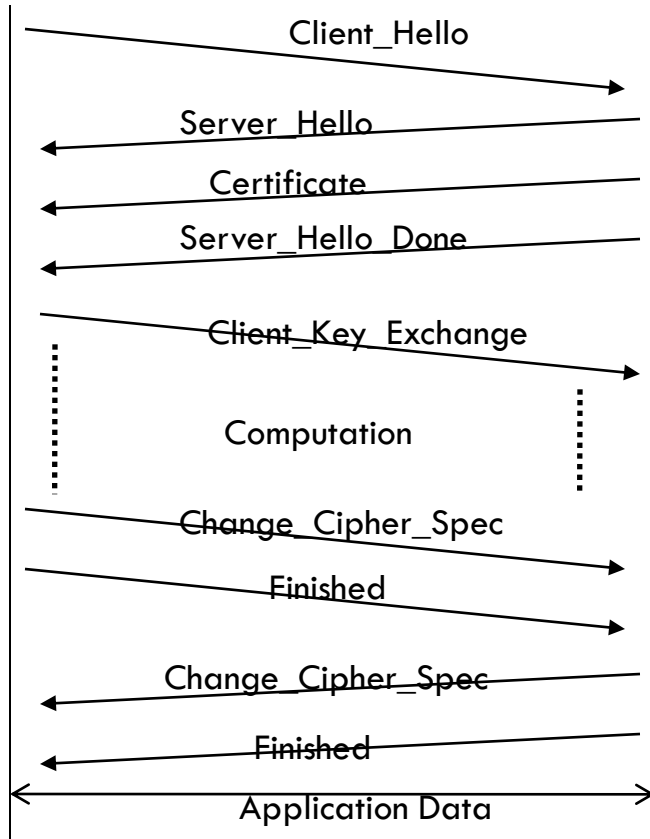
108

✓ ارسال پیام **Change_Cipher_Specification** توسط کاربر

• تغییر مشخصات نشست به مشخصات توافق شده، در ابتدای **Handshake**

Client

Server



✓ ارسال پیام **Finished** توسط کاربر

• پیام پایان با مشخصات جدید ارسال می شود.

✓ جواب های متقابل سرور به پیام های کاربر
و پایان فاز **Handshake** و آغاز نشست **SSL**

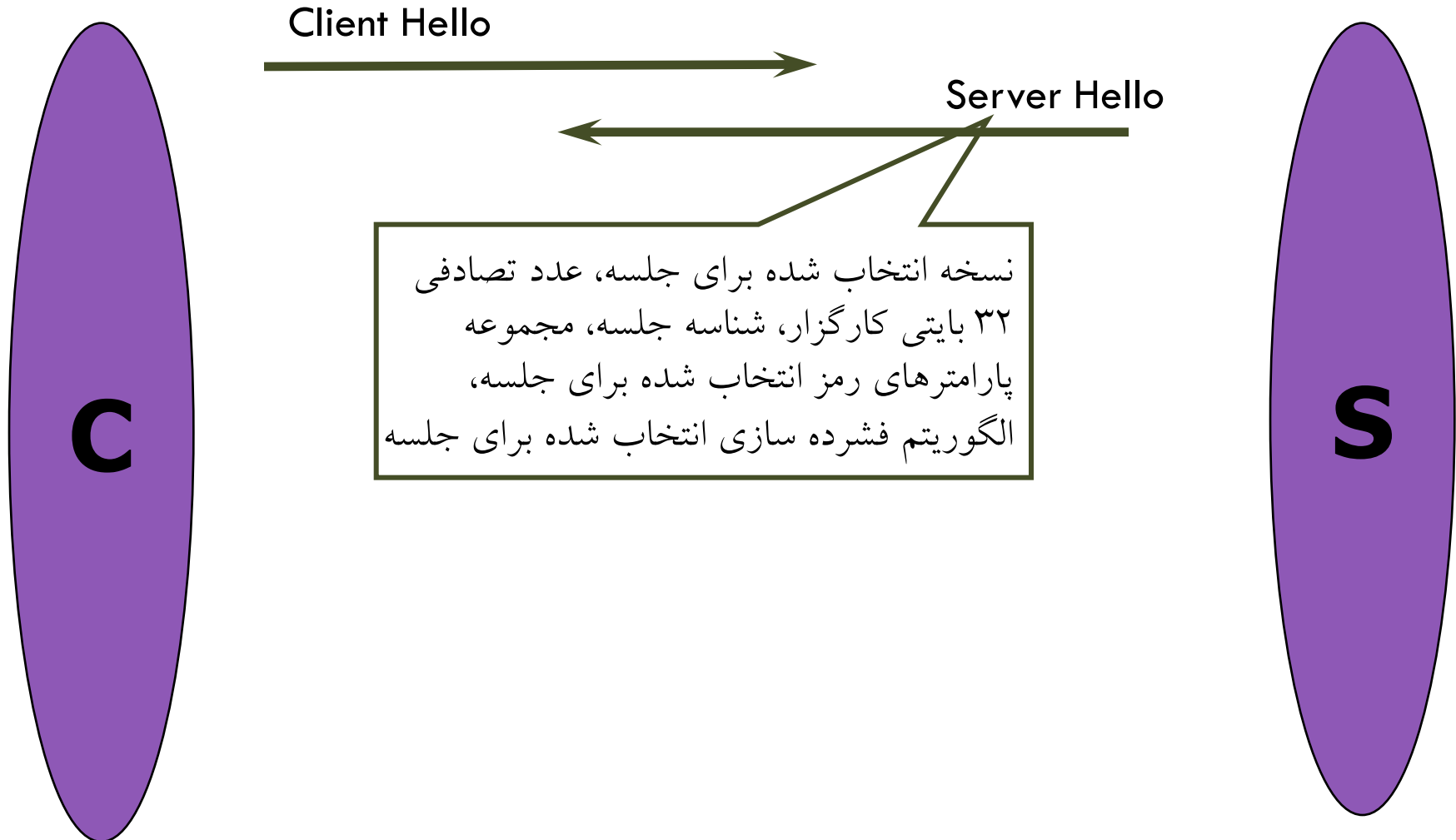
روند تبادل پیامها در یک Hand Shake کامل

109



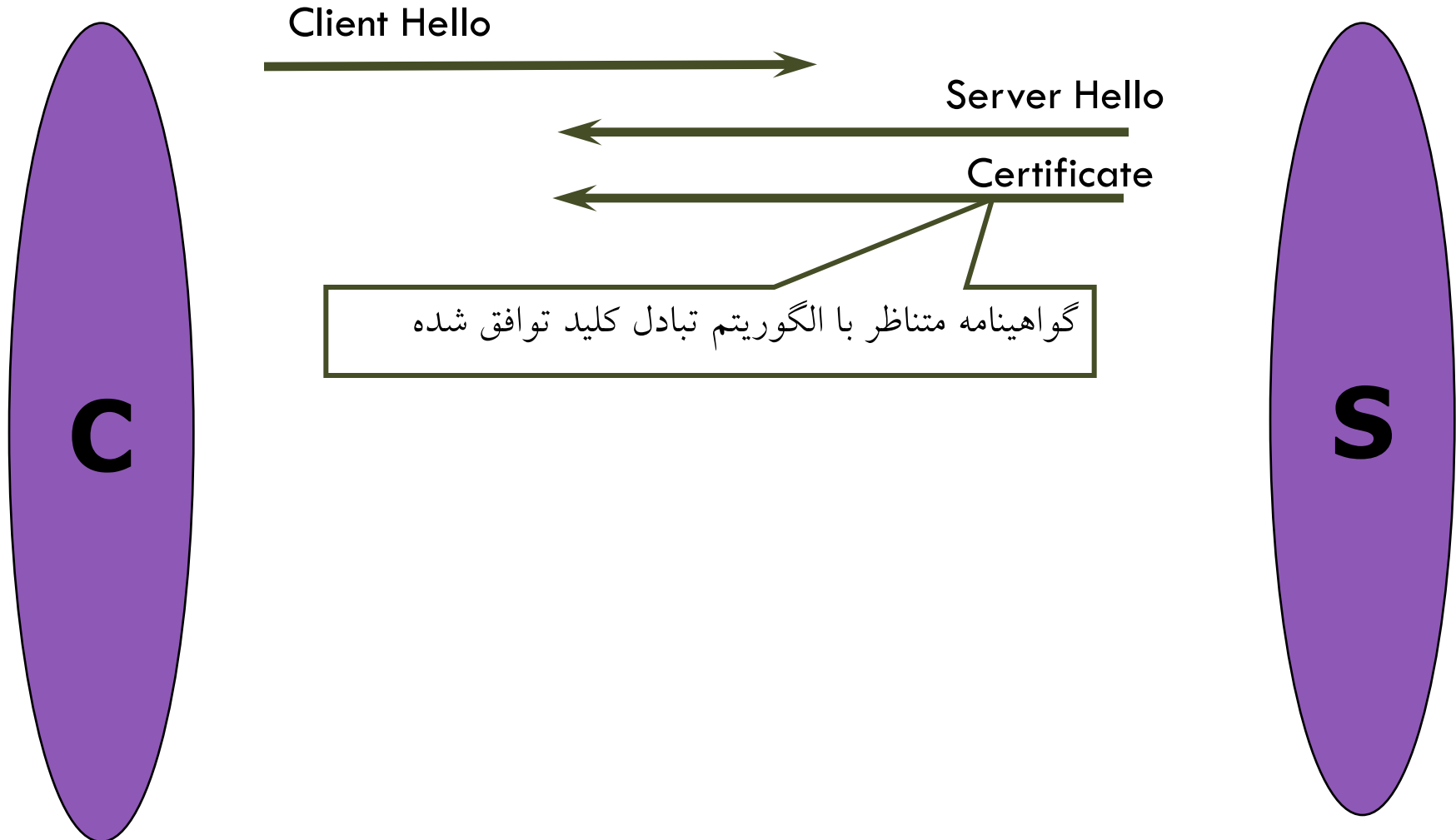
روند تبادل پیامها در یک Hand Shake کامل

110



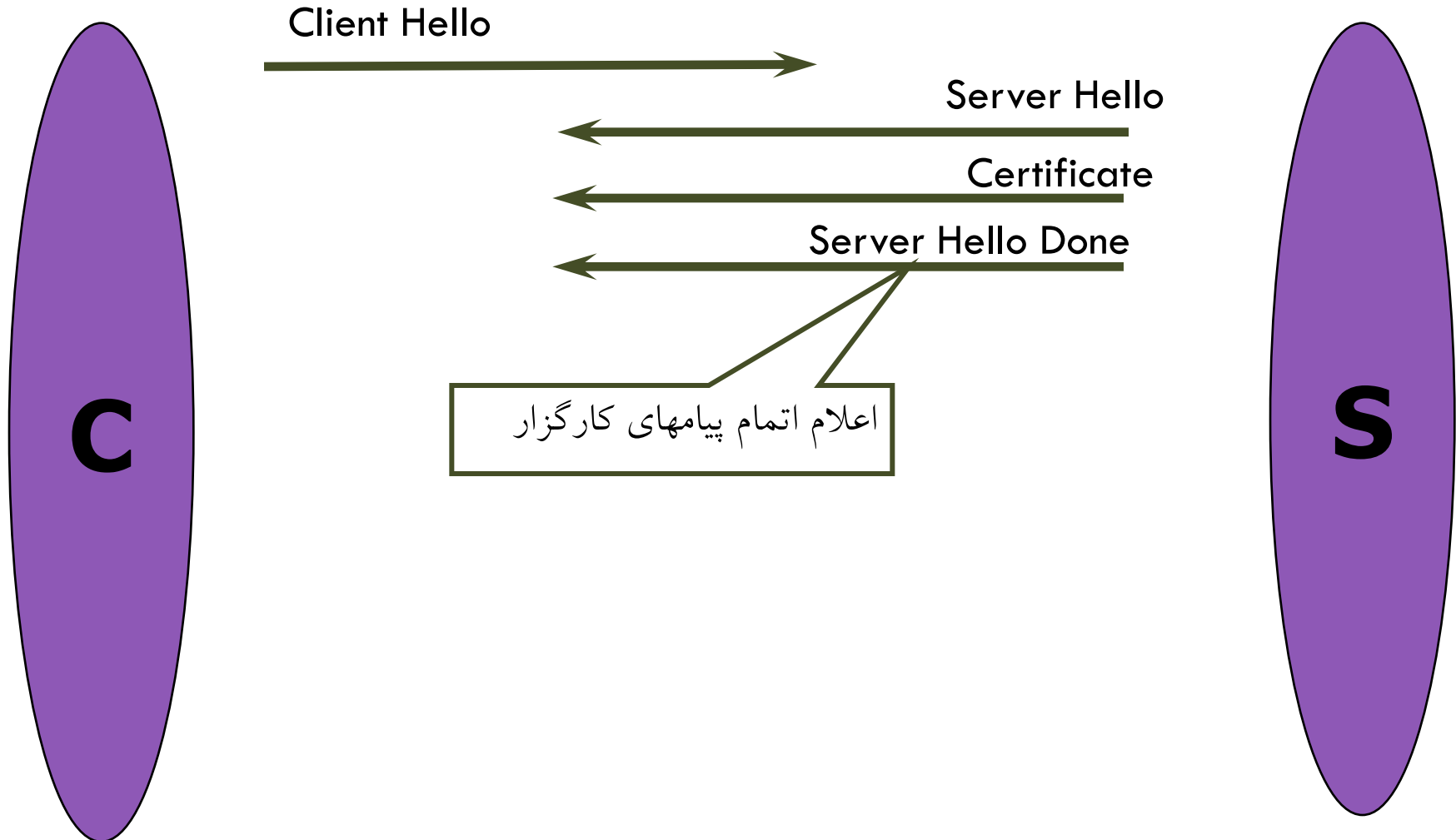
روند تبادل پیامها در یک Hand Shake کامل

111



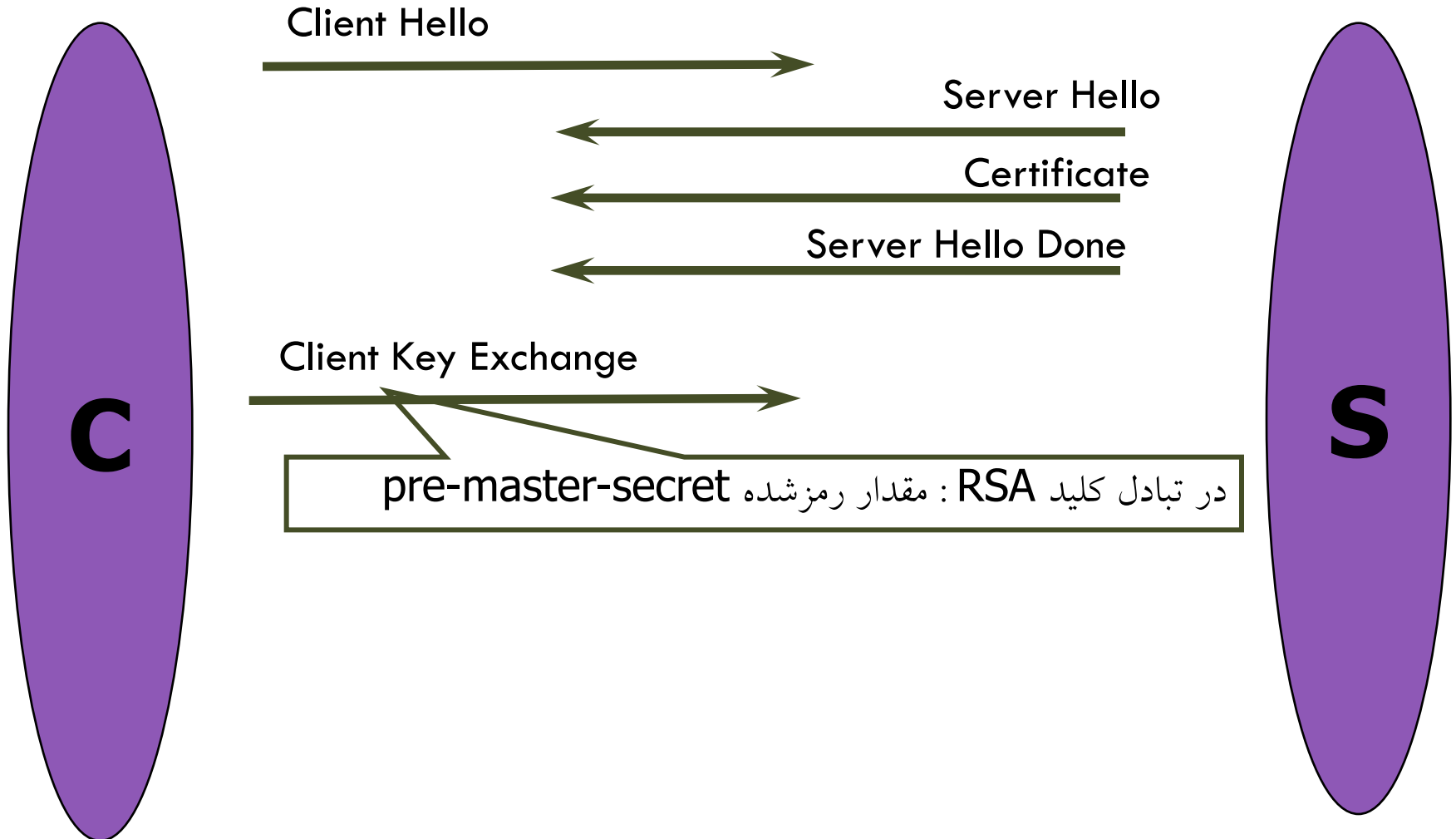
روند تبادل پیامها در یک Hand Shake کامل

112



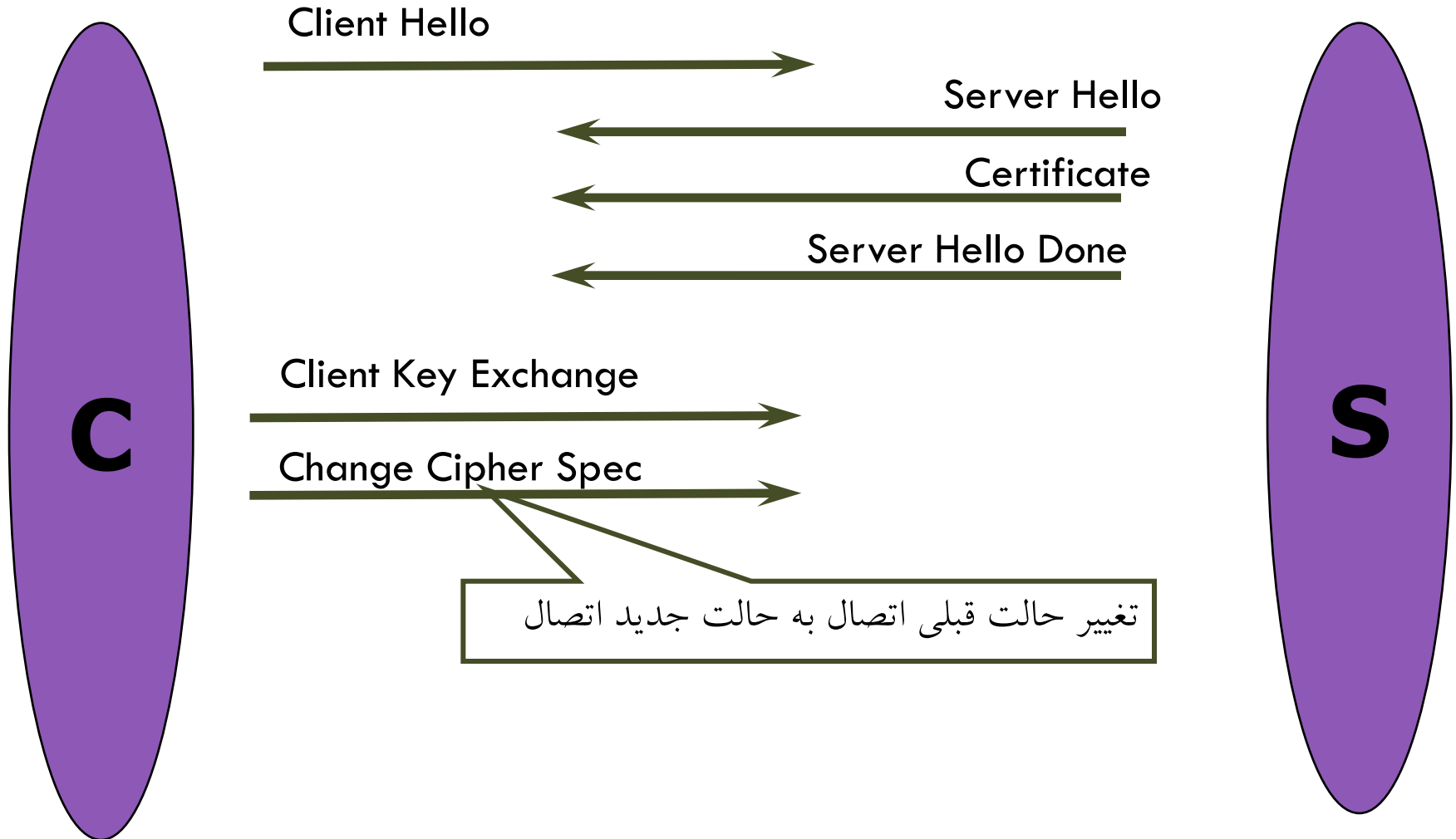
روند تبادل پیامها در یک Hand Shake کامل

113



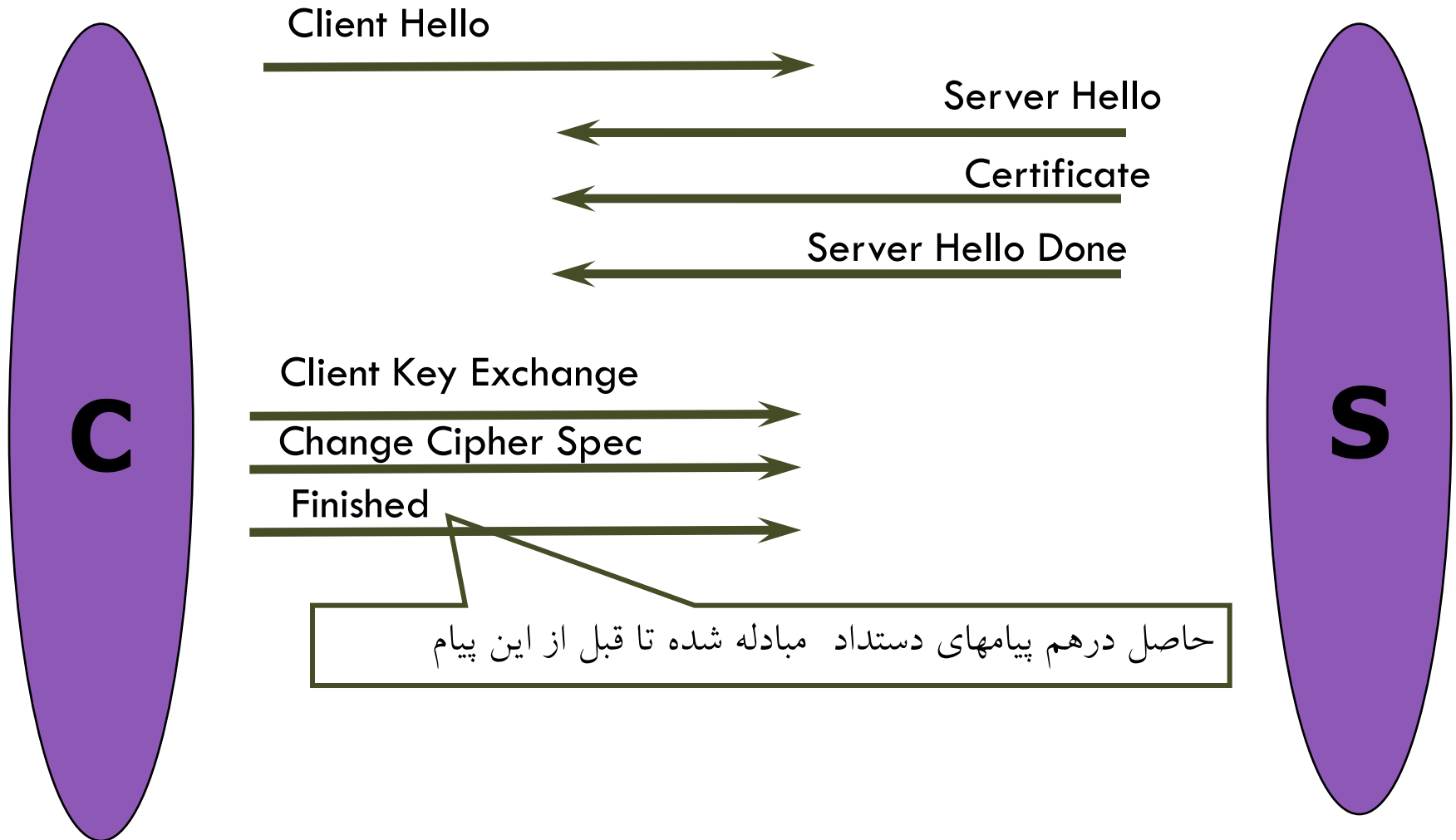
روند تبادل پیامها در یک Hand Shake کامل

114



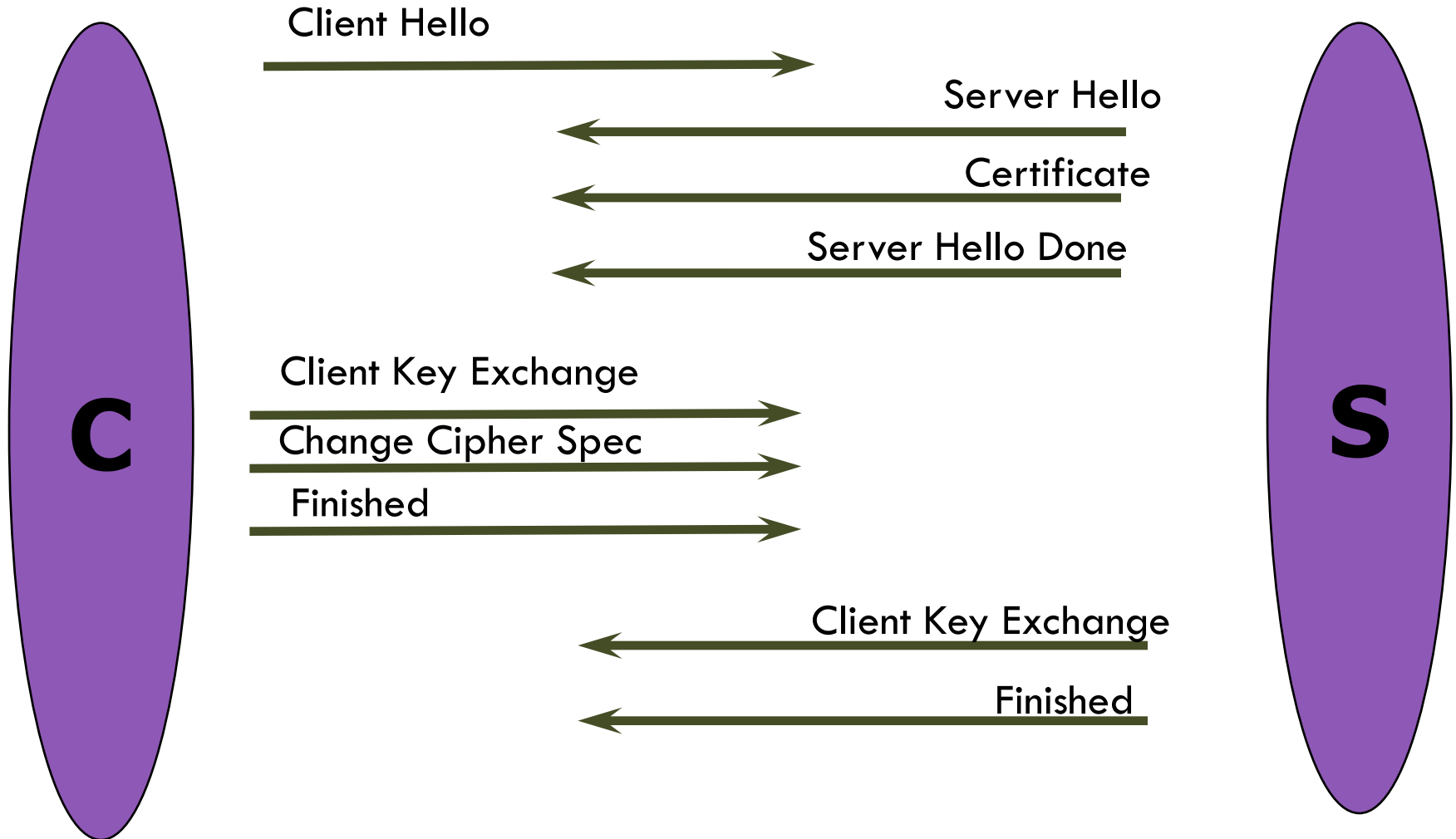
روند تبادل پیامها در یک Hand Shake کامل

115



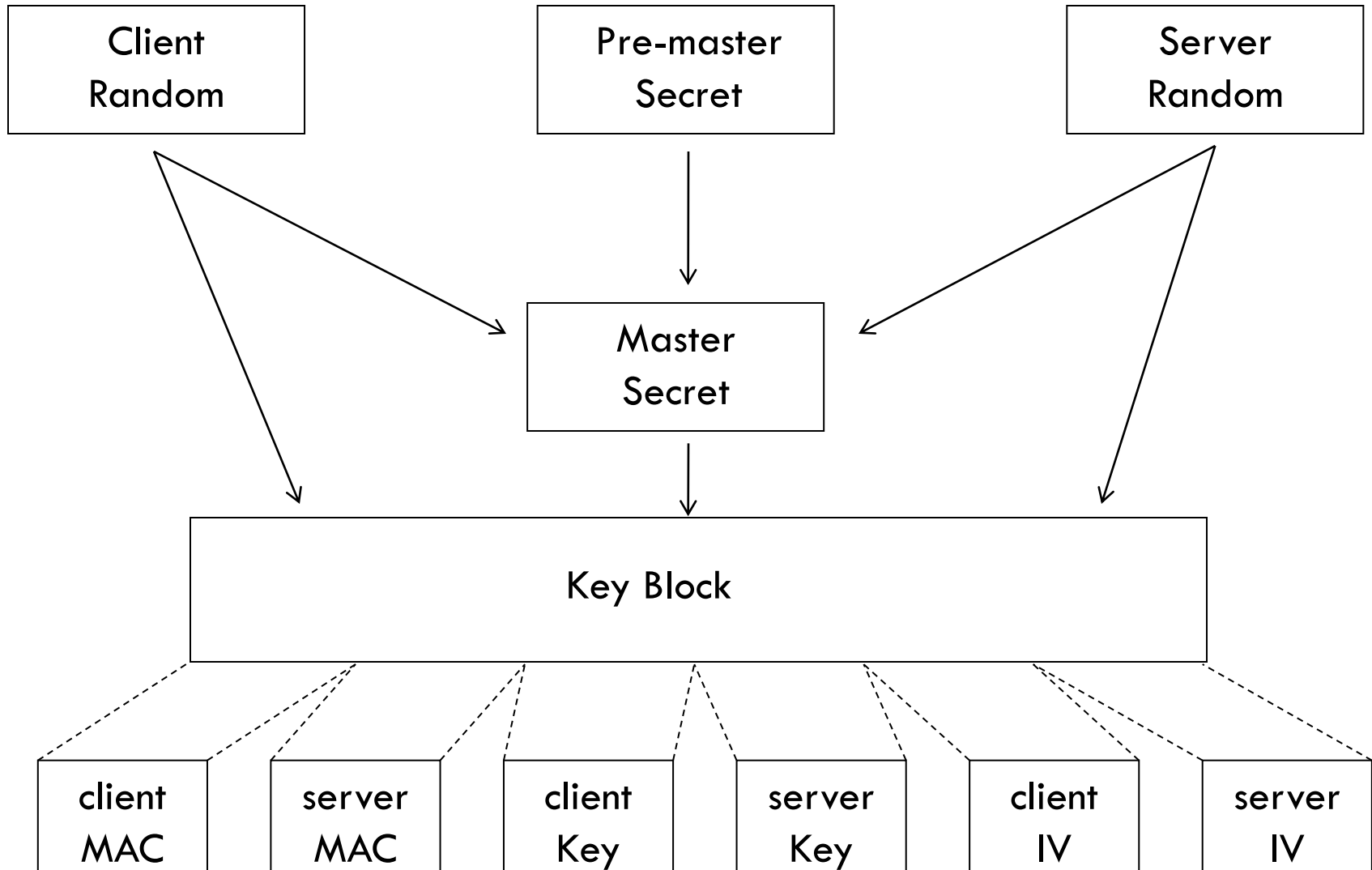
روند تبادل پیامها در یک Hand Shake کامل

116



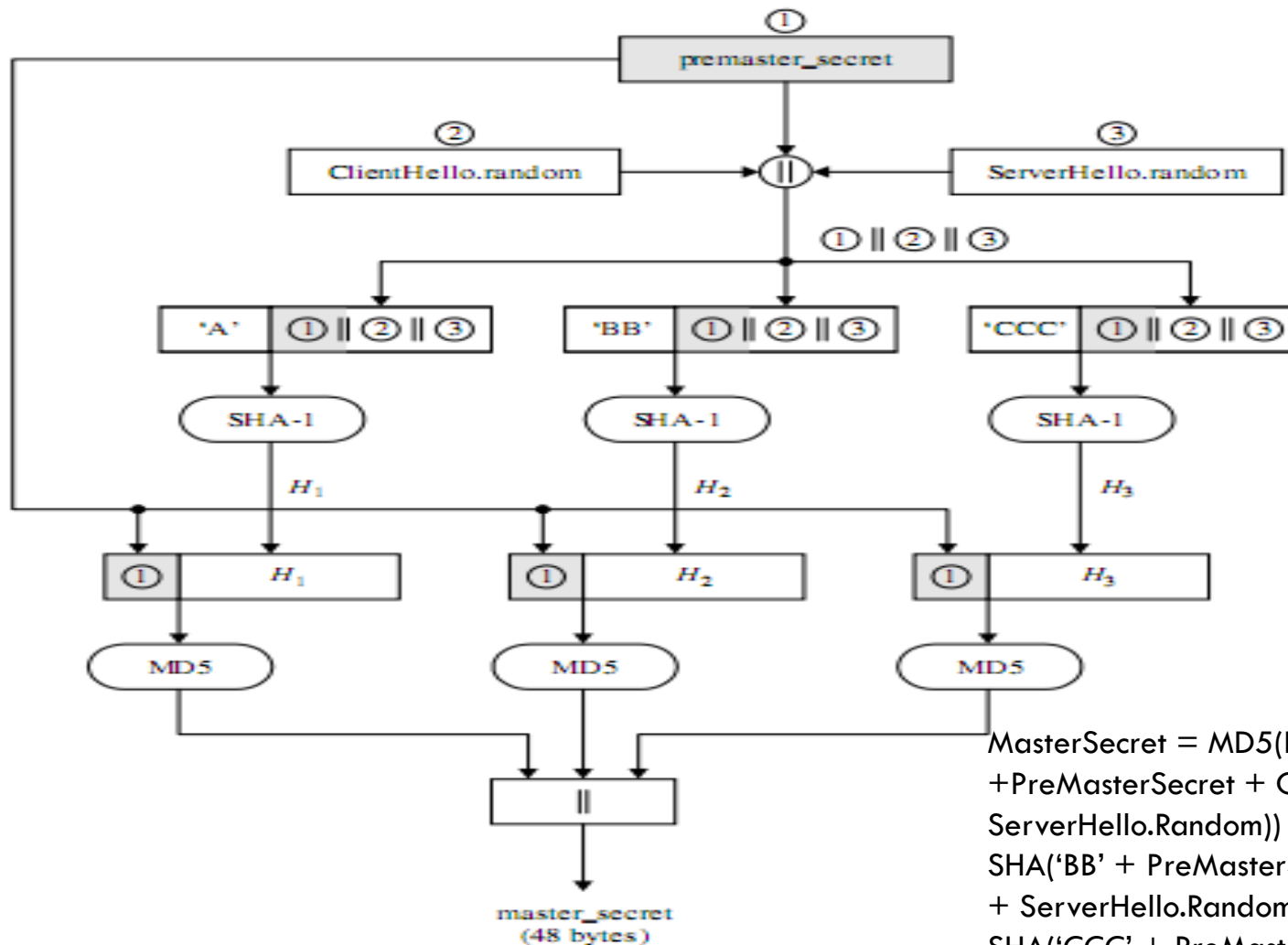
محابسه MasterSecret و KeyBlock

117



محابسه MasterSecret و KeyBlock

118

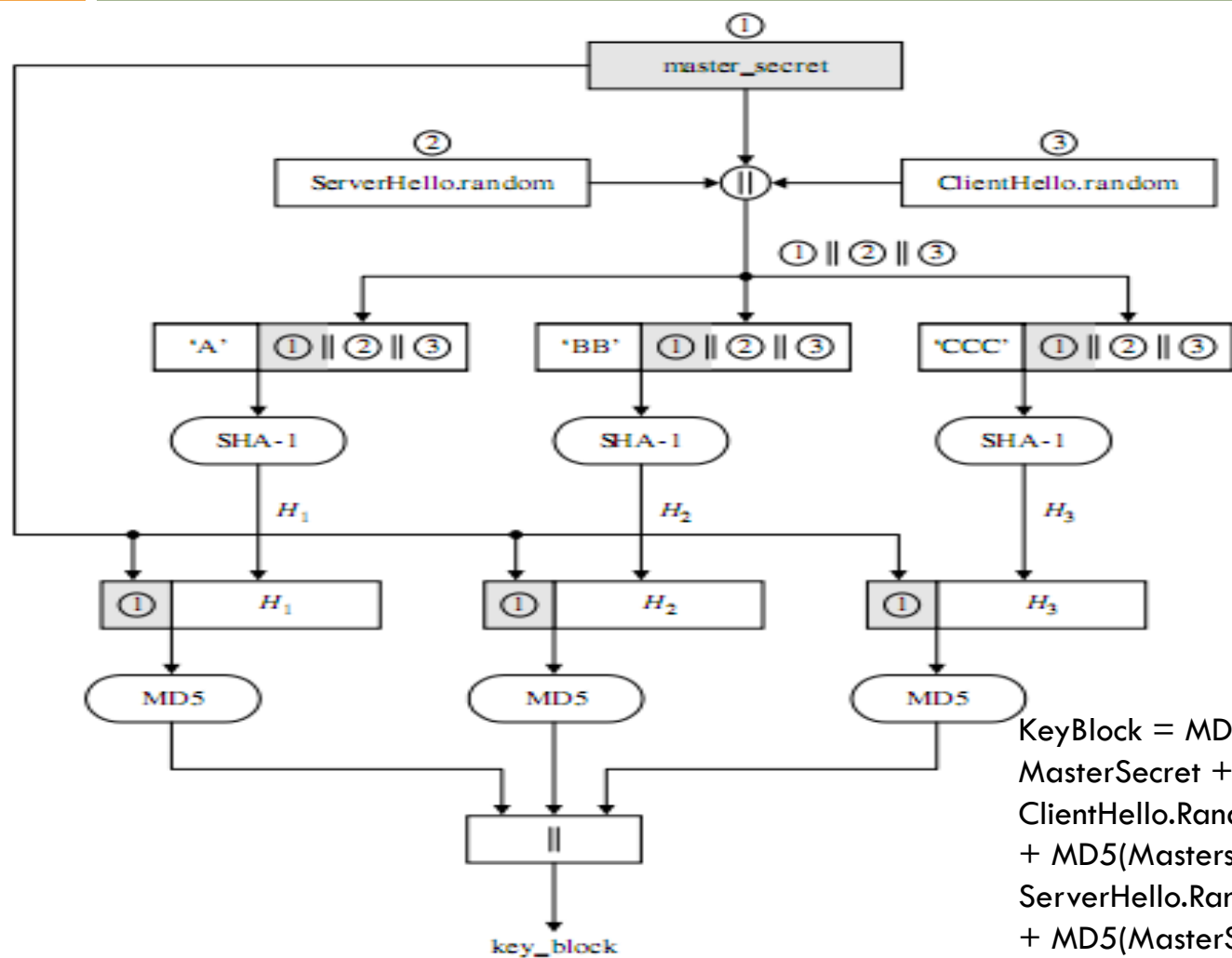


Computation of the master secret.

$$\text{MasterSecret} = \text{MD5}(\text{PreMasterSecret} + \text{SHA}('A' + \text{PreMasterSecret} + \text{ClientHello.Random} + \text{ServerHello.Random})) + \text{MD5}(\text{PreMasterSecret} + \text{SHA}('BB' + \text{PreMasterSecret} + \text{ClientHello.Random} + \text{ServerHello.Random})) + \text{MD5}(\text{PreMasterSecret} + \text{SHA}('CCC' + \text{PreMasterSecret} + \text{ClientHello.Random} + \text{ServerHello.Random}))$$

محابسه MasterSecret و KeyBlock

119



Generation of key block.

$\text{KeyBlock} = \text{MD5}(\text{MasterSecret} + \text{SHA}('A' + \text{MasterSecret} + \text{SecretHello.Random} + \text{ClientHello.Random}))$
 $+ \text{MD5}(\text{MasterSecret} + \text{SHA}('BB' + \text{MasterSecret} + \text{ServerHello.Random} + \text{ClientHello.Random}))$
 $+ \text{MD5}(\text{MasterSecret} + \text{SHA}('CCC' + \text{MasterSecret} + \text{ServerHello.Random} + \text{ClientHello.Random})) + \dots$

- تنزل نسخه (۱۹۹۶ میلادی)
- تنزل الگوریتم تبادل کلید (۱۹۹۶ میلادی)
- از قلم انداختن پیام Change Cipher Spec (۱۹۹۶ میلادی)
- دستیابی به محتوای قالبهای رمز شده با بهره گیری از ضعفهای رمز قالبی



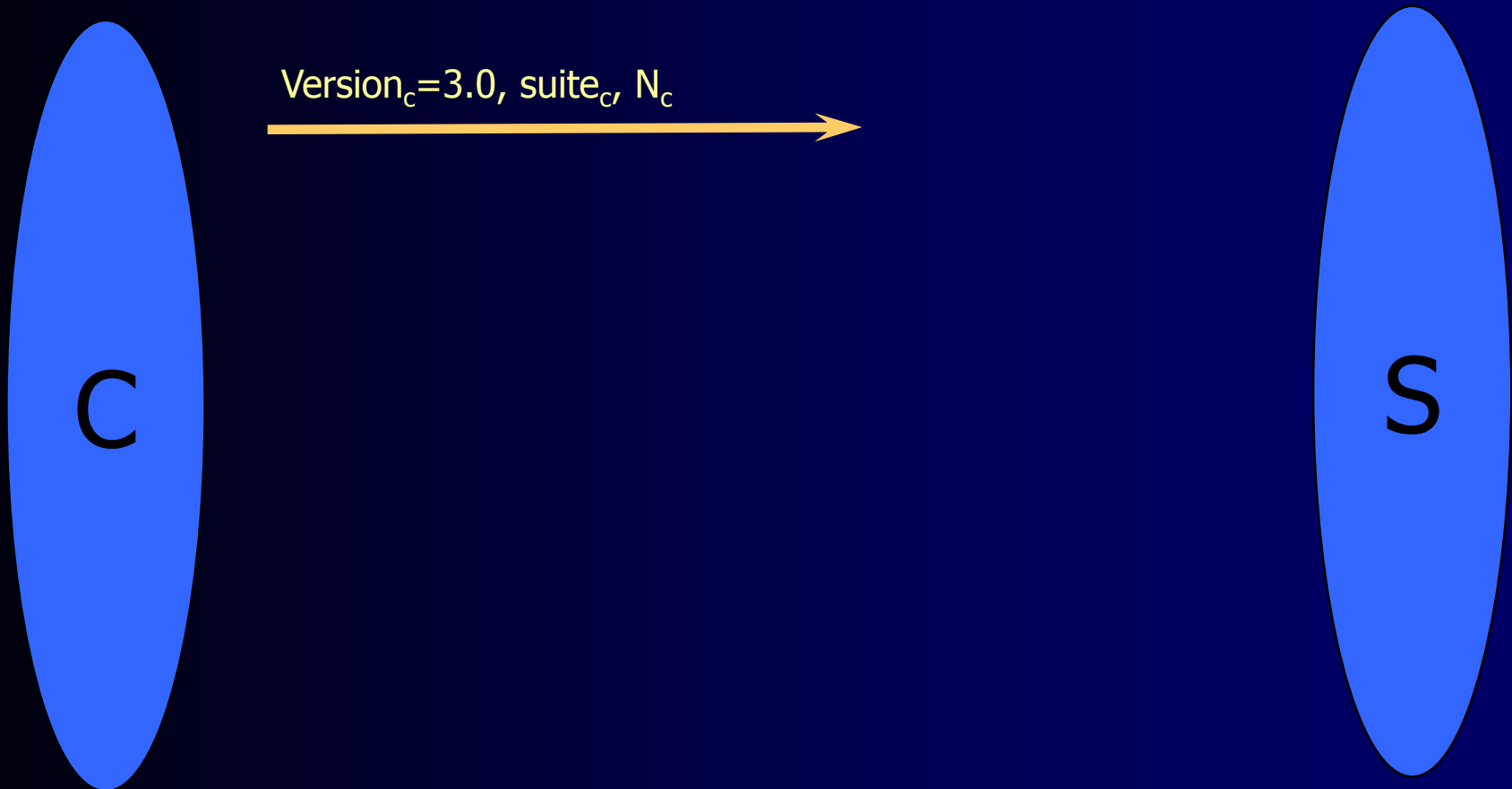
- حمله به RSA ← حمله زمانی (۲۰۰۳ میلادی)

حمله با بهره گیری از قالب pre-master-secret

آسیب پذیری ناشی از قالب PKCS#1 (۱۹۹۸ میلادی)

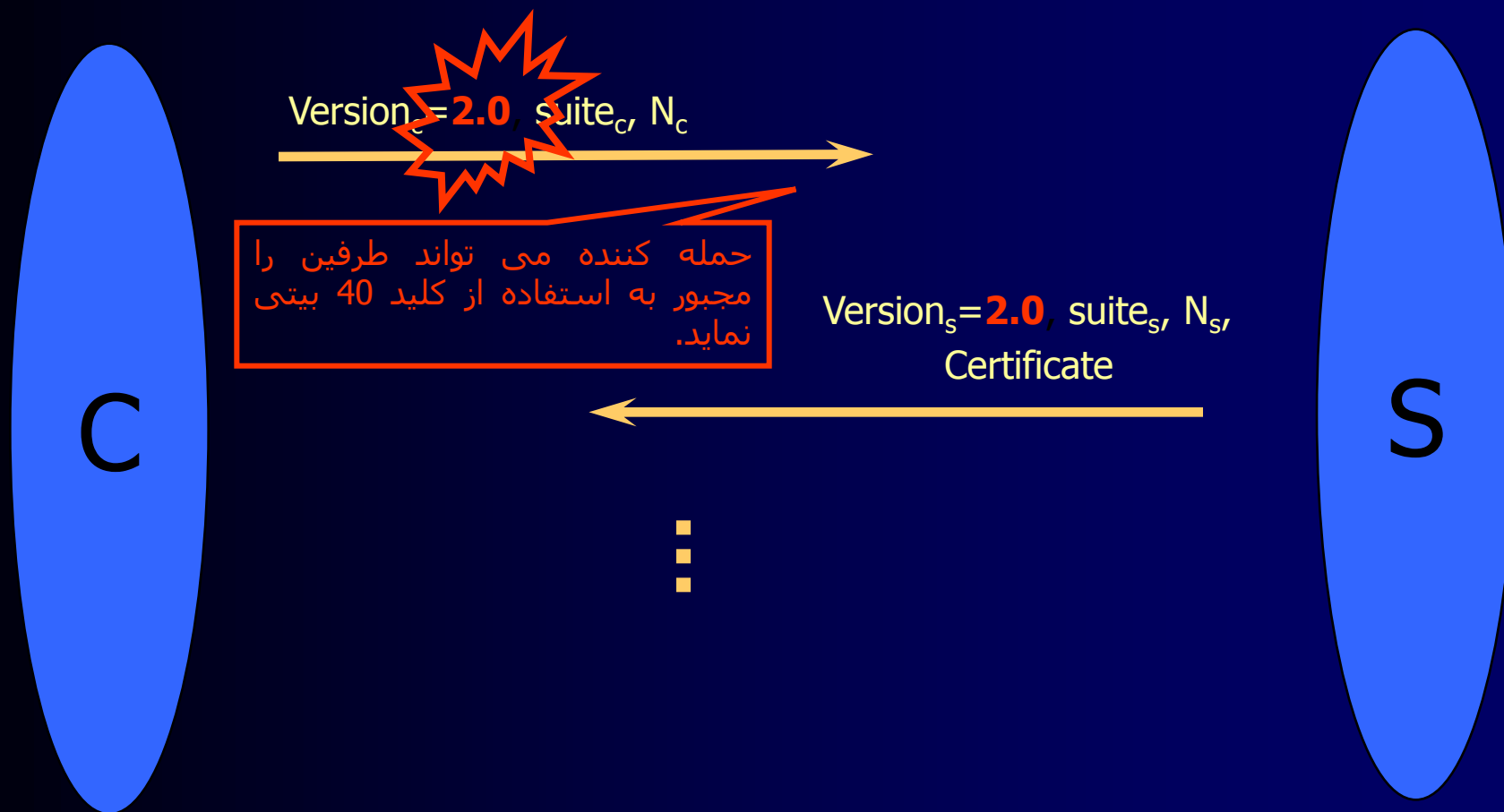
آسیب پذیری ناشی از قرار دادن مقدار نسخه در pre-master-secret (۲۰۰۳ میلادی)

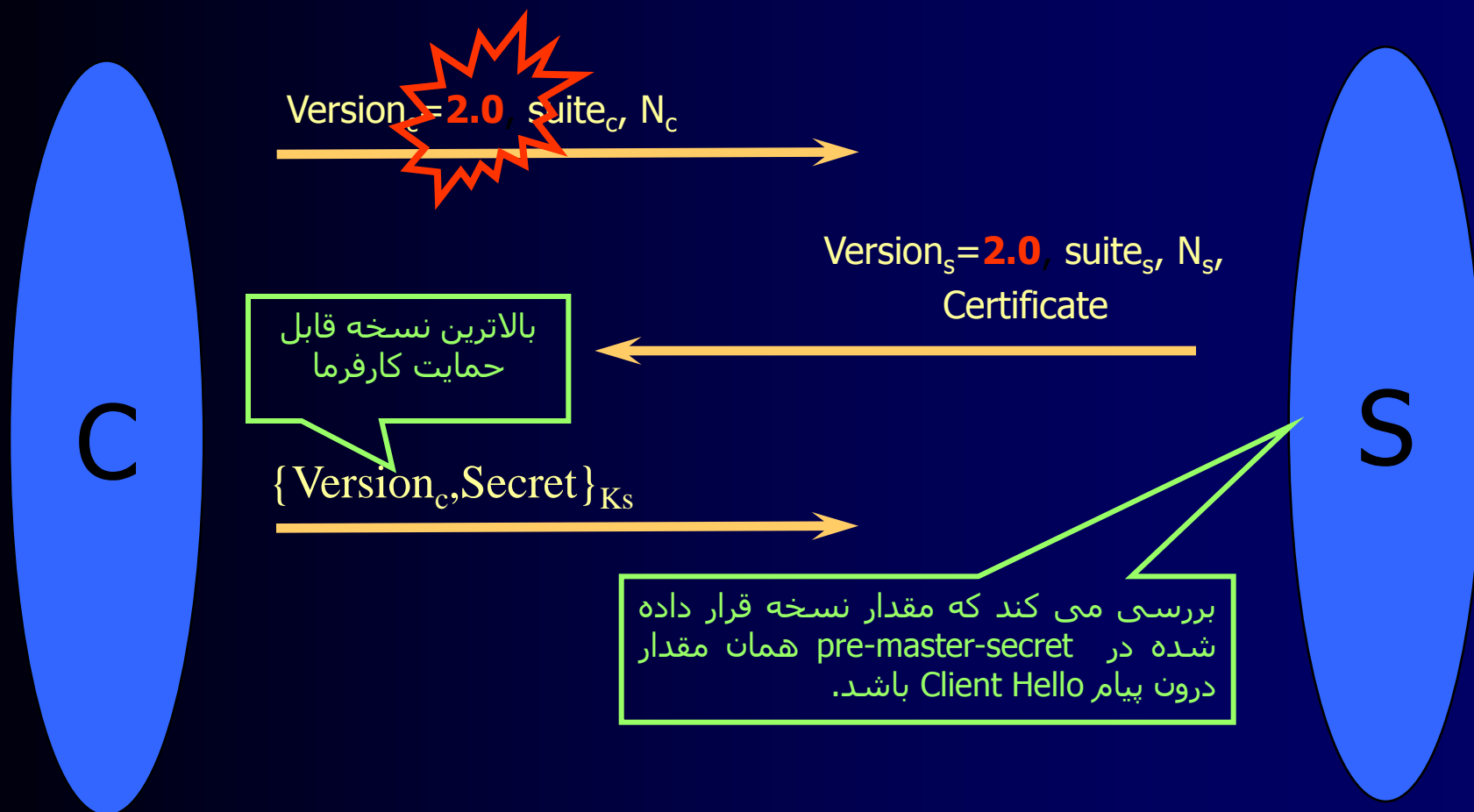
یکی از مهمترین ضعفهای نسخه SSL2.0 این است که پیامها را احراز اصالت نمی کند و حمله کننده به راحتی می تواند طرفین را مجبور به استفاده از کلید ۴۰ بیتی نماید.



حمله تنزل نسخه

یکی از مهمترین ضعفهای نسخه SSL2.0 این است که پیامها را احراز اصالت نمی کند و حمله کننده به راحتی می تواند طرفین را مجبور به استفاده از کلید ۴۰ بیتی نماید.





- تعریف

- راهکارهای مقابله با حمله DoS در SSL

۱. کمک گرفتن از کارفرما در رمزگشایی RSA

۲. معمای کارفرما

- SSL سرآیندهای TCP/IP را رمز نمی کند و در نتیجه اطلاعات مقصد، مبدأ و ساینز بسته ها قابل دسترسی است.

- روند حمله

۱. تهیه یک پایگاه داده از اطلاعات صفحات داخل سایت هدف
۲. شنود بسته های منتقل شده بین کارفرما و کارگزار با استفاده از ابزار شنودگر بسته
۳. جستجوی پایگاه داده برای یافتن صفحه منطبق با اطلاعات شنود شده
یک نمونه خروجی شنودگر بسته:

1460: 1463.herland.CS.Berkeley.EDU > 4243.amber.Berkeley.EDU

مبدأ

مقصد

ساینز بسته IP

- راهکارهای مقابله

۱. اصلاح خود پروتکلها


مثال: اضافه کردن پوشش تصادفی به بسته ها

۲. اصلاح و بازسازی سایتهای وب

مثال: شکستن صفحه به چندین صفحه کوچکتر

۳. استفاده از پروکسی میانی

- حملات شخص در وسط ← استفاده از ضعف کاربر



برای انجام حمله شخص در
وسط حمله کننده باید گواهینامه
معتبری ارائه دهد

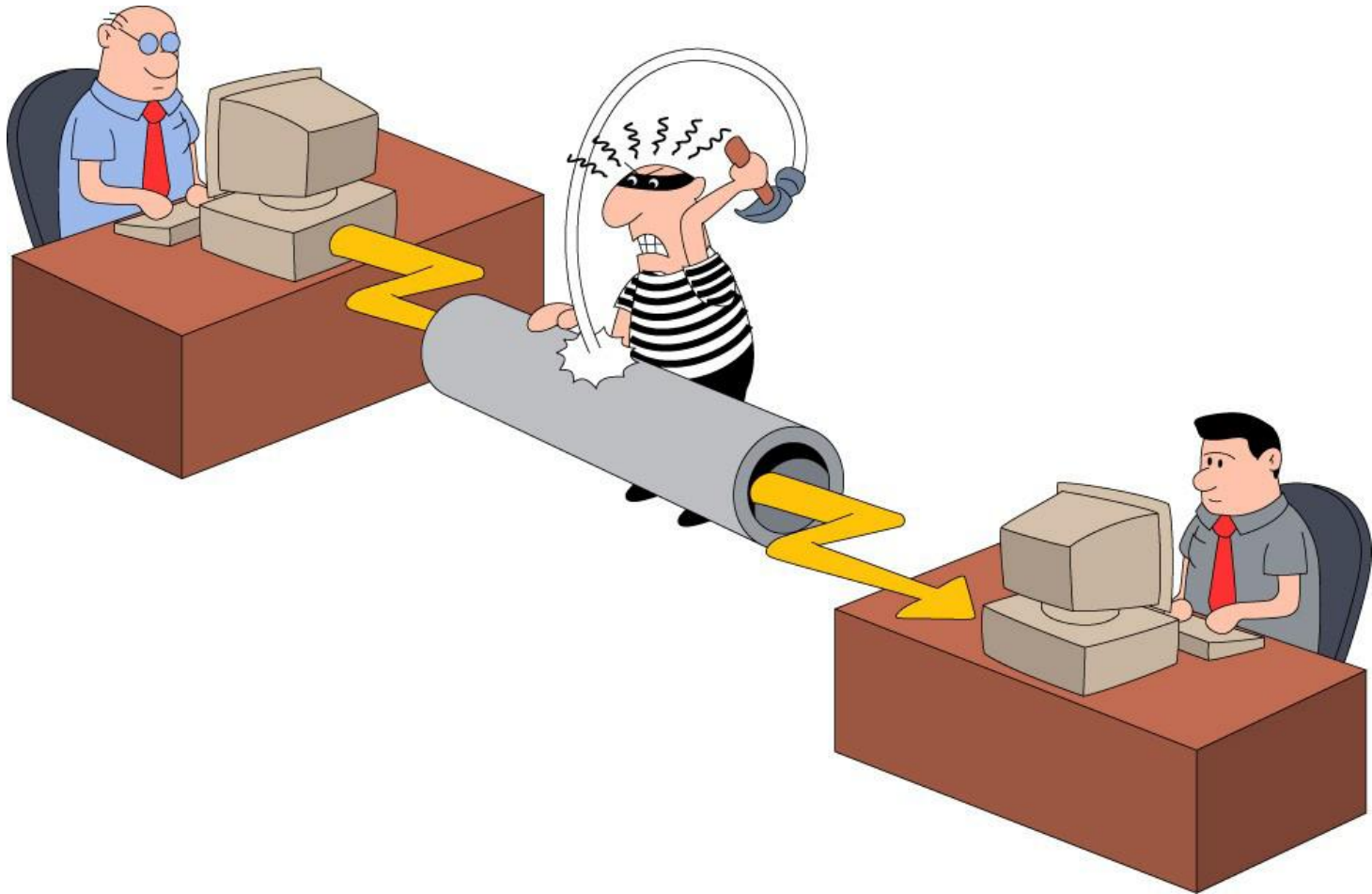
استفاده از پروتکل SSL

- حمله جستجوی کامل علیه کلیدهای ضعیف

کلیدهای ۴۰ بیتی در مدت زمان بسیار کوتاهی شکسته می شوند.

Man-In-The-Middle

128



حمله MITM به SSL/TLS

129

بیشتر مکانیزم های احراز هویت کاربر به کار گرفته شده، نمی توانند امنیت را در مقابل MITM حفظ کنند :

۱) احراز هویت سرور (در ارتباط SSL / TLS) به صورت ضعیف توسط مرورگر کاربر انجام می شود.

۲) در فرآیند برقراری session مرحله ی احراز هویت کاربر انجام نمی گیرد.

حمله MITM به SSL/TLS (چرا گوگل؟)

130

گوگل امکان فعال بودن همیشگی HTTPS روی کل محتوا را فراهم می کند.

راه های مقابله با چنین سرویس هائی از طرف کشور های مذکور :

- ۱- این سایت به طور کامل بلوکه شود.
- ۲- مهندسی معکوس کلید خصوصی گوگل.
- ۳- جعل گواهینامه دیجیتال و حمله MITM :

✓ تهیه گواهینامه از یکی از تأمین کنندگان معتبر (قانونی یا غیر قانونی)

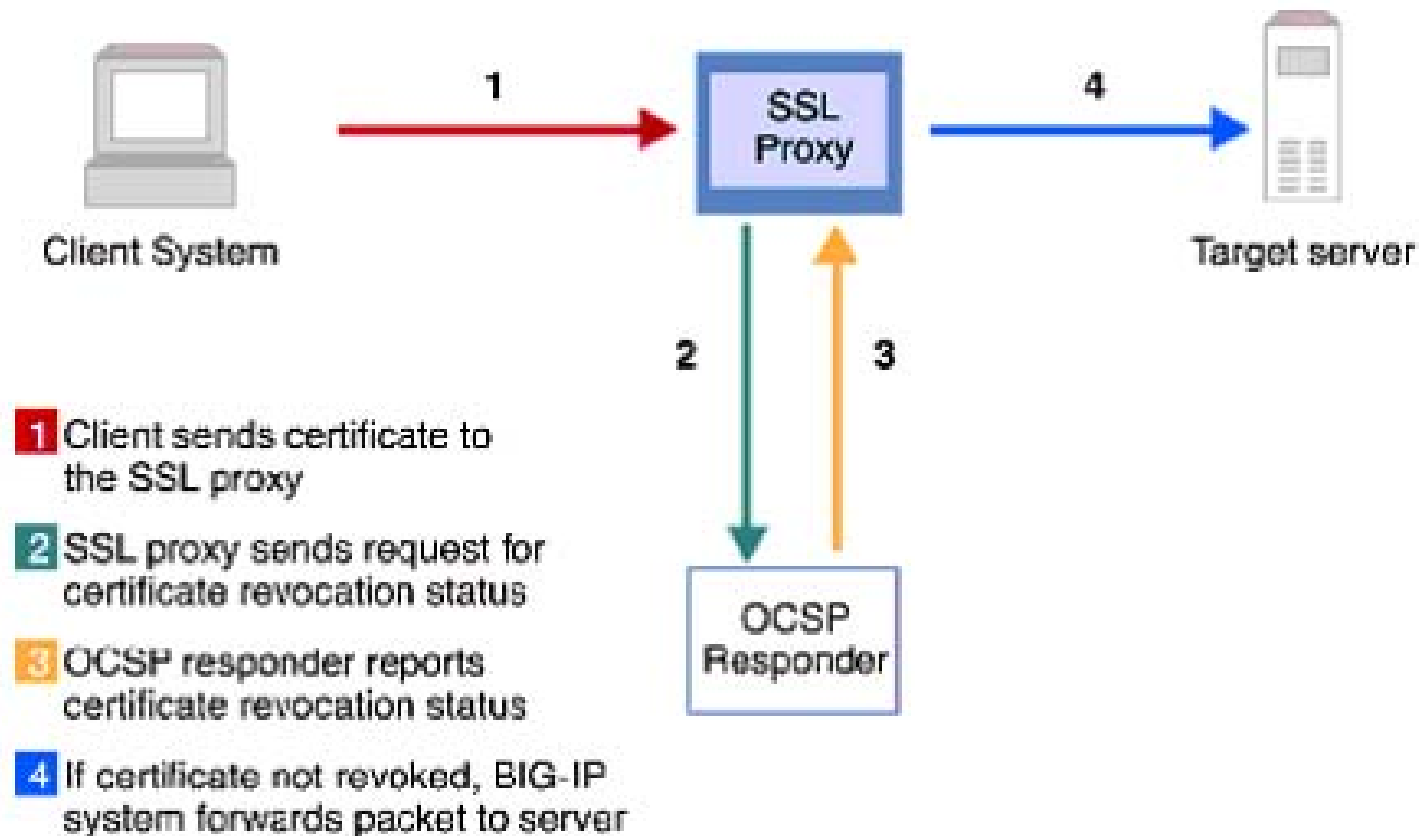
✓ انسداد امکان دسترسی به لیست CRL سرورهای تعیین اعتبار گواهینامه های دیجیتال (OCSP)

✓ فراهم بودن زیر ساخت اینترنت برای تغییر DNS ها

۴- ساخت و تحویل سیستم عامل یا مرورگر معیوب

نحوه دسترسی به OCSP

131



جعل گواهینامه برای MITM

132

✓ در ۱۵ مارس ۲۰۱۱ یک گروه هکر ایرانی موفق به نفوذ در یکی از نمایندگی های اروپائی شرکت آمریکائی **Comodo** شده و ۹ گواهینامه را برای ۷ سایت صادر کرد.

لیست سایتها به قرار زیر است:

- یک گواهینامه جعلی برای ساب دومین افزونه ها شرکت موزیلا (addons.mozilla.org)

- سه گواهینامه جعلی برای یاهو (login.yahoo.com)

- یک گواهینامه جعلی برای لایو میکروسافت (login.live.com)

- یک گواهینامه جعلی برای سرویس تلفن اینترنتی اسکایپ (login.skype.com)

- یک گواهینامه جعلی برای ([Global Trustee](https://GlobalTrustee.com))

- یک گواهینامه جعلی برای گوگل (www.google.com)

- یک گواهینامه جعلی برای جی میل (mail.google.com)

• شرکت **Comodo** ، IP و مشخصات هکر را به این ترتیب اعلام کرد :

• که این IP به شرکت پیشگامان توسعه ارتباطات تعلق دارد

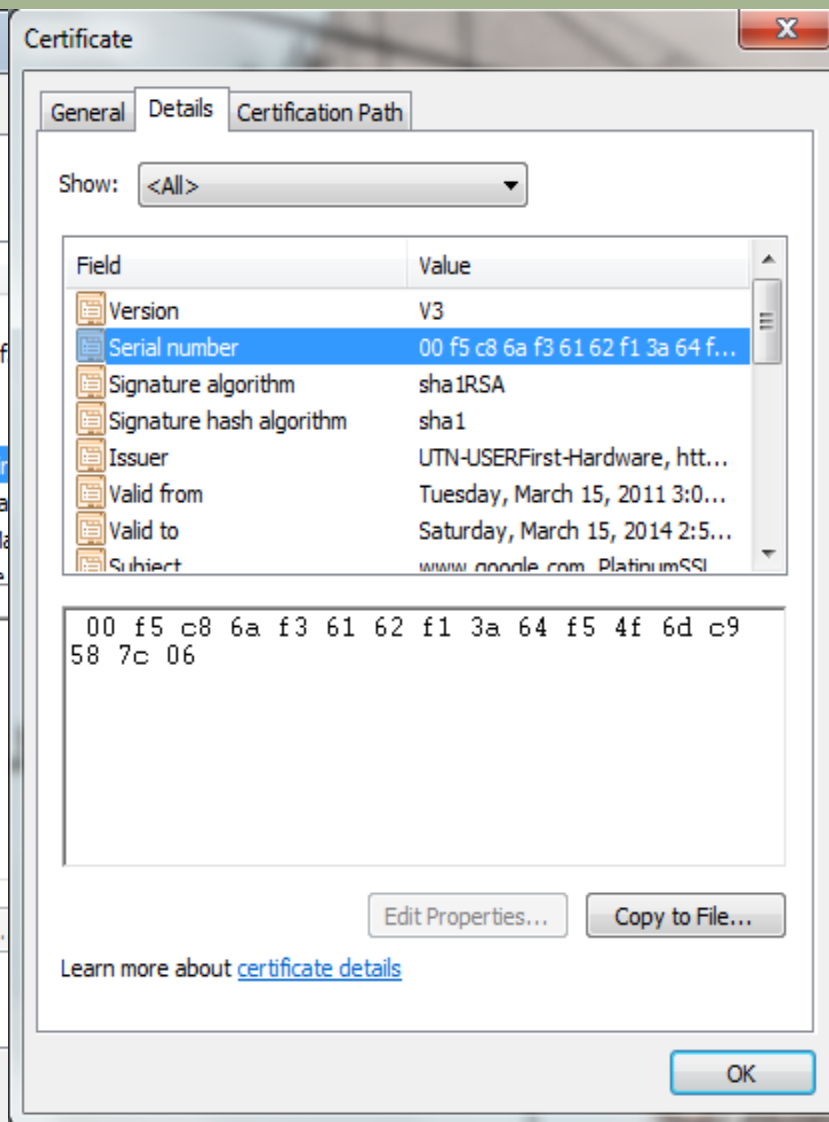
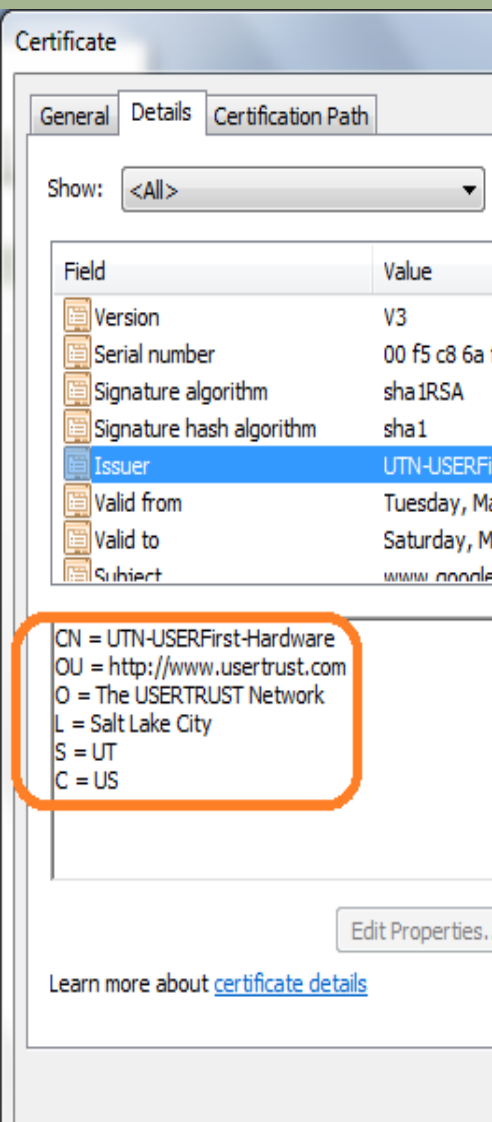
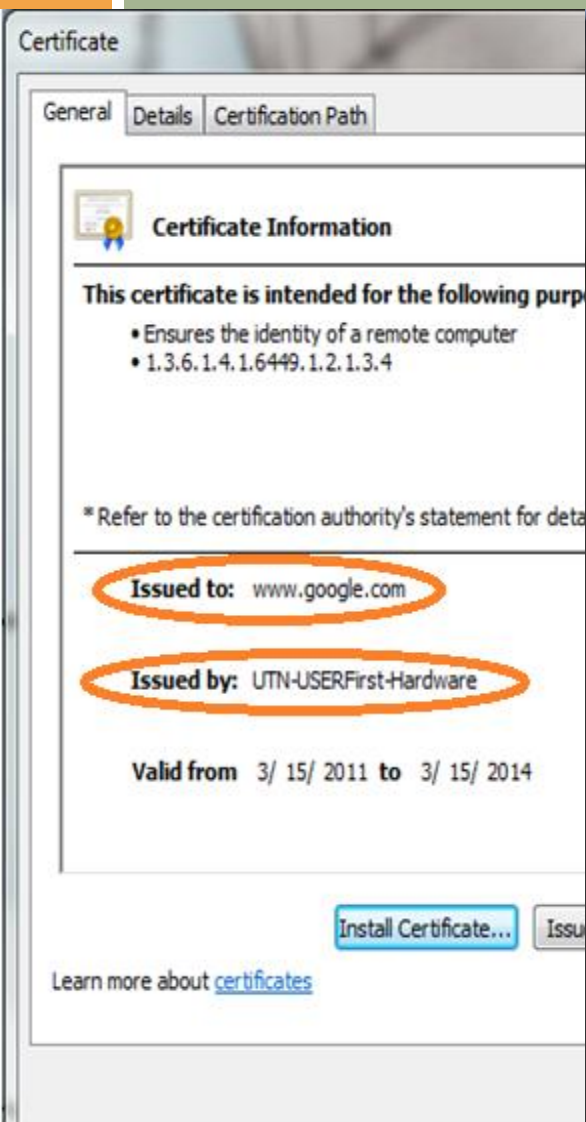
IP Address	212.95.136.18
City	Tehran
State or Region	Tehran
Country	Islamic Republic of Iran

✓ تعداد گواهی های صادر شده در حمله به **DigiNotar** در تاریخ ۱۰ ژوئیه ۵۰۰ عدد بوده و به نقل از بعضی بازرسان حتی برای سایت **CIA** نیز گواهی صادر شده بود.

✓ حمله مشابه دیگری در ماه مه به شرکت فروشنده **Certificate** به نام **Instant SSL** در ایتالیا نیز اتفاق افتاده بود.

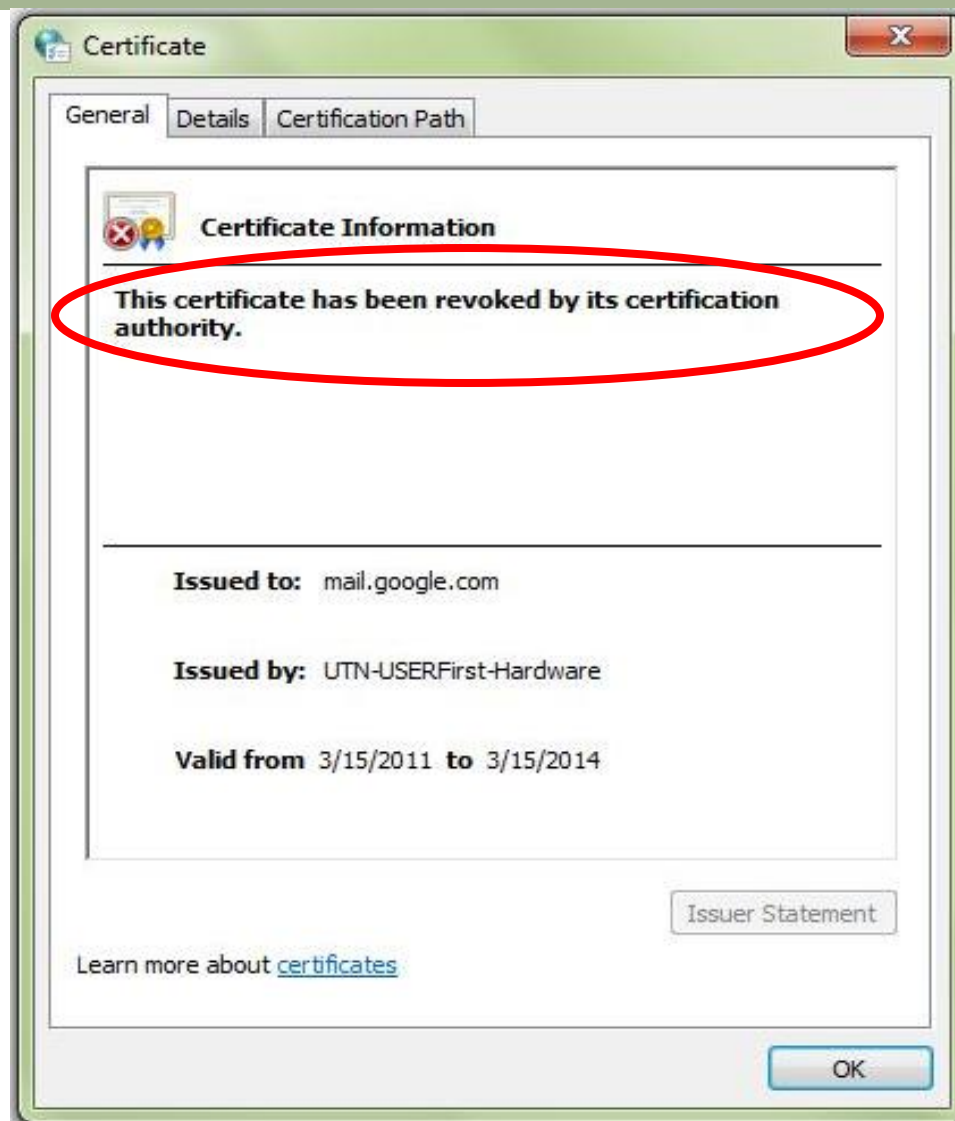
نمونه ای از گواهی های جعلی

133



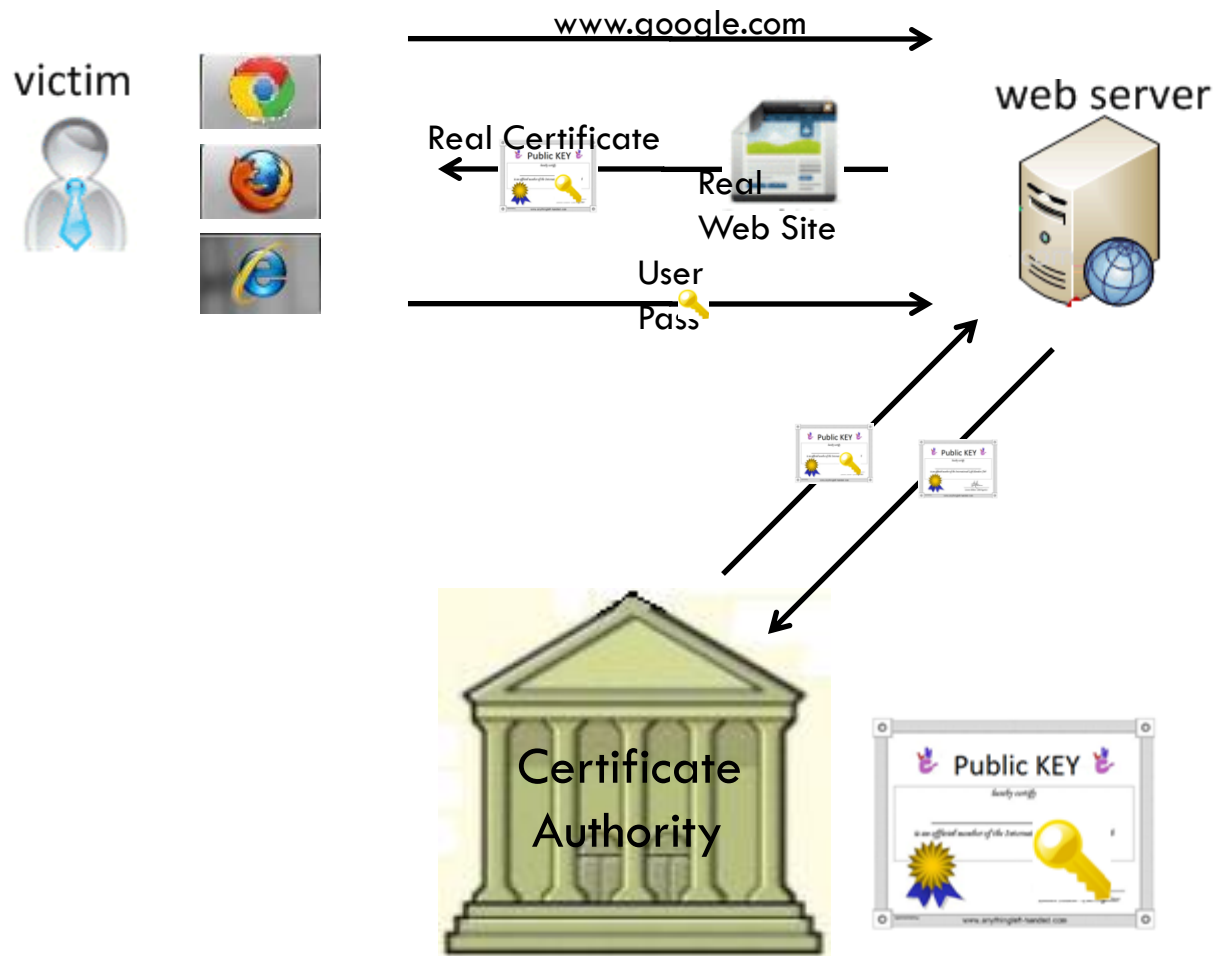
نمونه ای از گواهی های Revoke شده

134

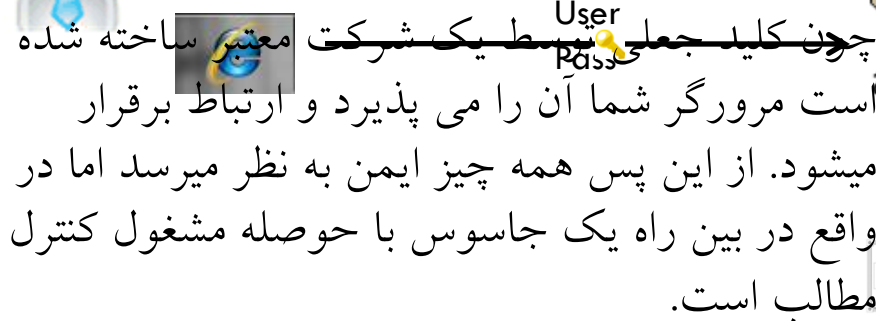


روند معمولی

135



136



نمونه ای از حمله توسط شرکت داتک

137

- در زمان بروز حملات، این سوال ایجاد شد که کدامیک از روترها و یا **Gateway** های مسیر، مسبب بروز مشکل است. با یک مقایسه ساده مسیر عبور (**Route**) ترافیک در زمانی که مشکلی وجود نداشت و در خلال فعال بودن حمله، این مورد به وضوح مشخص شد. یکی از **Gateway** های شرکت داتک مسبب بروز این مشکل بود. خروجی های **Traceroute** زیر نشان دهنده مسیر عبور ترافیک در هر دو حالت (معمولی و زمان حمله) می باشد.
- در زمان بروز حمله، کلیه ترافیک بجای عبور از **Gateway** همیشگی (۸۱.۹۱.۱۲۸.۱۱۴)، از یک **Gateway** ثانویه (۸۱.۹۱.۱۲۸.۱۱۸) عبور می کند.
- بمنظور جلوگیری از ایجاد گلوگاه (**Bottleneck**) بر روی سیستم شنود ترافیک بصورت کاملاً انتخابی به **Gateway** شنود هدایت میگردید و در صورت تلاش برای دسترسی به یکی از وب سایت های تحت حمله، ترافیک کاربر به سمت این **Gateway** خاص هدایت میشد.

مسیر ترافیک قبل از حمله

138

```
C:\windows\system32>tracert www.gmail.com
```

```
Tracing route to googlemail.l.google.com [72.14.234.83]  
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	48 ms	49 ms	49 ms	172.31.0.20
3	*	*	*	Request timed out.
4	48 ms	48 ms	48 ms	81.91.128.114
5	47 ms	55 ms	50 ms	ge-0-0-0.edge.datak-telecom.net [81.91.128.233]
6	49 ms	48 ms	47 ms	195.146.63.209
7	48 ms	48 ms	47 ms	195.146.63.253
8	201 ms	201 ms	200 ms	ldn-b1-link.telial.net [213.248.76.5]
9	246 ms	201 ms	199 ms	ldn-bb1-link.telial.net [80.91.248.90]
10	211 ms	207 ms	208 ms	prs-bb1-link.telial.net [80.91.247.34]
11	217 ms	217 ms	217 ms	ffm-bb1-link.telial.net [80.91.247.232]
12	217 ms	215 ms	217 ms	ffm-b7-link.telial.net [80.91.249.105]
13	390 ms	444 ms	397 ms	google-ic-120086-ffm-b7.c.telial.net [80.239.193.138]
14	403 ms	399 ms	400 ms	209.85.255.176
15	399 ms	403 ms	398 ms	209.85.251.112
16	402 ms	400 ms	403 ms	72.14.232.63
17	404 ms	403 ms	401 ms	mil01s07-in-f83.1e100.net [72.14.234.83]

```
Trace complete.
```

مسیر ترافیک در زمان حمله

139

===== [under attack] ===== [Google login] =====

```
C:\windows\system32>tracert www.gmail.com
```

Tracing route to googlemail.l.google.com [72.14.234.83]
over a maximum of 30 hops:

1	1 ms	<1 ms	<1 ms	192.168.1.1
2	49 ms	51 ms	50 ms	172.31.0.20
3	*	*	*	Request timed out.
4	48 ms	48 ms	48 ms	81.91.128.118
5	48 ms	51 ms	49 ms	ge-0-0-0.edge.datak-telecom.net [81.91.128.233]
6	48 ms	49 ms	47 ms	195.146.63.209
7	50 ms	51 ms	47 ms	195.146.63.253
8	203 ms	200 ms	201 ms	ldn-b1-link.telvia.net [213.248.76.5]
9	275 ms	202 ms	202 ms	ldn-bb1-link.telvia.net [80.91.248.90]
10	208 ms	208 ms	208 ms	prs-bb1-link.telvia.net [80.91.247.34]
11	217 ms	218 ms	216 ms	ffm-bb1-link.telvia.net [80.91.247.232]
12	217 ms	280 ms	217 ms	ffm-b7-link.telvia.net [80.91.254.249]
13	397 ms	399 ms	400 ms	google-118152-ffm-b7.c.telvia.net [213.248.102.234]
14	396 ms	397 ms	408 ms	209.85.255.176
15	402 ms	404 ms	401 ms	209.85.251.112
16	401 ms	409 ms	404 ms	72.14.232.63
17	401 ms	397 ms	399 ms	mil01s07-in-f83.1e100.net [72.14.234.83]

Trace complete.

چه اتفاقی برای Gmail افتاد؟

140

هکرها :

✓ زیر ساخت صدور گواهینامه SSL و EVSSL کمپانی را هدف قرار داده بودند.

✓ با پی بردن به این ضعف که همه سرورهای DigiNotar تحت کنترل یک User/Pass بودند که Pass آن نیز از لحاظ امنیتی زیاد قوی نبود، در Domain Server شرکت برای خود اجازه مدیریت صادر کرده بودند.

✓ پسورد ها و Zero-day Exploits را پیدا کرده ، در فایروال ها نفوذ کرده و سخت افزار رمز نگاری را که توسط DigiNotar برای remote access طراحی شده بود را دور زده بودند. (هنگامی که از یک ضعف امنیتی در همان روزی که کشف می شود برای حمله ای استفاده شود، این اصطلاح به کار می رود.)

۱- امکان صدور گواهینامه را برای گوگل و شرکت های بزرگ مشابه آن بلوکه و یا حداقل محدود کنیم.

۲- توسعه طرح هایی مثل **DNSSEC** برای رمز نگاری خود نام دامنه ها و ایمن کردن اطلاعات نام دامنه.

۳- اجازه به **DNS** ها برای مشخص کردن **CA** های خاص برای صدور گواهی های مربوط به آن ها (**CAA**)

۴- **DANE** برای اجازه پخش گواهی نامه ها بر روی **DNS**.

۵- استفاده از سیستم هایی که گواهی های صادره از **CA** های غیر معمول، برای یک سایت را با کمک گرفتن از **CA** های معروف بررسی می کنند.

۶- مرورگرها می توانند یک **Whitelist** از گواهی های معتبر ۱۰ یا ۲۰ سایت پر کاربر مثل **Google**، **Facebook**، **Yahoo** که معمولاً بیشتر هدف اقدامات جاسوسی قرار می گیرند، نگه داری کنند.

در حال حاضر چه می توان کرد؟

142

۱- استفاده از add-ons هایی مثل Certificate Patrol، Link Extend، Convergence در Fire Fox و امکاناتی مثل HTTPS Pinning در Chrome.

۲- هنگامی که نشانگر موس را بر روی لینکی قرار می دهید، لینک مورد نظر در نوار وضعیت نمایان می شود و با دقت در آن می توانید صحت یا عدم صحت اش را تشخیص دهید.





۳- حذف گواهینامه های مربوط به DigiNotar از لیست گواهینامه های موجود در مرورگر و یا به روز رسانی مرورگر ها.

۴- تعویض همه پسورد ها در فاصله های زمانی متناوب.

۵- استفاده از روش احراز هویت دو مرحله ای

در حال حاضر چه می توان کرد؟

143

Icon	What it means
	The site isn't using SSL. Most sites don't need to use SSL because they don't handle sensitive information. Avoid entering sensitive information, such as usernames and passwords, on the page.
 https://	Google Chrome has successfully established a secure connection with the site. Look for this icon and make sure the URL has the correct domain, if you're required to log in to the site or enter sensitive information on the page. If a site uses an Extended Validation SSL (EV-SSL) certificate, the organization's name also appears next to the icon in green text. Make sure the browser is set to check for server certification revocation to identify sites with EV-SSL certificates.
 https://	The site uses SSL, but Google Chrome has detected insecure content on the page. Be careful if you're entering sensitive information on this page. Insecure content can provide a loophole for someone to change the look of the page.
 https://	The site uses SSL, but Google Chrome has detected either high-risk insecure content on the page or problems with the site's certificate. Don't enter sensitive information on this page. Invalid certificate or other serious https issues could indicate that someone is attempting to tamper with your connection to the site.

در حال حاضر چه می توان کرد؟

144

□ اگر مرورگر شما خطاری با مفهوم عدم تایید ارتباط ایمن داد آن را جدی بگیرید مگر آنکه مطمئن باشید بی خطر است. مثلاً "بانکداری الکترونیکی ایران در شروع با همین اخطار مواجه میشود اما بی خطر است. اما اگر در ایمیل و ... به این شکلها برخورد کردید مسلماً "جاسوسی در میان است."



Suspected Web Forgery!

The web site at www.mozilla.com has been reported as a web forgery designed to trick users into sharing personal or financial information.

Entering any personal information on this page may result in identity theft or other fraud.

These types of web forgeries are used in scams known as phishing attacks, in which fraudulent web pages and emails are used to imitate sources you may trust.

You can find out more about [how Firefox protects you](#) from phishing attacks.

Get me out of here!



This Connection is Untrusted

You have asked Firefox to connect securely to **172.16.254.20**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

► Technical Details

► I Understand the Risks

در حال حاضر چه می توان کرد؟

145

Two-Step Verification امکان جدید گوگل برای افزایش امنیت حساب کاربران

✓ این قابلیت به کاربر اجازه می دهد برای شناسایی و احراز هویت خود، علاوه بر رمز عبور، به یک کد ثانویه که به صورت یک بار مصرف و تصادفی ایجاد شده و از طرف گوگل برایش ارسال می شود نیز اتکا کند.

• این کد به سه طریق می تواند در اختیار کاربر قرار گیرد

۱- نرم افزاری برای گوشی های اندروید، آیفون و بلک بری

(نرم افزار کار این نرم افزار به این شکل است که بارکدی که گوگل به شما تحویل می دهد را با گوشی خود اسکن می کنید و سپس نرم افزار مربوطه، کدهای رمز ثانویه را با توجه به بارکدی که اسکن کرده، تولید می کند.) تماس صوتی از جانب گوگل

It 's time to move beyond this method of security...

پایان