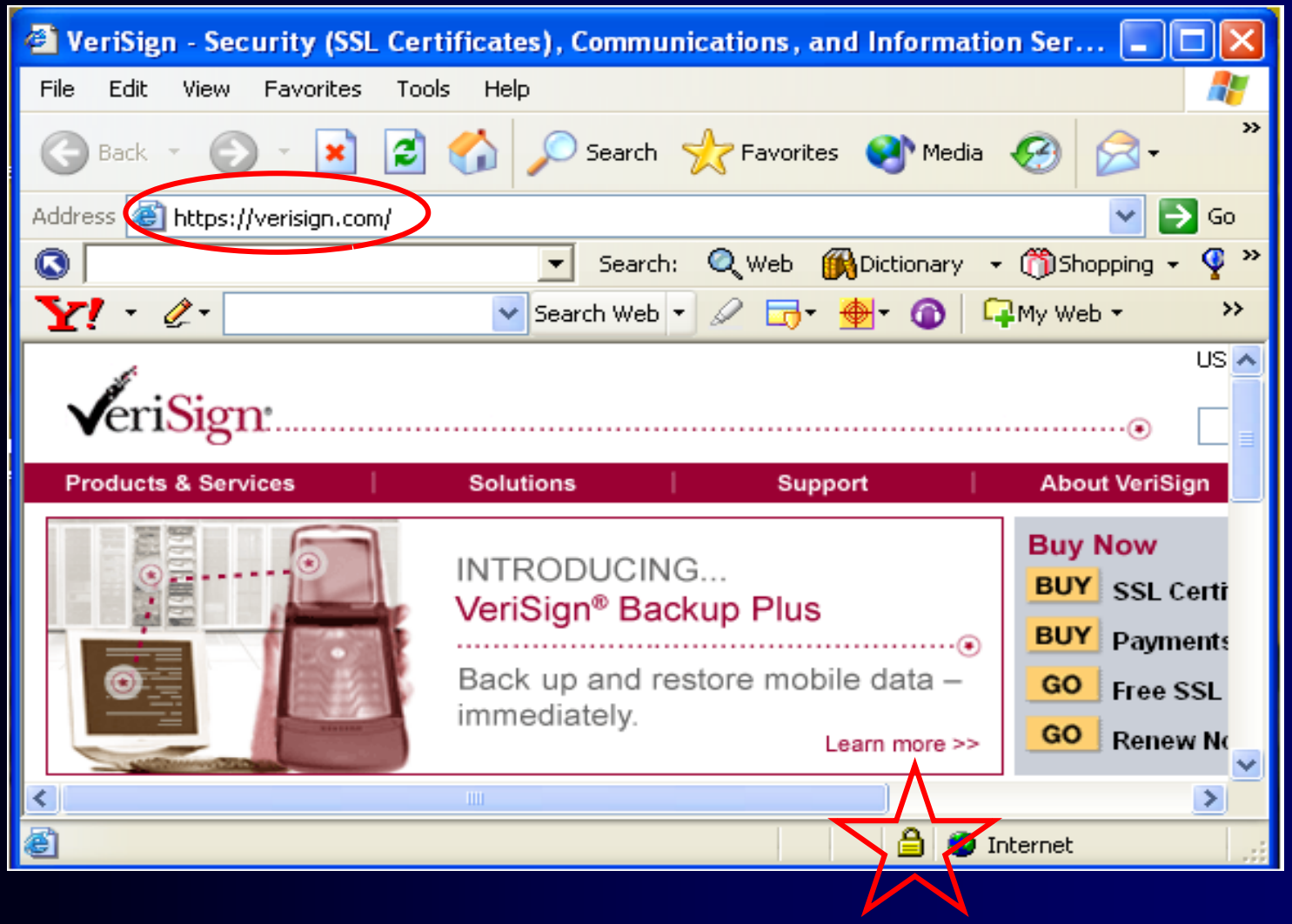
پروتکل SSL

فهرست مطالب

- مقدمه
- معرفی پروتکل SSL
- بررسی حملات انجام شده علیه SSL

مقدمه


VeriSign - Security (SSL Certificates), Communications, and Information Ser...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://verisign.com/
Go
Search: Web Dictionary Shopping
Search Web My Web
US
VeriSign
Products & Services
Solutions
Support
About VeriSign
INTRODUCING...
VeriSign® Backup Plus
Back up and restore mobile data – immediately.
Learn more >>
Buy Now
BUY SSL Certi
BUY Payments
GO Free SSL
GO Renew Nc
Internet

تاریخچه

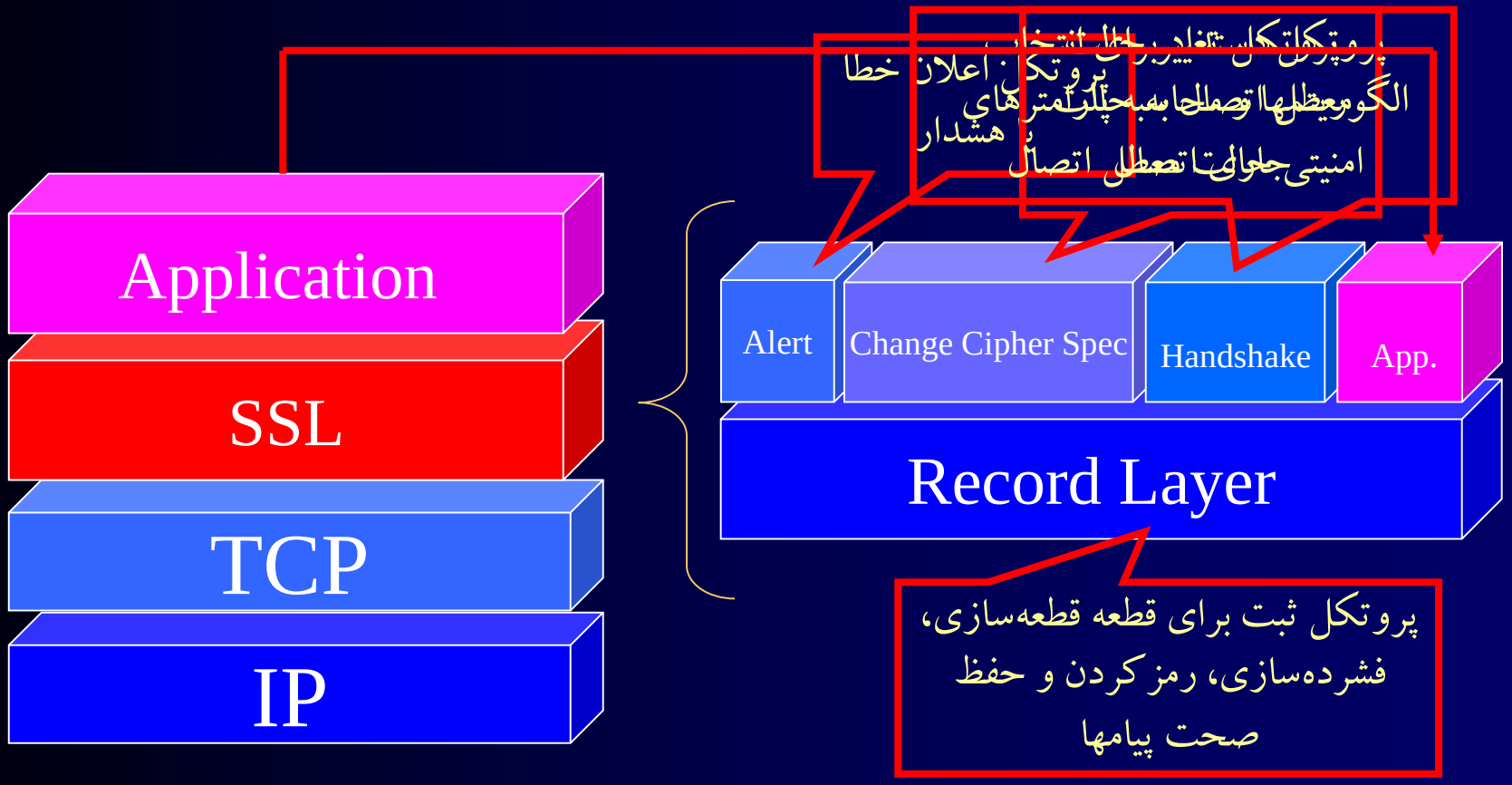
- **SSL1.0** اولین طراحی شرکت Netscape * سال ۱۹۹۴ میلادی.
  این نسخه هیچگاه منتشر نشد !
- SSL2.0 توسط شرکت Netscape طراحی و منتشر شد * اوایل سال ۱۹۹۵میلادی.
- SSL3.0 توسط شرکت Netscape طراحی و منتشر شد * اوایل سال ۱۹۹۶ میلادی.
  در ابتدای ماه می سال ۱۹۹۶ میلادی، توسعه SSL تحت مسئولیت IETF در آمد.
- TLS1.0 اولین نسخه استاندارد پروتکل SSL * اوایل سال ۱۹۹۹ میلادی.
- TLS1.1 برای رفع ضعفهای TLS1.0 منتشر شد.

فهرست مطالب

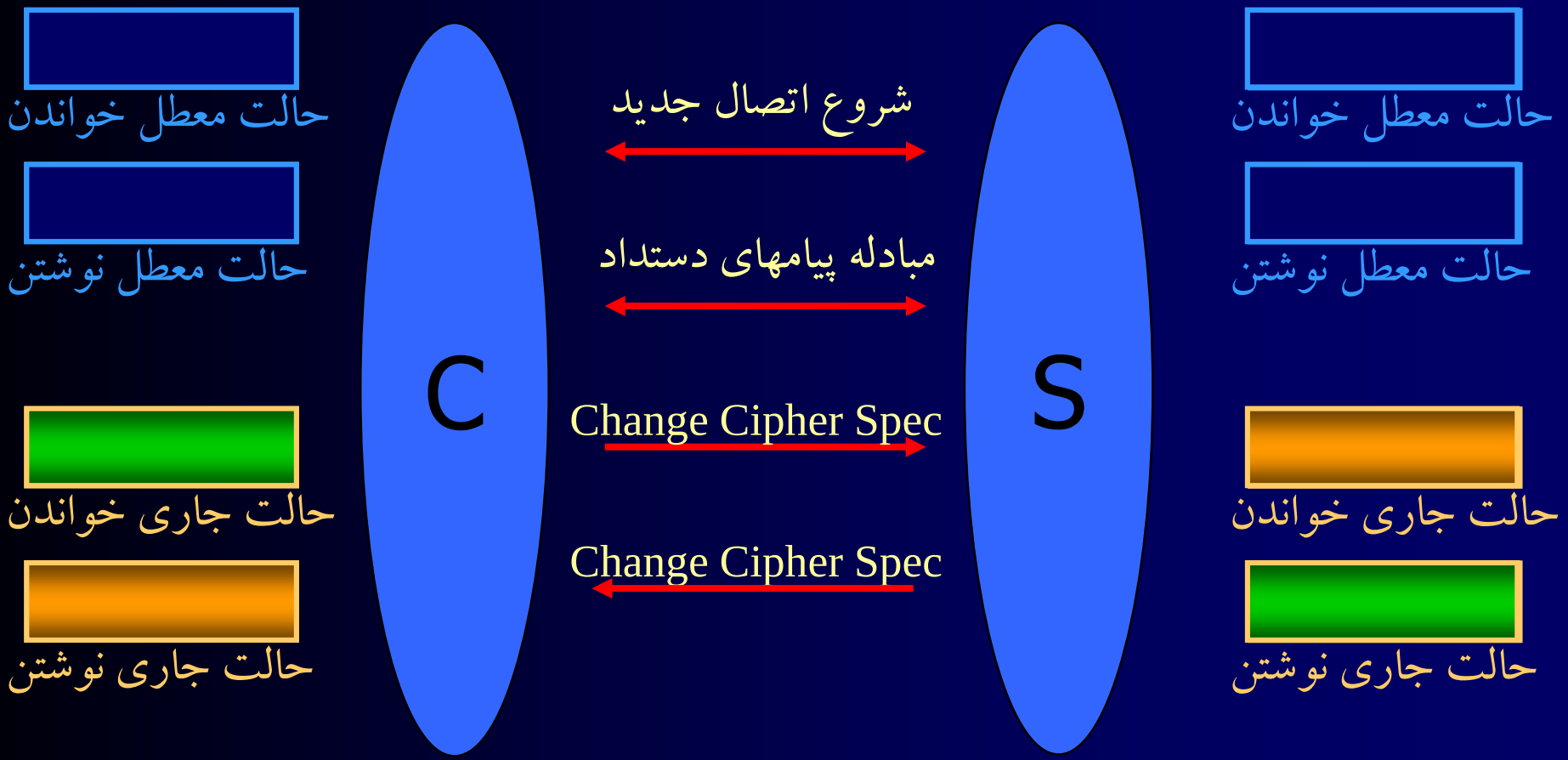
- مقدمه
- معرفی پروتکل SSL
- بررسی حملات انجام شده علیه SSL

Secure Socket Layer

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



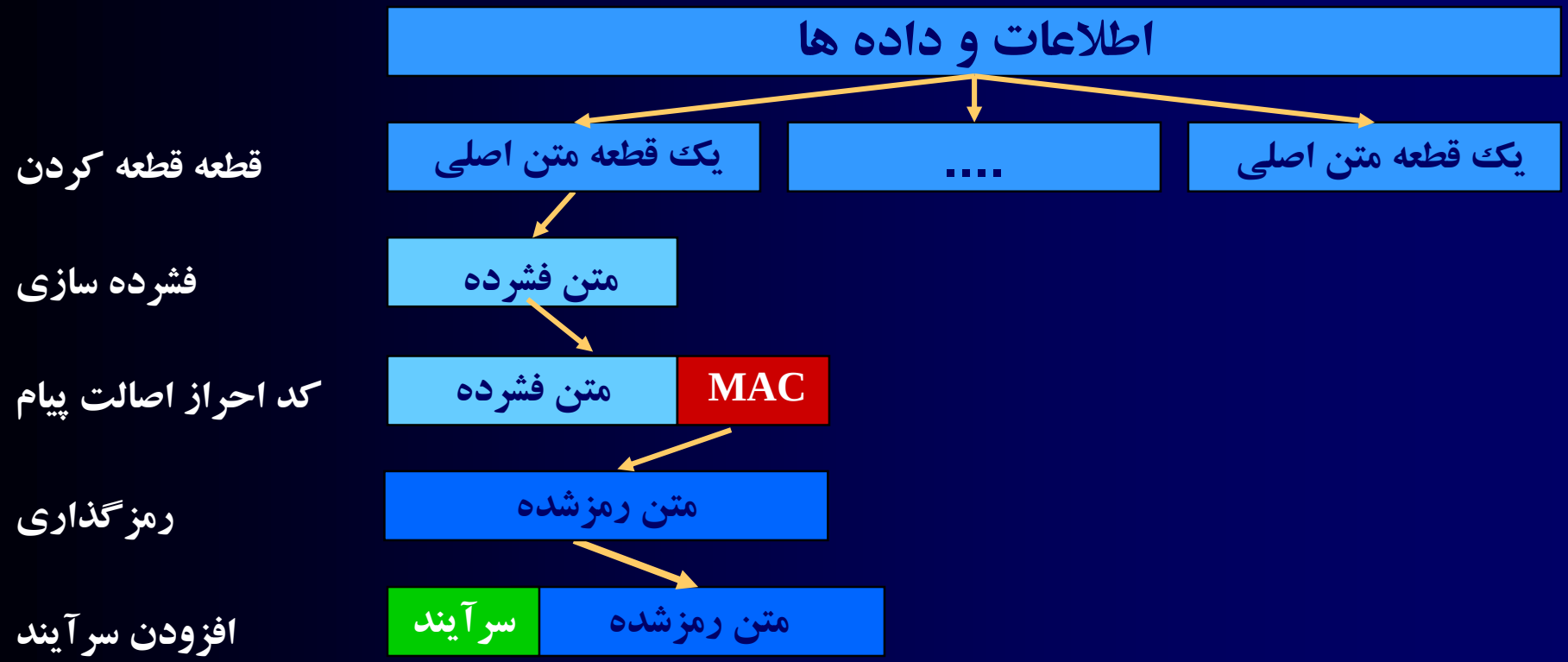
حالات چهار گانه اتصال



پروتکل ثبت

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.



سرآیند ثبت =

پروتکل اعلان خطا

- پیام این پروتکل شامل دو بایت است.

شدت خطا

اگر خطا در حد هشدار باشد : مقدار بایت = ۱

اگر خطا مهلک باشد: مقدار بایت = ۲

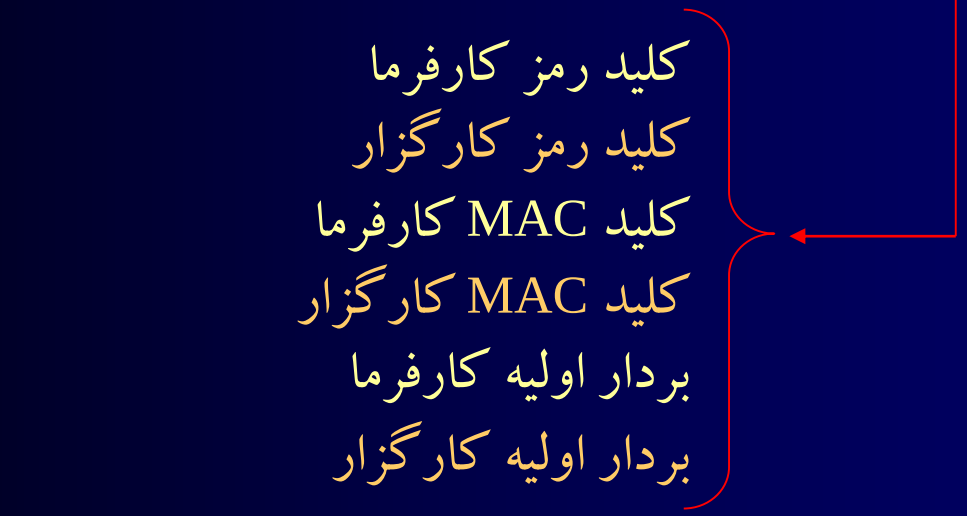
شرح خطا

پروتکل دستداد

- توافق روی الگوریتمهای لازم برای جلسه
- تبادل پارامترهای رمزنگاری لازم برای توافق طرفین روی یک pre-master-secret
- مبادله گواهینامه به منظور احراز اصالت طرفین
- تولید پارامترهای امنیتی حالت معطل اتصال برای لایه ثبت
- ایجاد اطمینان از درستی محاسبات و مذاکرات

محاسبه پارامترهای امنیتی حالت معطل اتصال

- محاسبه master-secret به کمک pre-master-secret و اعداد تصادفی مبادله شده
- محاسبه پارامترهای امنیتی لازم به کمک master-secret و اعداد تصادفی مبادله شده

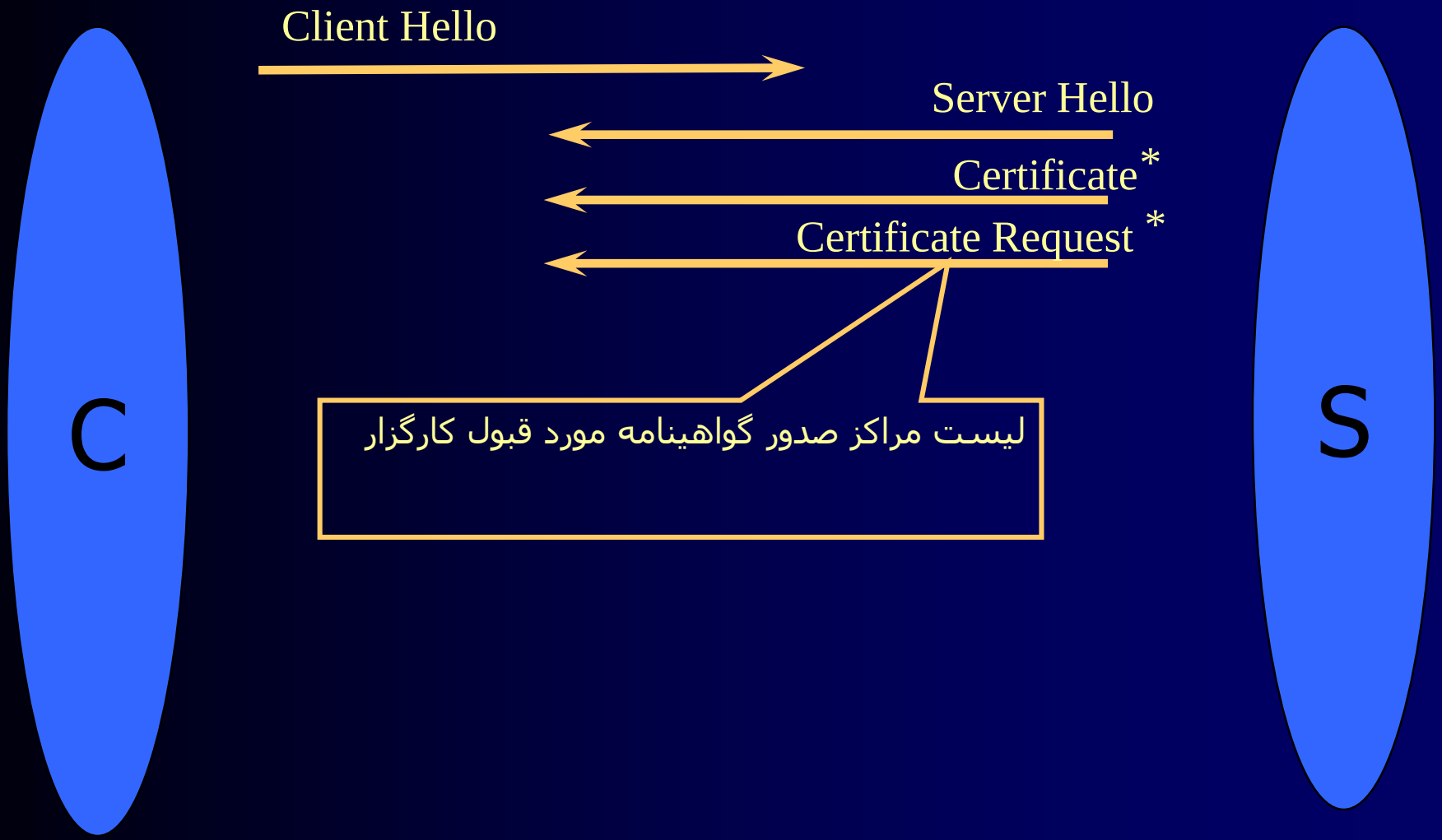


روند تبادل پیامها در یک دستداد کامل

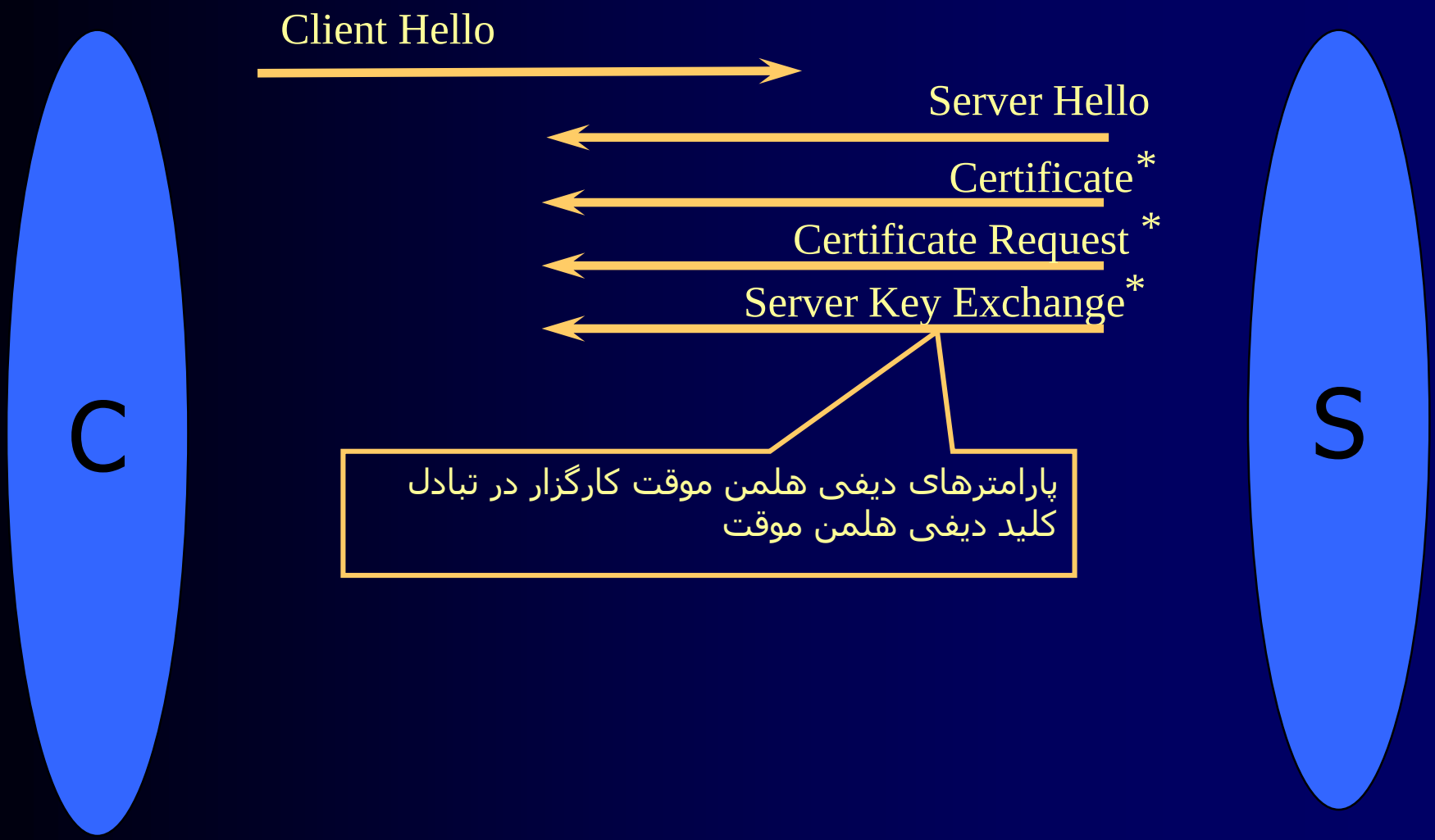
روند تبادل پیامها در یک دستداد کامل

روند تبادل پیامها در یک دستداد کامل

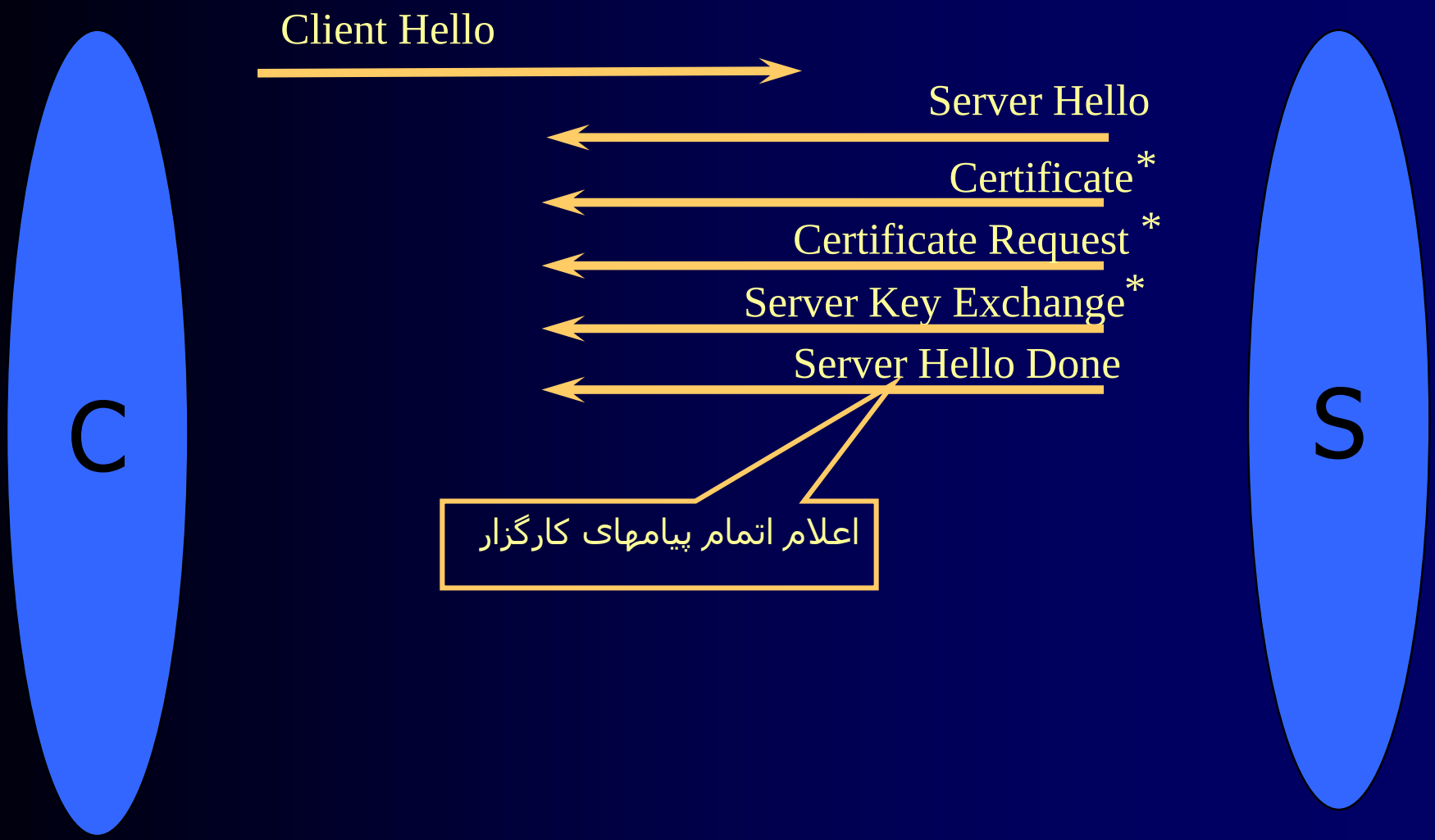
روند تبادل پیامها در یک دستداد کامل



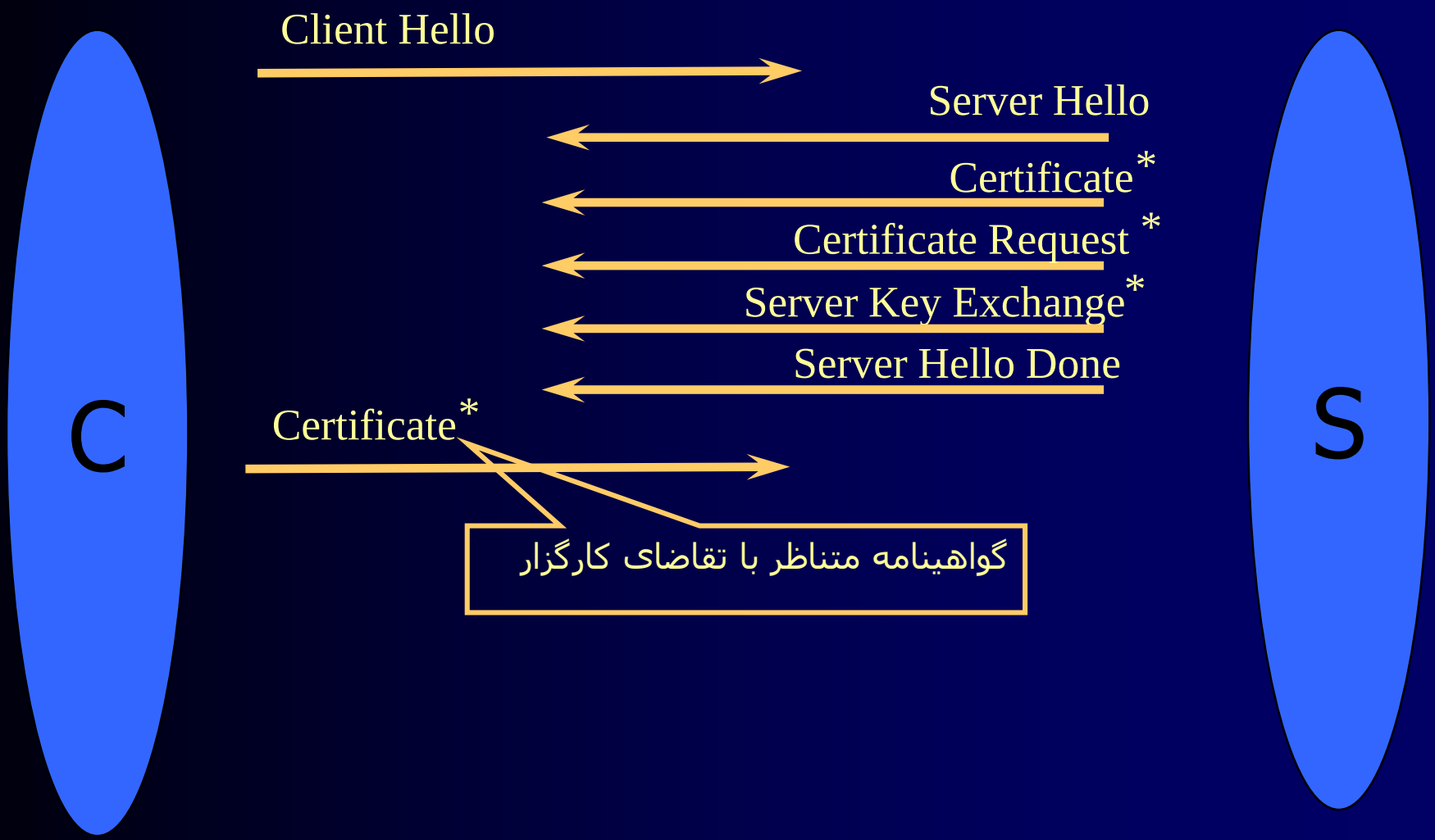
روند تبادل پیامها در یک دستداد کامل



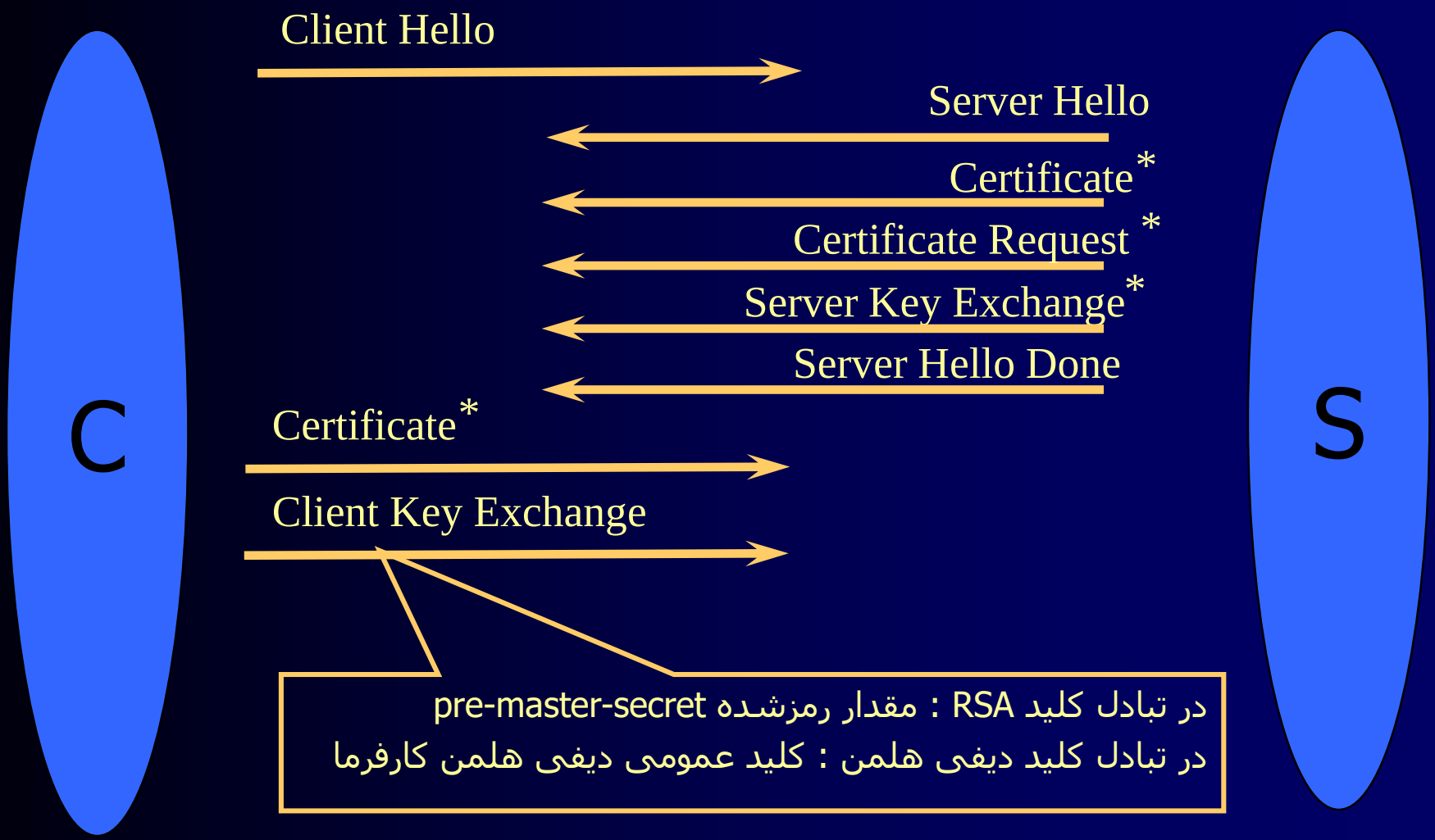
روند تبادل پیامها در یک دستداد کامل



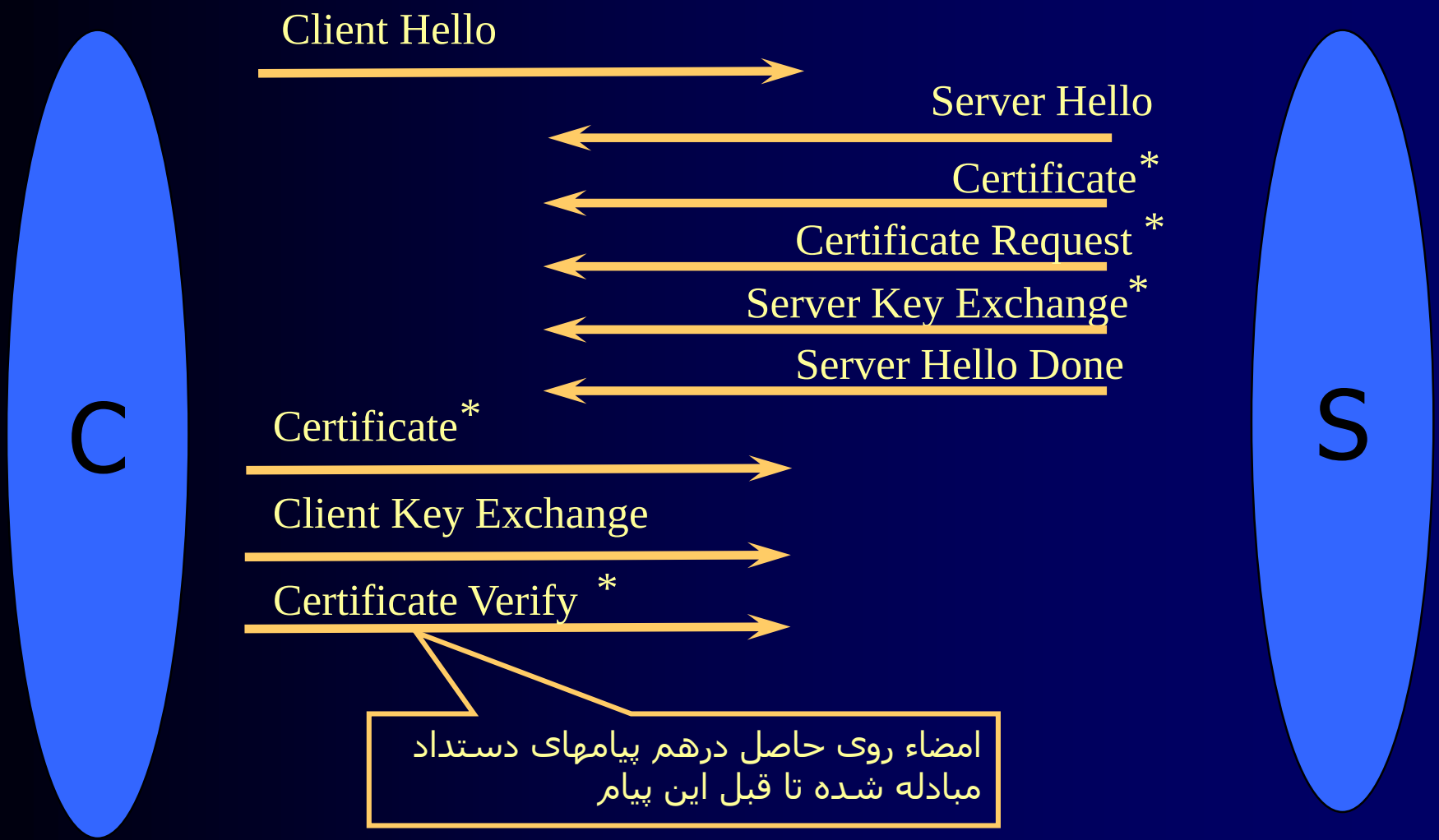
روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل



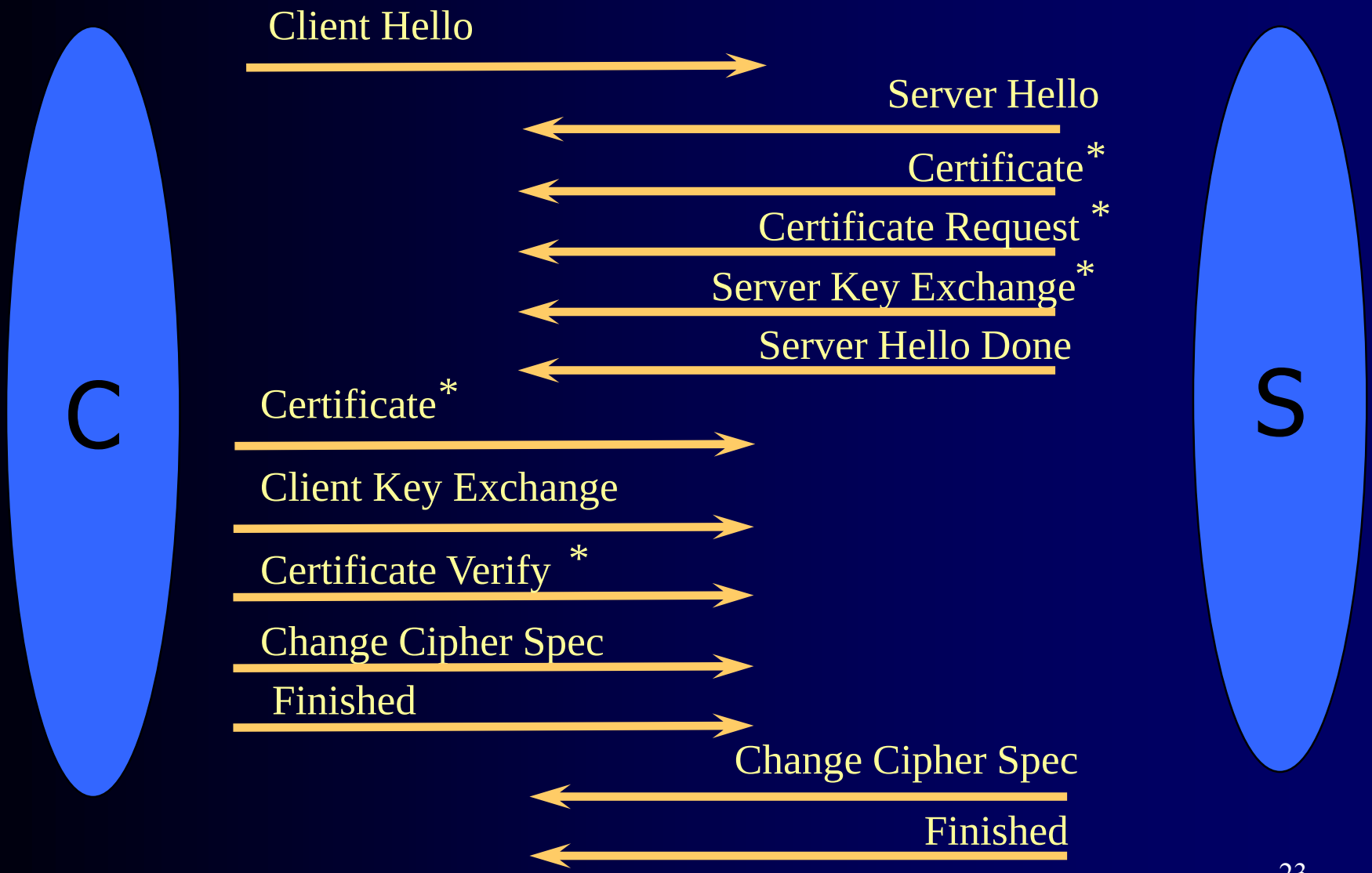
روند تبادل پیامها در یک دستداد کامل



روند تبادل پیامها در یک دستداد کامل

روند تبادل پیامها در یک دستداد کامل

روند تبادل پیامها در یک دستداد کامل



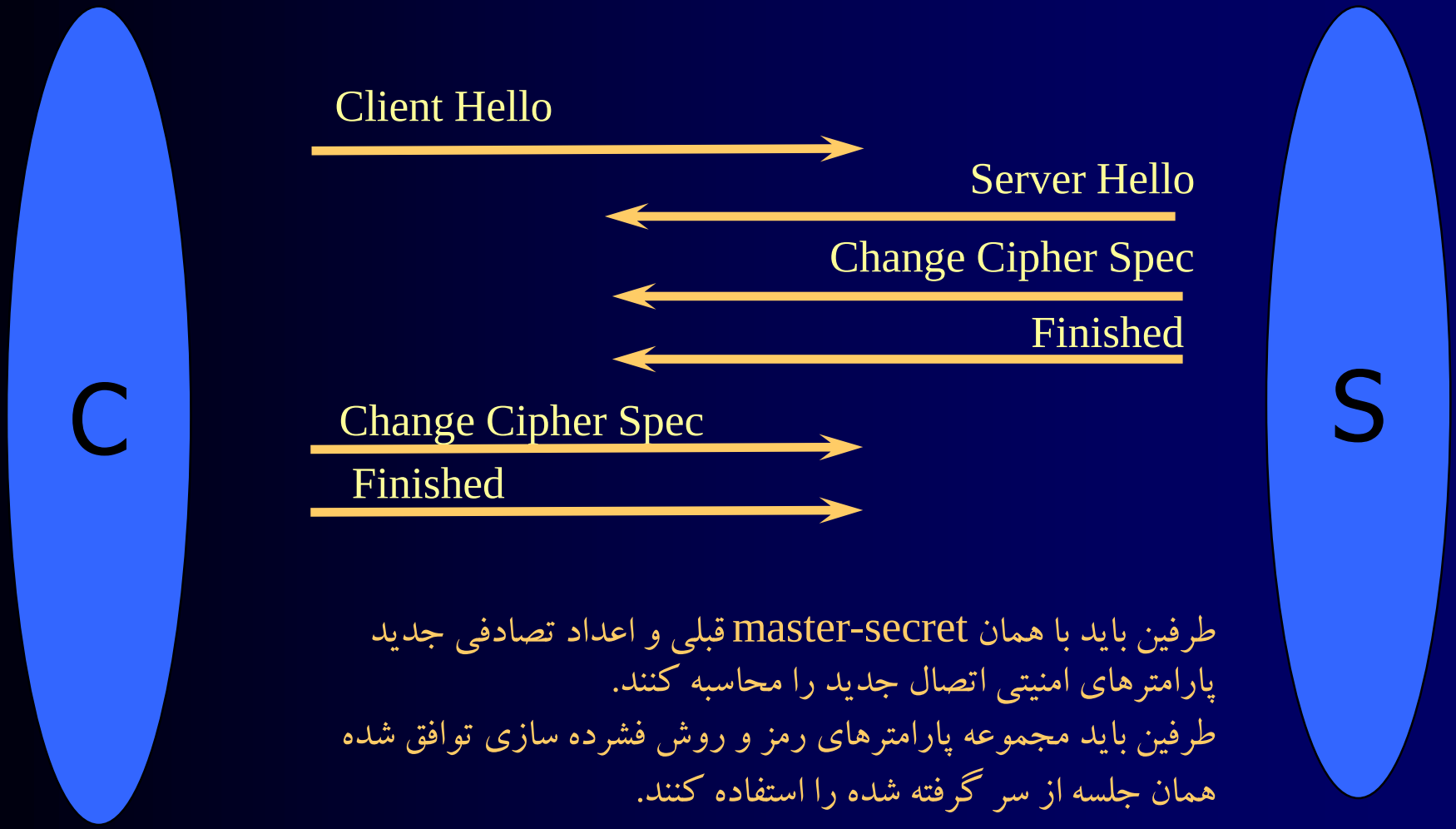
از سر گیری جلسه

- فرآیند تبادل کلید موجب کاهش سرعت برقراری جلسه است.

- تفاوت اتصال و جلسه

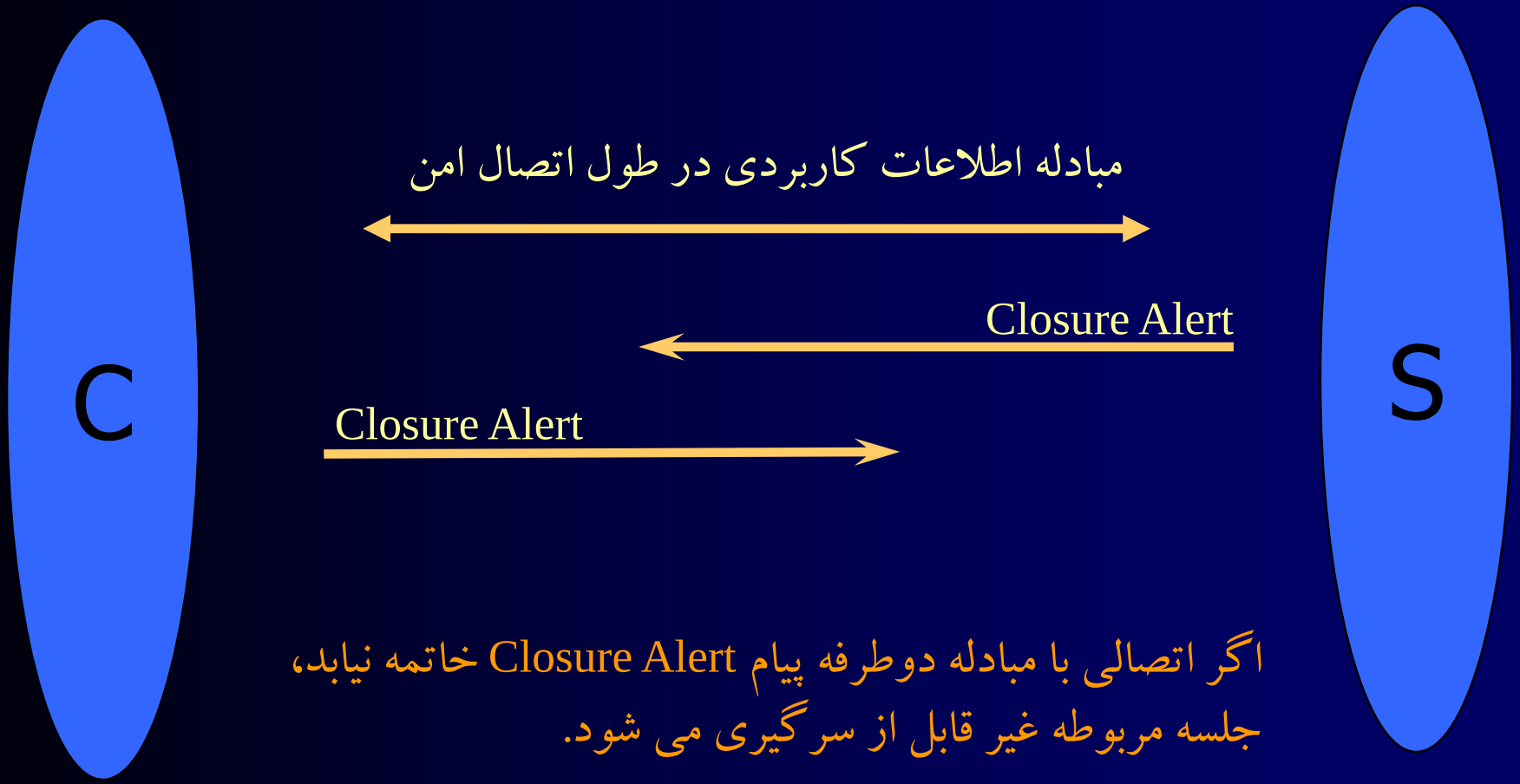
یک جلسه می تواند چندین اتصال را در بر داشته باشد.

روند تبادل پیامها هنگام از سر گیری جلسه



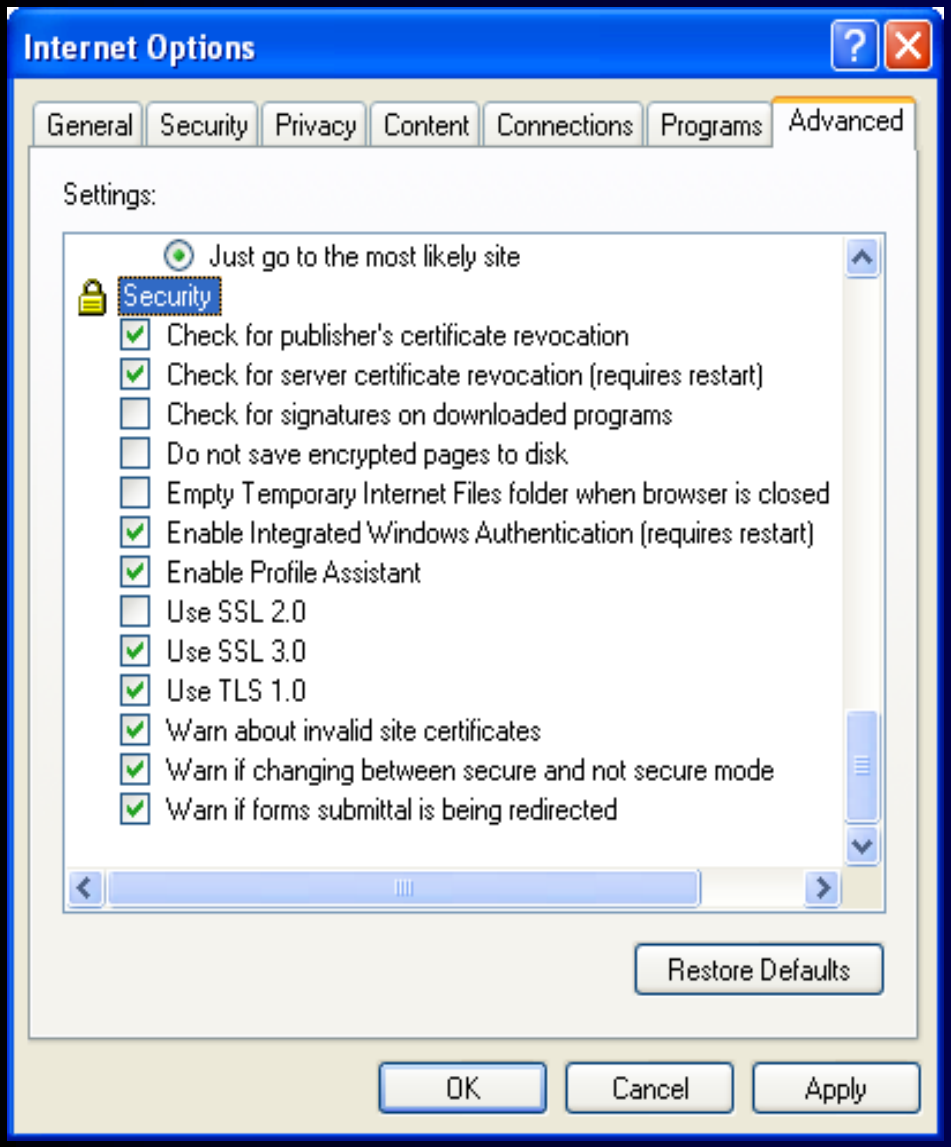
طرفین باید با همان master-secret قبلی و اعداد تصادفی جدید پارامترهای امنیتی اتصال جدید را محاسبه کنند.
طرفین باید مجموعه پارامترهای رمز و روش فشرده سازی توافق شده همان جلسه از سر گرفته شده را استفاده کنند.

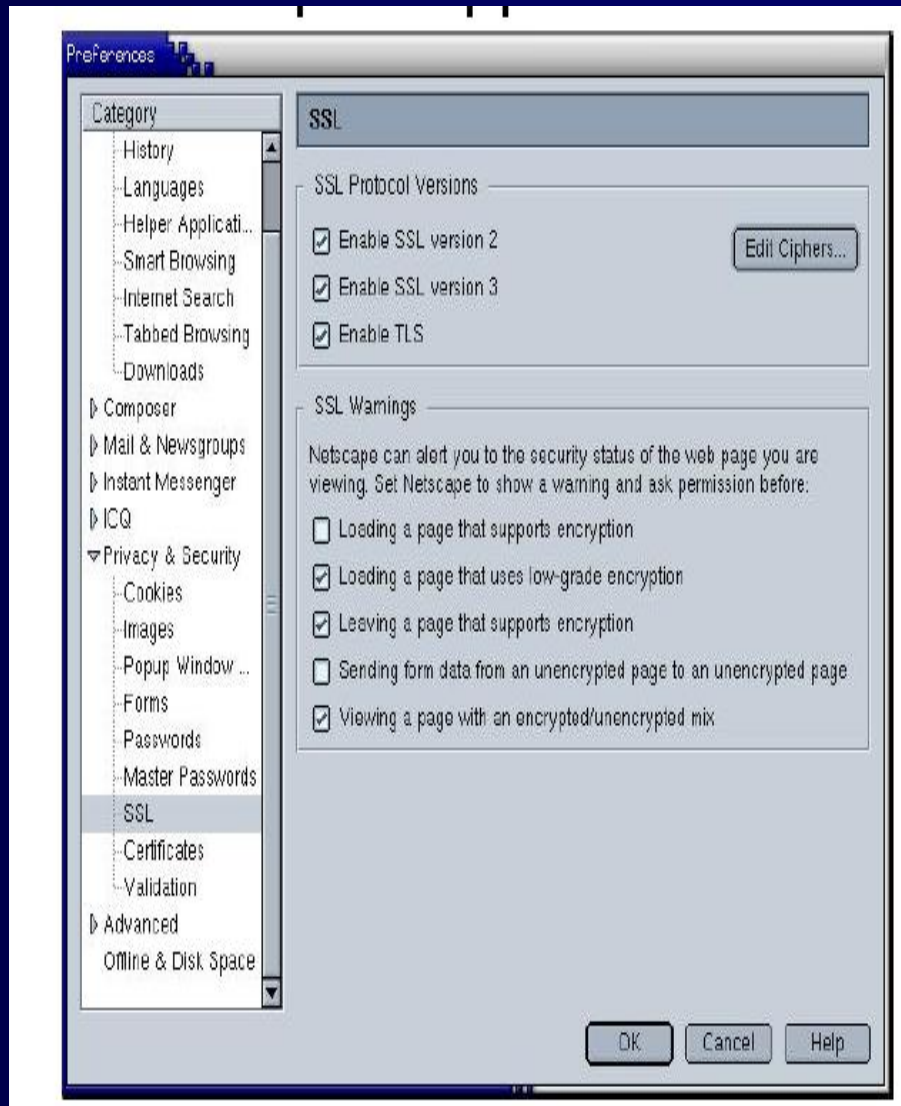
اعلان خاتمه برای پایان دادن اتصال



اگر اتصالی با مبادله دوطرفه پیام Closure Alert خاتمه نیابد، جلسه مربوطه غیر قابل از سر گیری می شود.

SSL/TLS Configuration Options
Internet Explorer 6.0& Netscape





فهرست مطالب

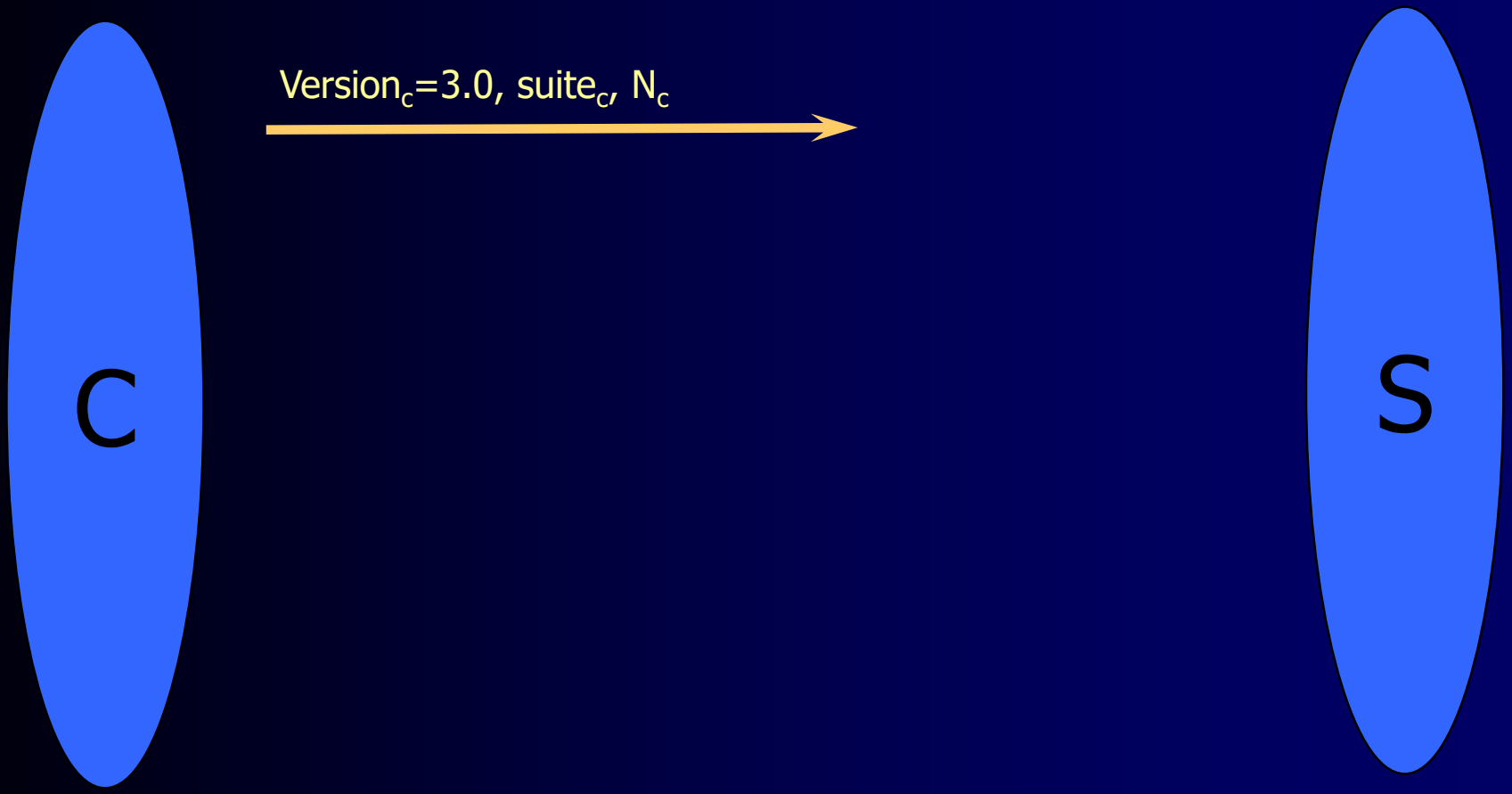
- مقدمه
- معرفی پروتکل SSL
- بررسی حملات انجام شده علیه SSL

حملات انجام شده با بهره گیری از ضعفهای پروتکل

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

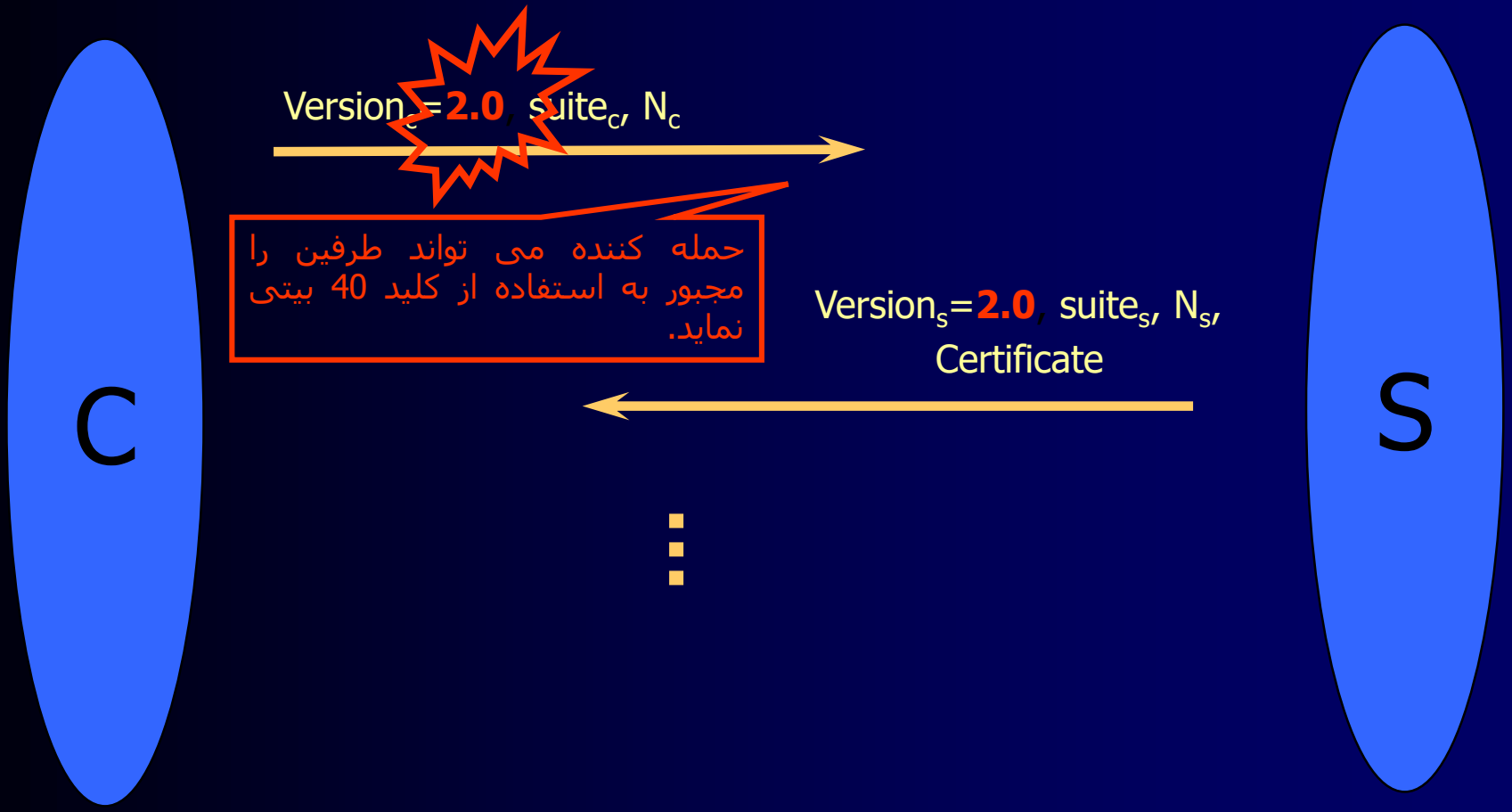
حمله تنزل نسخه

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.

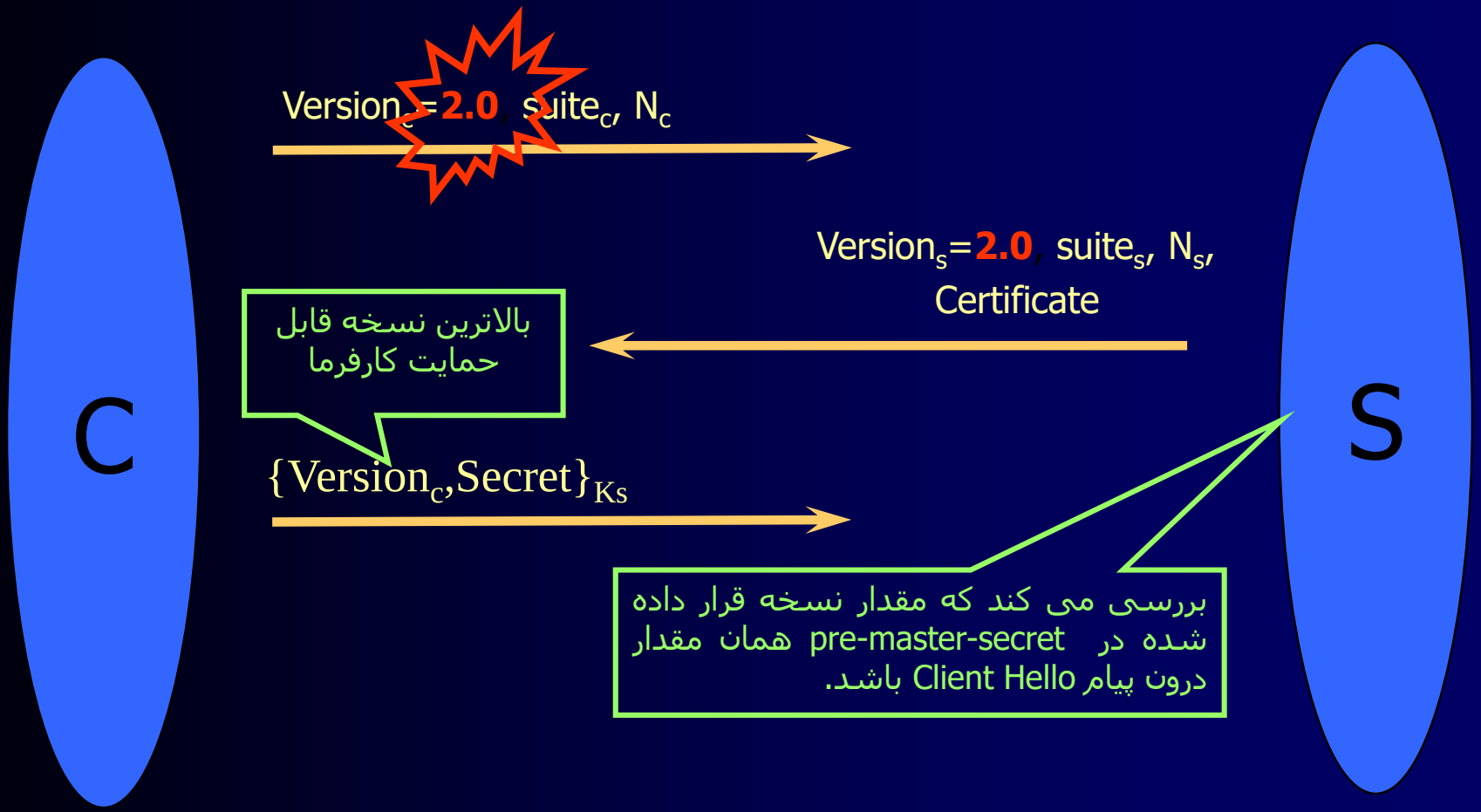


حمله تنزل نسخه

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.



آشکار کردن حمله تنزل نسخه



حمله از کاراندازی سرویس
Denial of Service (DoS)

- تعریف

- راهکارهای مقابله با حمله DoS در SSL

۱. کمک گرفتن از کارفرما در رمزگشایی RSA

۲. معمای کارفرما

حمله تحلیل ترافیک

- SSL سرآیندهای TCP/IP را رمز نمی کند و در نتیجه اطلاعات مقصد، مبدأ و سایز 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:

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

مبدأ مقصد سایز بسته IP

حمله تحلیل ترافیک (ادامه)

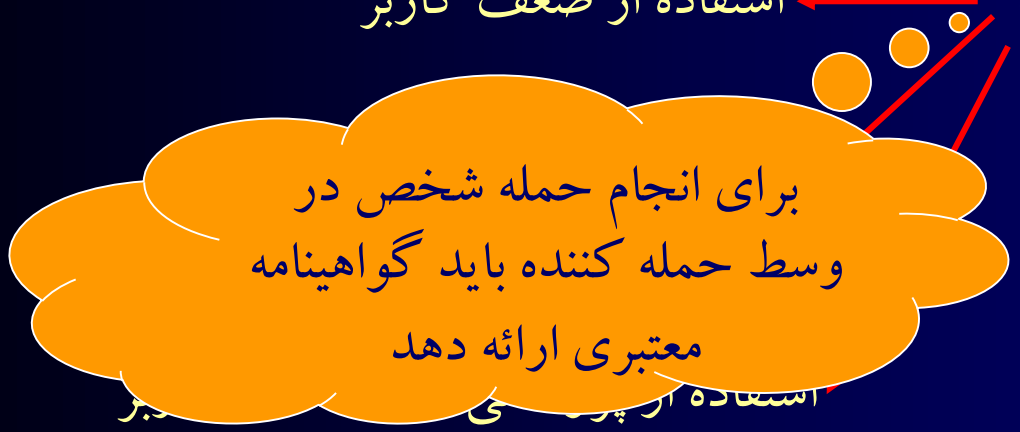
- راهکارهای مقابله

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

حملات انجام شده با بهره گیری از ضعفهای محیط اجرای SSL

- حملات شخص در وسط ← استفاده از ضعف کاربر



- حمله جستجوی کامل علیه کلیدهای ضعیف

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