**Investiga y explica cómo funciona el protocolo SSL/TLS, el cifrado SSL/TLS, la autenticación SSL/TLS, y el protocolo SSH. Contenido y extensión a criterio del alumnado.**

**Protocolo SSL/TLS**

El protocolo SSL, "Secure Socket Layer" (en español, capa de puertos seguros), es el predecesor del protocolo TLS "Transport Layer Security" (Seguridad de la Capa de Transporte, en español). Se trata de protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación. Esto garantiza que la información transmitida por dicha red no pueda ser interceptada ni modificada por elementos no autorizados, garantizando de esta forma que sólo los emisores y los receptores legítimos sean los que tengan acceso a la comunicación de manera íntegra.



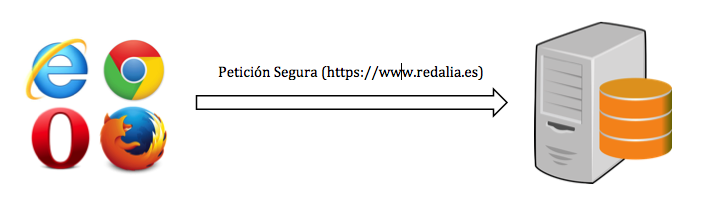
El protocolo SSL opera entre las capas de aplicación y transporte del modelo OSI y se emplea para garantizar comunicaciones seguras en internet. Su uso más común es con HTTP, formando HTTPS, que protege la transferencia de información sensible, como datos personales, contraseñas e información bancaria, entre un usuario y un sitio web.

# **¿Cómo funciona el protocolo SSL?**

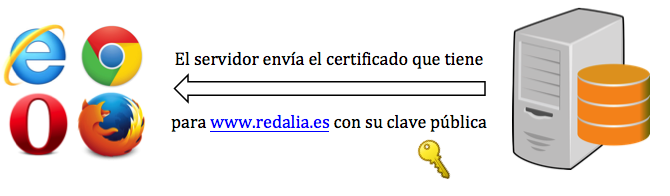
En el protocolo SSL se utiliza tanto criptografía asimétrica como simétrica. La primera se utiliza para realizar el intercambio de las claves, que a su vez serán usadas para cifrar la comunicación mediante un algoritmo simétrico.

Para que el protocolo SSL funcione en sitios web, es necesario un certificado SSL instalado en el servidor web. Cuando un cliente accede al sitio, el servidor envía el certificado junto con su clave pública. Esto permite establecer una conexión segura mediante cifrado simétrico. En combinación con HTTP, se crea HTTPS, que asegura la transferencia de datos entre el cliente y el servidor.

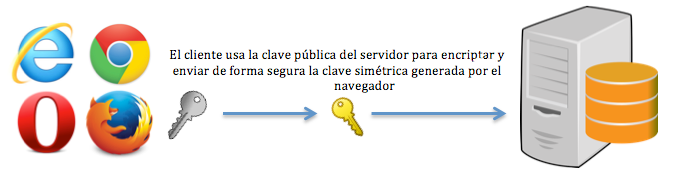
* *Un usuario realiza una petición HTTP segura a través de un navegador a un sitio web (HTTPS://www.redalia.es/)*



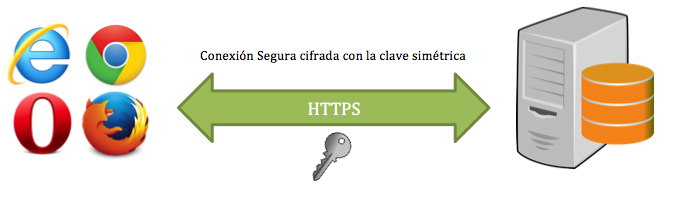
* *El servidor donde está alojado el sitio web, envía (si lo tiene) el certificado que incluye la clave pública del servidor. En caso de no tener certificado SSL, se producirá un error.*



* *El navegador comprueba que la entidad emisora del certificado o CA sea de confianza. En caso contrario, pedirá al usuario que acepte el certificado bajo su responsabilidad.*
* *Llegados a este punto, el navegador generará una clave simétrica, que será cifrada mediante la clave pública del servidor para ser enviada de manera segura al mismo.*



* *De esta forma, la comunicación ya se ha establecido de manera segura, y será cifrada en ambos sentidos mediante la clave generada en el punto anterior.*



# **Integridad de la información**

El protocolo SSL/TLS no solo asegura la confidencialidad, sino también la integridad de la información mediante un código de autenticación de mensaje (MAC). Este código, calculado con una función hash y una clave secreta compartida entre el cliente y el servidor, detecta cualquier modificación en los datos, garantizando su autenticidad.

**Cifrado SSL/TLS**

El cifrado SSL/TLS protege los datos enviados entre dos nodos, como un navegador y un servidor, evitando que sean vistos o manipulados por atacantes. Es esencial para asegurar datos confidenciales como contraseñas e información de pagos en sitios web.



# **¿Cómo funciona el cifrado SSL/TLS?**

El SSL/TLS emplea cifrados simétricos y asimétricos para proteger la confidencialidad e integridad de los datos en tránsito. El cifrado asimétrico se utiliza para establecer una sesión segura entre cliente y servidor, y el simétrico para intercambiar datos dentro de la sesión segura

Un sitio web debe tener un certificado SSL/TLS para que su servidor web/nombre de dominio utilice el cifrado SSL/TLS. Una vez instalado, el certificado permite al cliente y al servidor negociar de forma segura el nivel de cifrado en los siguientes pasos:

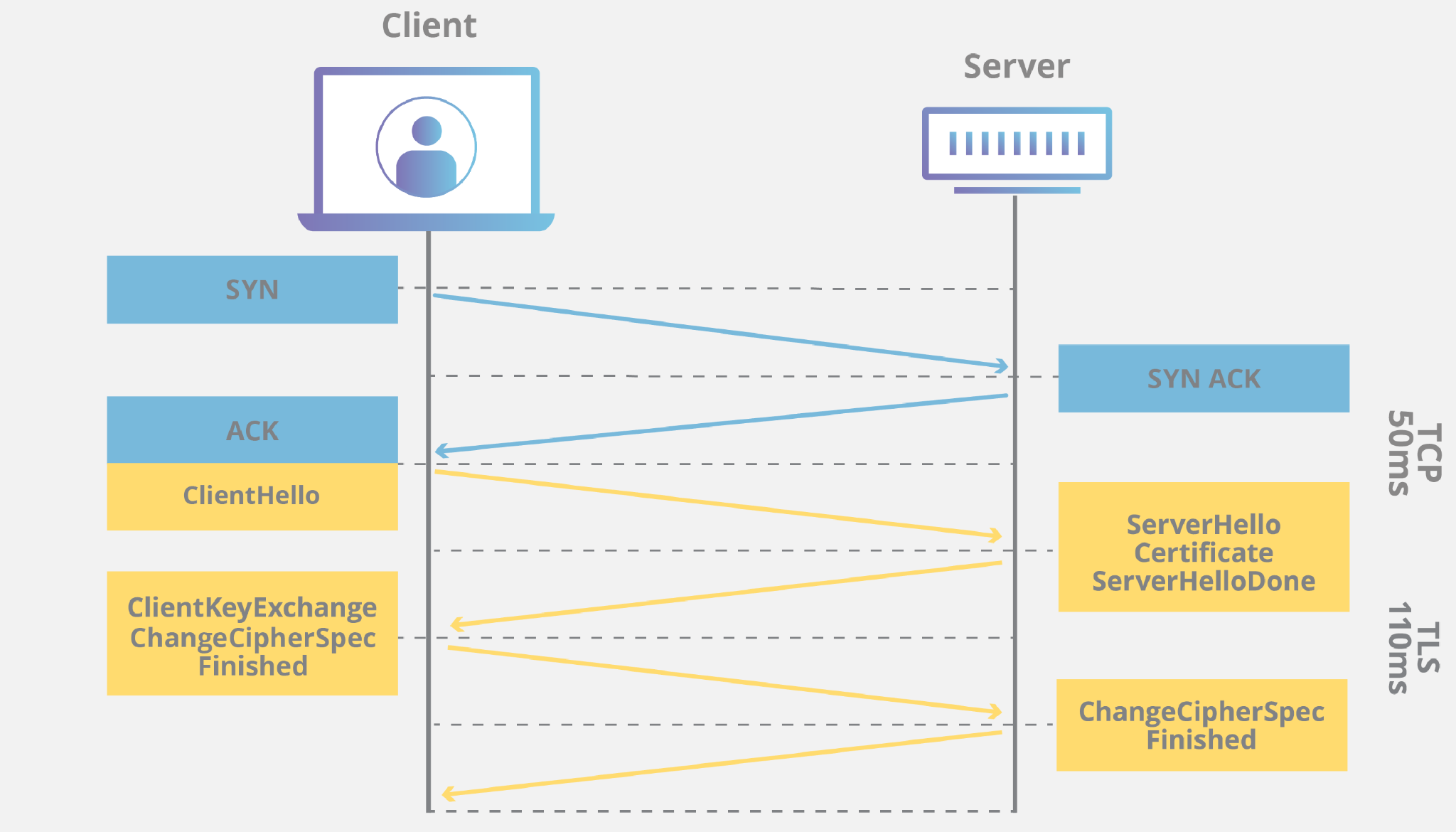
1. El cliente se pone en contacto con el servidor mediante una URL segura (HTTPS...).
2. El servidor envía al cliente su certificado y clave pública.
3. El cliente verifica esto con una autoridad de certificación raíz de confianza para comprobar que el certificado es legítimo.
4. El cliente y el servidor negocian el tipo de cifrado más potente que ambos pueden resistir.
5. El cliente cifra una clave de sesión (secreta) con la clave pública del servidor y se la devuelve al servidor.
6. El servidor descifra la comunicación del cliente con su clave privada y se establece la sesión.
7. Ahora se usa la clave de sesión (cifrado simétrico) para cifrar y descifrar los datos transmitidos entre el cliente y el servidor.

Tanto el cliente como el servidor usan ahora HTTPS (SSL/TLS + HTTP) para sus comunicaciones. Los navegadores validan esto con un icono de candado en la barra de direcciones del navegador. El HTTPS funciona sobre el puerto 443.

Cuando se sale de la página web, las claves se descartan. En la siguiente visita, se negociará un nuevo acuerdo y se generará un nuevo conjunto de claves.

**Autenticación SSL/TLS**

La autenticación SSL/TLS es un proceso que garantiza que las partes que intercambian información sean quienes afirman ser. Este proceso se basa en la utilización de certificados digitales y la criptografía de clave pública.



Cuando un usuario navega a un sitio web que usa TLS, se inicia el protocolo de enlace TLS entre el dispositivo del usuario (también conocido como dispositivo cliente) y el servidor web. Durante este protocolo, se negocian los detalles de la conexión, incluyendo la versión de TLS a utilizar y las suites de cifrado. Además, el servidor web autentica su identidad mediante el uso de un certificado TLS.

El certificado TLS contiene información importante sobre la propiedad del dominio, así como la clave pública del servidor. Esta información es necesaria para validar la identidad del servidor. El cliente verifica el certificado del servidor utilizando una autoridad de certificación (CA) confiable. Si el certificado es válido y confiable, el cliente procede a establecer una conexión segura.

En el caso del TLS mutuo (mTLS), tanto el cliente como el servidor tienen un certificado y se autentican utilizando su par de claves públicas/privadas. Este proceso adicional de autenticación proporciona una capa adicional de seguridad, ya que ambas partes deben demostrar su identidad.

**Protocolo SSH**

SSH son las siglas de Secure Shell y es un protocolo de red destinado principalmente a la conexión con máquinas a las que accedemos por línea de comandos. En otras palabras, con SSH podemos conectarnos con servidores usando la red Internet como vía para las comunicaciones. Esto es algo en lo que profundizamos en Comandos básicos para administrar servidores Linux por SSH.



SSH garantiza una comunicación segura al encriptar los datos transmitidos, protegiendo la confidencialidad del tráfico y evitando que terceros intercepten información o claves de acceso.

**El puerto predeterminado para las conexiones SSH es el 22.**

# **¿Cómo funciona SSH?**

El protocolo SSH utiliza una arquitectura cliente-servidor para establecer conexiones seguras. Aquí hay un resumen de cómo funciona:

* **Cliente SSH:** Es la aplicación que utilizas para conectarte a un servidor remoto. Puedes utilizar diferentes clientes SSH, como OpenSSH en sistemas Linux o PuTTY en Windows.
* **Servidor SSH:** Se ejecuta en el servidor remoto al que deseas acceder. Este servidor está configurado para aceptar conexiones SSH y autenticar a los usuarios..
* **Autenticación:** Cuando intentas conectarte a un servidor remoto, el cliente SSH y el servidor SSH inician un proceso de autenticación. Esto generalmente implica el uso de un nombre de usuario y una contraseña (o una clave SSH). La clave SSH es una forma más segura de autenticación y se recomienda encarecidamente su uso.

# **¿Para qué se utiliza SSH?**

Debido a su seguridad, SSH es el modo preferido para la realización de conexión con servidores que necesitamos administrar. La diferencia con respecto a otros protocolos más antiguos como Telnet es que el protocolo SSH siempre es seguro.

También se utiliza para otros objetivos como:

* **Transferencia de Archivos Segura:** Permite transferir archivos de forma segura entre sistemas locales y remotos utilizando herramientas como el comando SCP o SFTP
* **Creación de Túneles de Red:** SSH se utiliza para crear túneles de datos seguros que redirigen el tráfico de red a través de conexiones SSH, lo que puede ayudar a proteger la comunicación en redes no seguras. Se usan en sistemas como Ngrok, un software que permite a los desarrolladores exponer de manera remota los trabajos, tal como los tienen funcionando en su servidor de desarrollo local

# 

# **Técnicas de cifrado SSH**

El protocolo SSH utiliza diferentes técnicas de seguridad para proteger sus conexiones.

# **Cifrado Simétrico**

El cifrado simétrico es una técnica en la que se utiliza la misma clave tanto para cifrar como para descifrar los datos entre el cliente y el servidor, lo que garantiza su seguridad y confidencialidad.

# **Cifrado Asimétrico**

En cambio, el cifrado asimétrico utiliza dos claves: una pública y otra privada; en otras palabras, se hace uso de una clave para el cifrado y otra para el descifrado, verificando así la identidad tanto del cliente como la del servidor.

Cuando un cliente se conecta a un servidor, utiliza la clave pública del servidor para cifrar un mensaje que sólo puede descifrarse con la clave privada correspondiente.

# **Hashing**

El hashing es una técnica que se utiliza para verificar la integridad de los datos transmitidos. El algoritmo toma un conjunto de datos y genera un valor hash único, que es una representación de los datos originales.

Este valor se envía junto con los datos a través de la conexión SSH. En el extremo receptor, los datos se vuelven a calcular y se genera un nuevo valor hash.

* Si coincide con el recibido, se confirma que los datos no se han modificado.
* Si no coincide, los datos podrían haber sido alterados y se considera una posible amenaza de seguridad.