# Introducción al protocolo HTTPS

Despliegue de Aplicaciones Web

José Juan Sánchez Hernández

Curso 2024/2025

# Índice


1 ¿Qué es el protocolo HTTPS? 1

2 ¿Qué puerto utiliza HTTPS? 2

3 ¿Qué es la criptografía simétrica? 3

4 ¿Qué es la criptografía asimétrica? 4

5 Cómo funciona HTTPS 5

6 ¿Qué es una Autoridad de Certificación (CA)? 7

7 Cuántos tipos de certificados SSL/TLS existen 8

8 ¿Qué sucede cuando escribimos una URL en un navegador web? 9

9 Referencias 12

10 Licencia 13

# Índice de figuras

# Índice de cuadros

# 1 ¿Qué es el protocolo HTTPS?

HTTPS (*Hypertext Transfer Protocol Secure*) es la versión segura del protocolo HTTP, es un protocolo de la capa de aplicación y es el principal protocolo utilizado en la Web (*World Wide Web*).

Este protocolo utiliza el protocolo criptográfico TLS (*Transport Layer Security*) anteriormente conocido como SSL (*Secure Sockets Layer*). El protocolo TLS se encarga de cifrar los datos transmitidos entre el cliente y el servidor garantizando: (1) la encriptación de los datos, (2) la autenticidad del cliente y servidor, (3) la integridad de los datos, es decir, que no han sido modificados.

# 2 ¿Qué puerto utiliza HTTPS?

El protocolo HTTPS utiliza el puerto `443`, mientras que el protocolo HTTP utiliza el puerto `80`.

# 3 ¿Qué es la criptografía simétrica?

La **criptografía simétrica**, utiliza **una única clave tanto para cifrar como para descifrar**. Las dos partes que se comunican deben tener la misma clave y mantenerla en secreto.

La ventaja de este método es que es rápido y eficiente, pero puede tener problemas de seguridad a la hora de distribuir la clave de forma segura.

Ejemplo: AES (Advanced Encryption Standard).

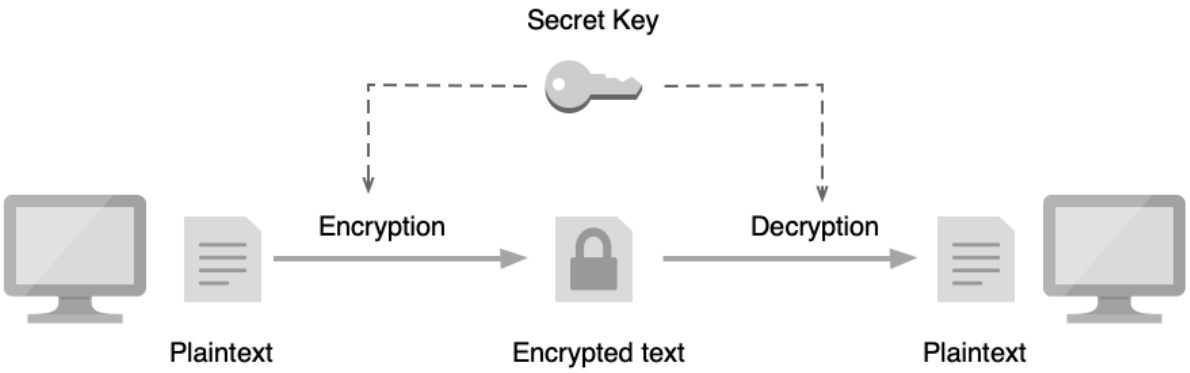


*Imagen 1: Imagen de elaboración propia (CC BY-NC-SA).*

Se recomienda la lectura del artículo sobre criptografía simétrica de Wikipedia.

# 4 ¿Qué es la criptografía asimétrica?

La **criptografía asimétrica**, utiliza dos claves distintas: **una clave pública (para cifrar)** y **una clave privada (para descifrar)**. La clave pública se puede compartir sin ningún problema, pero la clave privada se tiene que mantener en secreto.

Este método es más seguro, aunque tiene el inconveniente que es más lento que la criptografía simétrica.

Ejemplo: RSA (Rivest-Shamir-Adleman).

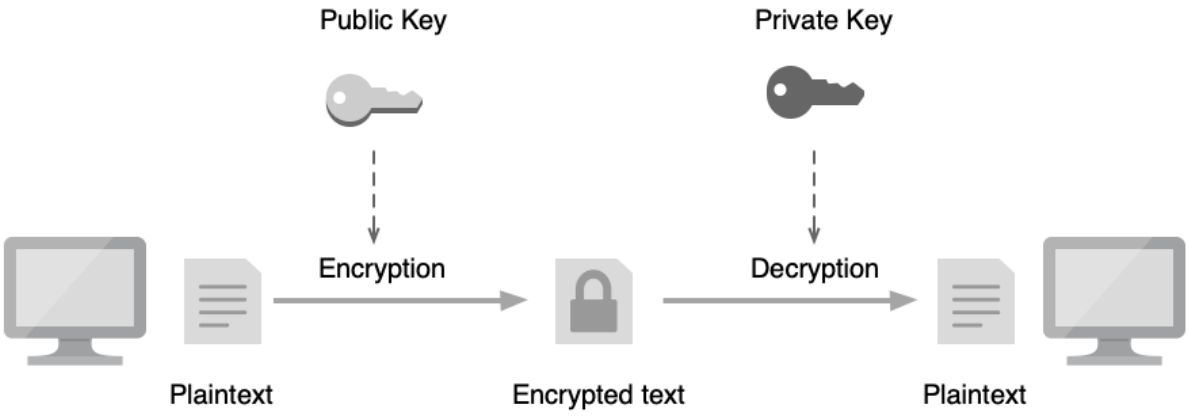


*Imagen 2: Imagen de elaboración propia (CC BY-NC-SA).*

Se recomienda la lectura del artículo sobre criptografía asimétrica de Wikipedia.

# 5 Cómo funciona HTTPS

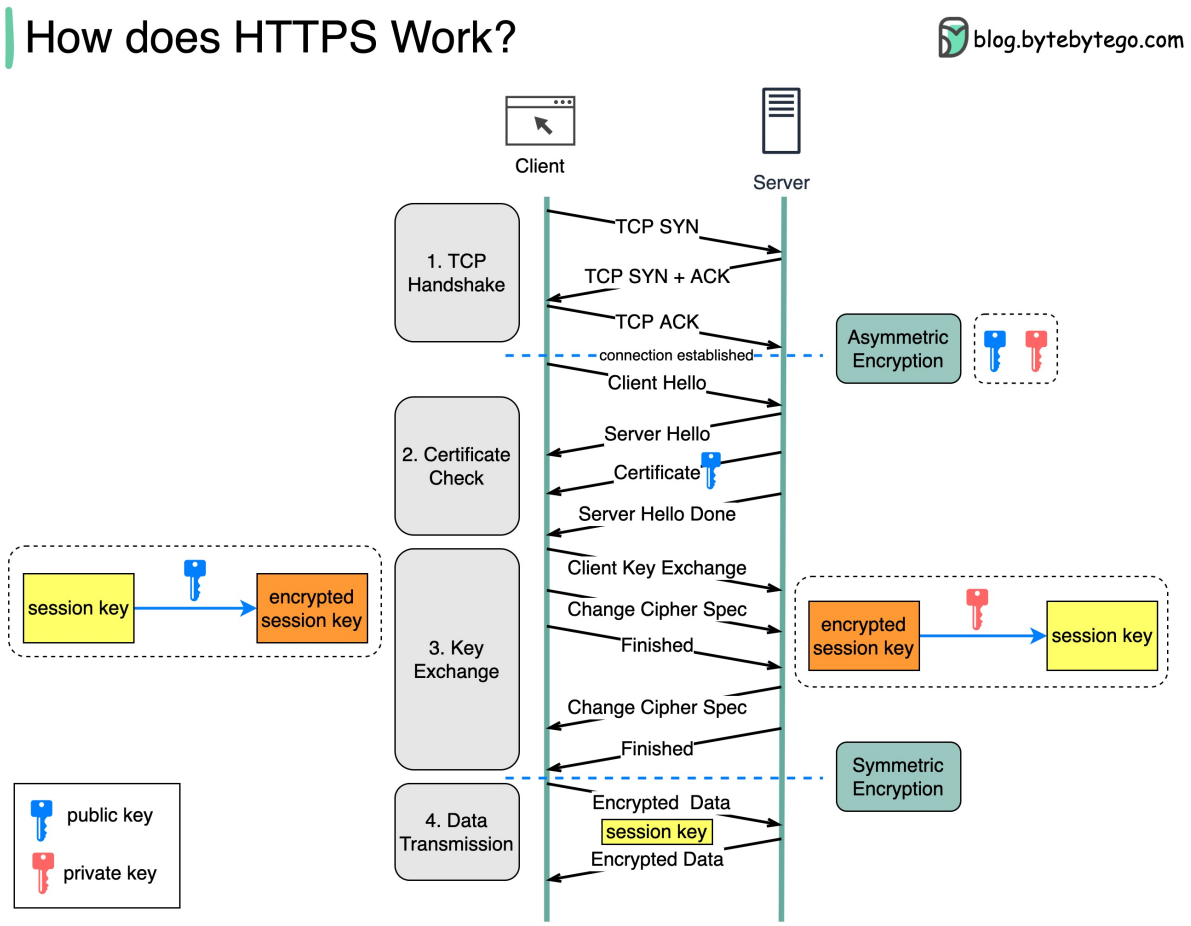


*Imagen 3: Imagen obtenida de ByteByteGo.com.*

A continuación, se detallan los pasos que se realizan en una comunicación HTTPS:

**Paso 1. TCP 3-Way Handshake**

1. En primer lugar, el cliente y el servidor establecen una conexión TCP, utilizando el procedimiento conocido como TCP 3-Way Handshake.

**Paso 2. Validación del Certificado SSL/TLS**

2. El cliente envía al servidor un mensaje `ClientHello` que contiene:
   - La última versión de TLS que el cliente puede utilizar.

- Lista de algoritmos de cifrado preferidas por el cliente.

3. El servidor responde con un mensaje `ServerHello` que contiene:
   - La versión de TLS seleccionada.
   - Los algoritmos de cifrado seleccionados.

4. El servidor envía su certificado SSL/TLS al cliente. El certificado contiene su clave pública, el nombre del dominio, fecha de expiración, etc. y tiene que estar firmado por una autoridad de certificación (CA) de confianza. El cliente verifica el certificado.

**Paso 3. Intercambio de la clave de sesión**

5. Una vez que el cliente ha verificado el certificado SSL/TLS, genera un clave de sesión y la cifra con la clave pública del servidor.

6. El cliente genera una clave de sesión secreta (*session key*) y la cifra con la clave pública certificado del servidor. Luego, envía la clave cifrada al servidor.

7. El servidor descifra la clave de sesión secreta con su clave privada y obtiene la clave de sesión secreta (*session key*).

**Paso 4. Intercambio de datos**

8. A partir de este punto, la comunicación entre el cliente y el servidor se cifra utilizando la clave de sesión compartida (encriptación simétrica).

# 6 ¿Qué es una Autoridad de Certificación (CA)?

Una Autoridad de Certificación (CA) es una entidad de confianza encargada de emitir y revocar certificados digitales, para garantizar la seguridad en las comunicaciones realizadas mediante el protocolo TLS utilizado en HTTPS.

Se recomienda la lectura del artículo sobre Autoridad de Certificación de Wikipedia.

# 7 Cuántos tipos de certificados SSL/TLS existen

Existen tres tipos de certificados SSL/TLS:

1. **Certificados de dominio único**: Sólo se pueden utilizar para un único dominio. Por ejemplo, podríamos tener un certificado para `iescelia.org`.
2. **Certificados *wilcard***: Son válidos para un dominio y todos sus subdominios. Por ejemplo, podríamos tener un certificado para `iescelia.org` y para todos los subdominios de `*.iescelia.org`, como `openstack.iescelia.org`, etc.
3. **Certificados multidominio (SAN/UCC):** En este caso, un único certificado es válido para varios dominios diferentes. Las sigas SAN hacen referencia a *Subject Alternative Name* y UCC a *Unified Communications Certificate*. Por ejemplo, podríamos tener el mismo certificado para `iescelia.org` y para `otrodominio.org`.

# 8 ¿Qué sucede cuando escribimos una URL en un navegador web?

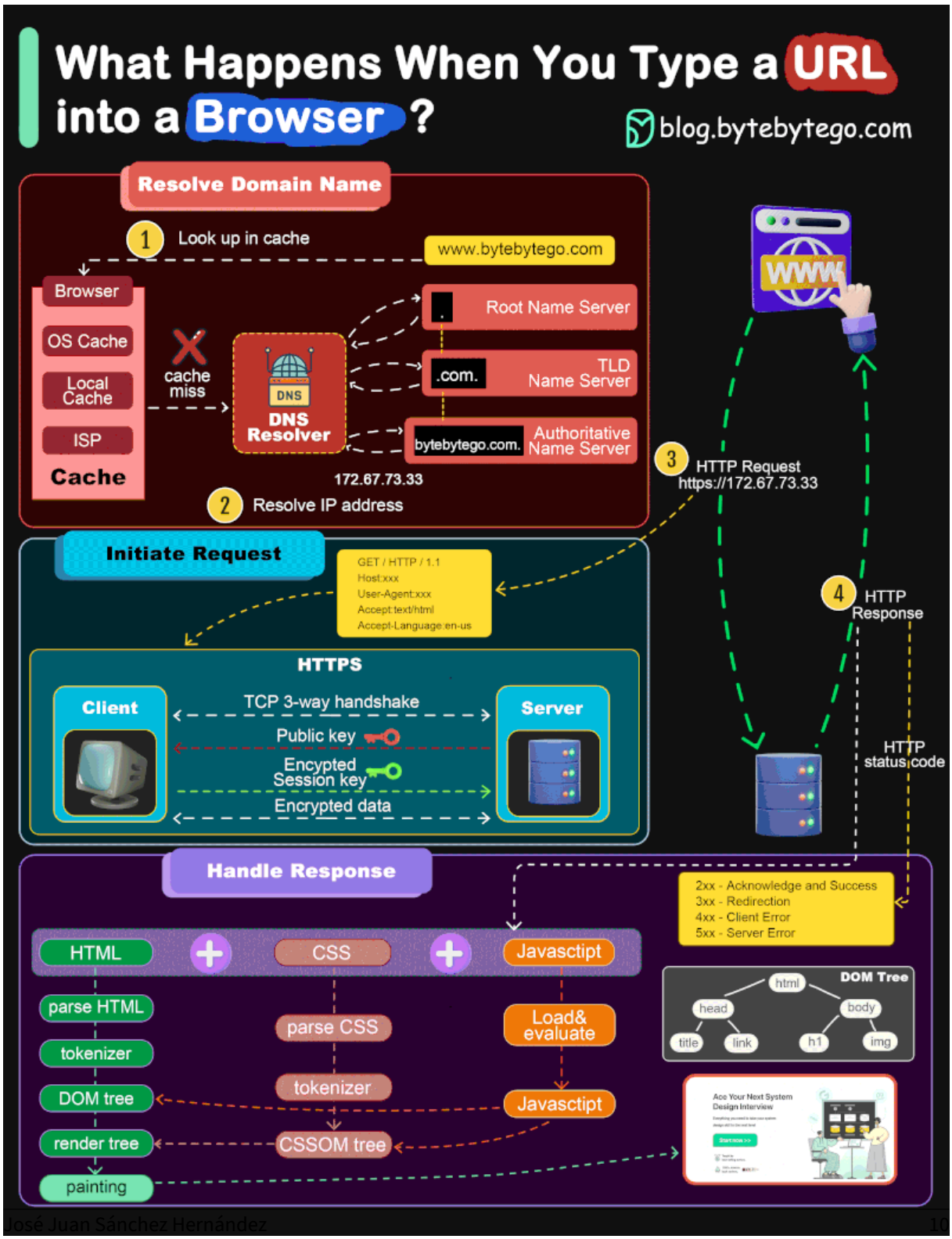

*Imagen 4: Imagen obtenida de ByteByteGo.com.*

# 9 Referencias


- HTTP - Protocolo de transferencia de hipertexto. Wikipedia
- HTTPS - Protocolo seguro de transferencia de hipertexto. Wikipedia
- Seguridad en la capa de transporte. Wikipedia
- Certificado Digital. Wikipedia
- Certificado de clave pública. Wikipedia
- Criptografía asimétrica. Wikipedia
- Criptografía simétrica. Wikipedia
- Autoridad de Certificación. Wikipedia
- System Design 101. ByteByteGo
- Infraestructura de clave pública. Wikipedia
- ¿Qué es HTTPS?. Documentación oficial de Cloudflare.

# 10 Licencia

Esta página forma parte del curso Despliegue de Aplicaciones Web de José Juan Sánchez Hernández y su contenido se distribuye bajo una licencia Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional.