PRÁCTICA 4: CERTIFICADOS Y FIRMA DIGITAL

1. Selección de un servidor web público e investigar cuáles son los puertos a nivel de transporte que utiliza para brindar el servicio web ¿Qué sentido tiene?

Como bien nos sugiere el enunciado, vamos a usar el servidor web de la UVA para realizar las pruebas correspondientes.

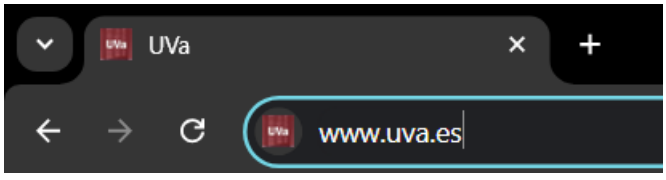
Vamos primero a comprobar gracias a nmap, que puertos están abiertos en el servidor web de la uva y, por lo tanto, podemos inferir que los servicios correspondientes a estos puertos están activos:

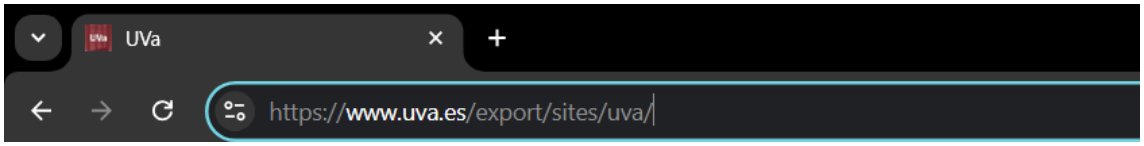
```
sirdidi@LAPTOP-KN7F97L0:/mnt/c/Users/danig$ sudo nmap -sS www.uva.es -p 80,443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 13:14 CET
Nmap scan report for www.uva.es (157.88.25.8)
Host is up (0.039s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
```

Podemos ver, que en el servidor de la UVA, tanto el puerto 80 como el 443 están abiertos, por lo que el servicio http y https está *running*

La pregunta que nos hacemos ahora es: si https es mucho más seguro que http, ya que ofrece comunicación cifrada, ¿Por qué el servidor de la UVA también acepta http si ya tiene el servicio https?

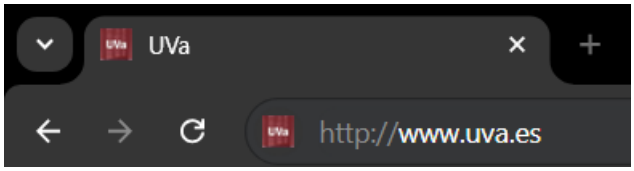
Para responder a la pregunta, vamos a realizar una prueba directamente desde el navegador. Si ponemos la URL directamente, sin especificar http o https podemos ver lo siguiente:

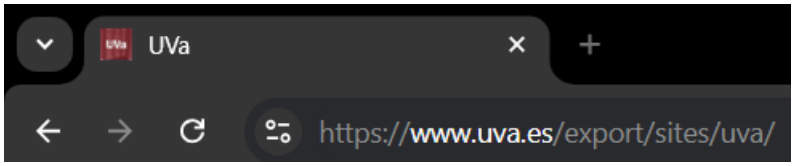




Lo que ha ocurrido se denomina como “URL resolution”. En este proceso, el navegador es capaz de autodetectar el protocolo que se usa para determinada página web y aplicarlo directamente a la URL. En este caso, al ser https más seguro, obtenemos este prefijo para la URL.

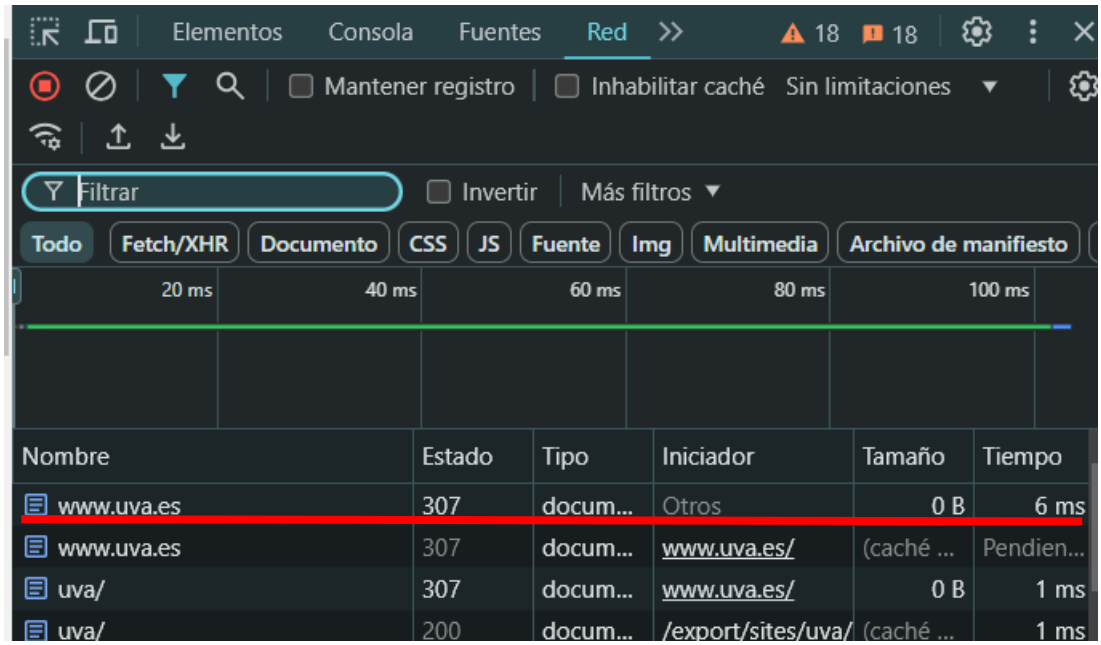
Vamos a ver que es lo que ocurre en el caso de que queramos forzar el http://:





Como podemos ver, el servidor Web nos redirecciona directamente al servicio seguro. Vamos a inspeccionar la página al realizar la búsqueda para observar el proceso de lo acontecido.

En el apartado de red dentro de la pestaña de inspeccionar, podemos ver información relacionada con las solicitudes y respuestas de red que se hacen cuando cargas o interactúas con una página web.



En nuestro caso, podemos observar una solicitud de estado 307. Esto significa lo siguiente: ENLACE

¿Qué es la redirección temporal HTTP 307?

HTTP 307 es un código de estado que puedes encontrar mientras navegas por Internet. **Es un mensaje que tu navegador recibe de un servidor web, indicando que la página o el contenido que estás buscando se ha movido temporalmente a una nueva ubicación.** Esto significa que tu navegador necesita enviar otra solicitud a la nueva ubicación para obtener el contenido que estabas buscando.

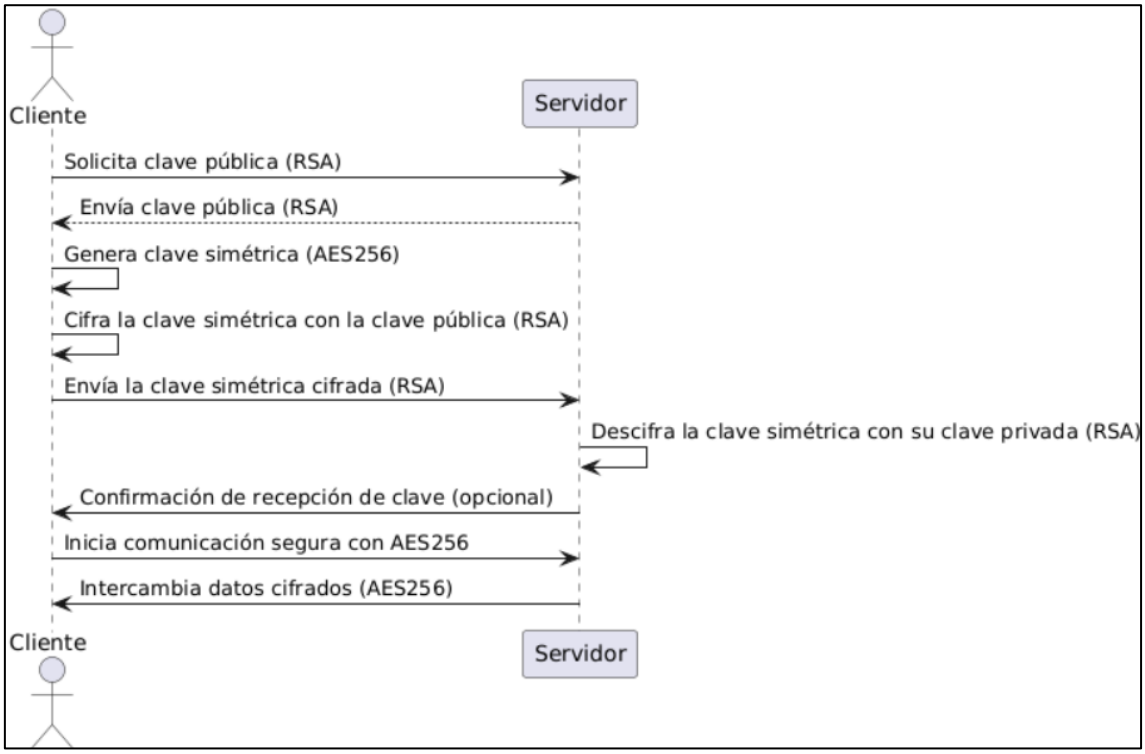
Podemos ver que nuestra teoría era cierta y que cuando el usuario accede a http://www.uva.es, el propio navegador redirecciona a este a https permitiendo así una conexión más segura.

2. DIAGRAMA DE SECUENCIA DE EL USO DE CRIPTOGRAFÍA DE CLAVE PÚBLICA O PRIVADA

Antes de el diagrama de secuencia, vamos a explicar porque es útil la criptografía de clave pública/privada en la comunicación:

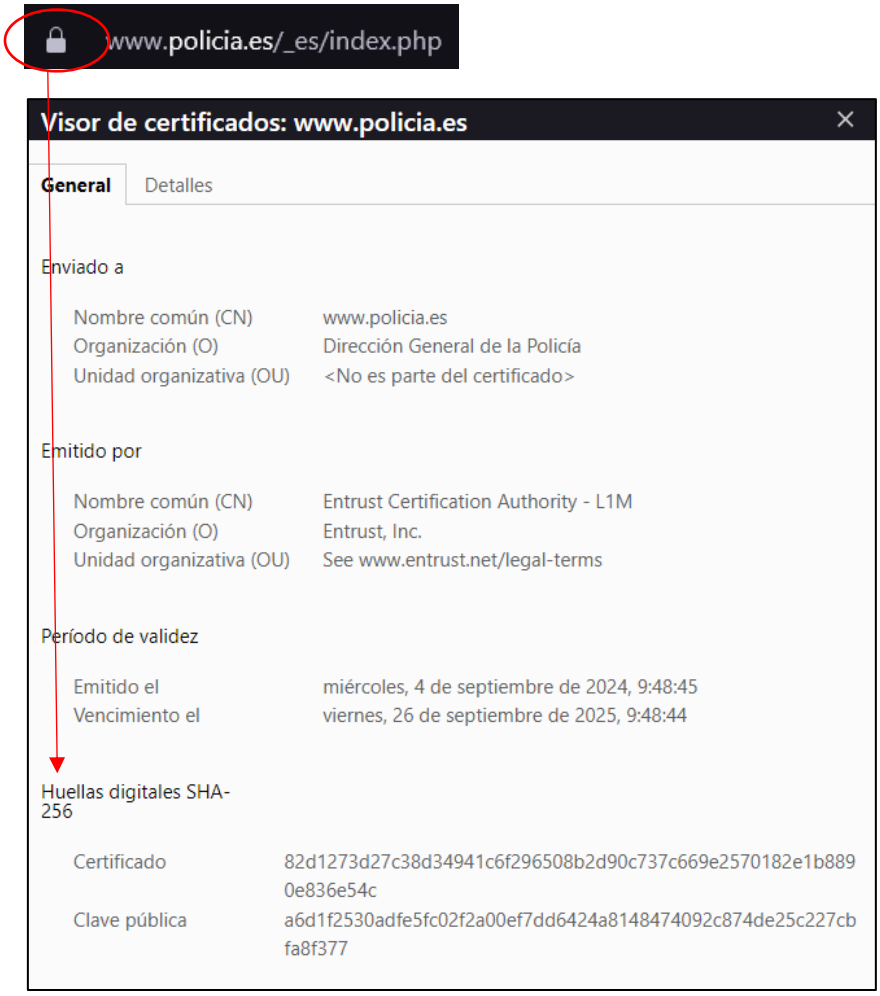
- **Autenticidad y Verificación de Identidad:** La criptografía de clave pública/privada permite a las partes comprobar la identidad de quien envía un mensaje.
- **Confidencialidad:** Nadie más, incluso si intercepta el mensaje, puede leer su contenido.
- **Integridad de los Datos:** La criptografía de clave pública/privada puede garantizar que los datos no se han alterado durante la transmisión mediante el uso de funciones *hash* y firmas digitales

Mostramos aquí el diagrama de secuencia asociado a el procedimiento del enunciado:

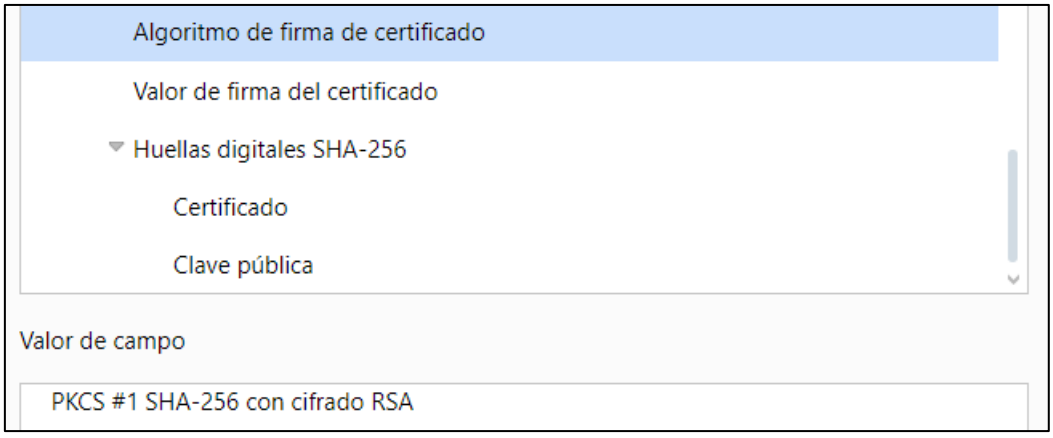


Comprobemos ahora si este ejemplo se aplica en la vida real a servidores web.

Ejemplo Servidor Web Policía Nacional:



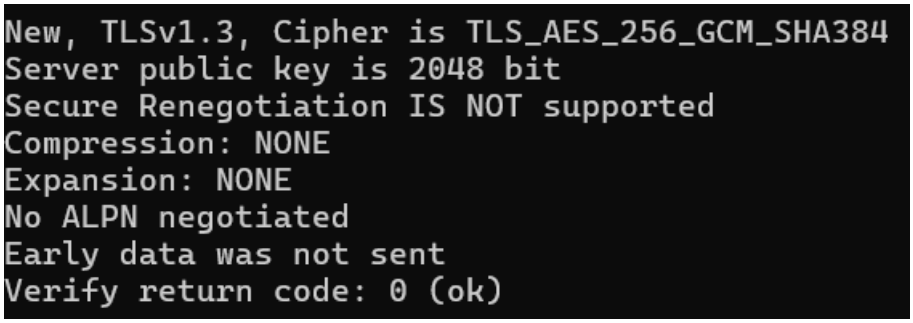
Si entramos dentro de la pestaña detalles, podemos observar el algoritmo de forma más específica:



Directamente desde el navegador, no podemos ver el algoritmo de clave privada que se está usando por el servidor. Para esto, vamos a usar el siguiente comando:

openssl s_client -connect www.policia.es:443

Tras obtener la salida, interpretamos la información para descubrir que algoritmo de clave privada es el que se está usando:



Podemos ver en la primera línea, que el cifrado seleccionado sería TLS_AES_256_GCM_SHA384. Esto significa:

- AES256 - cifrado
- GCM – modo autenticado
- SHA384 – función de hash

Tras esto ya hemos obtenido todas las partes que constituyen el diagrama de secuencia entre un cliente y el servidor web de la policía nacional.

NOTA: No se ha realizado más contenido de la práctica, ya que el profesor indicó en la clase de presentación de la práctica que hasta el punto 2 era lo necesario.