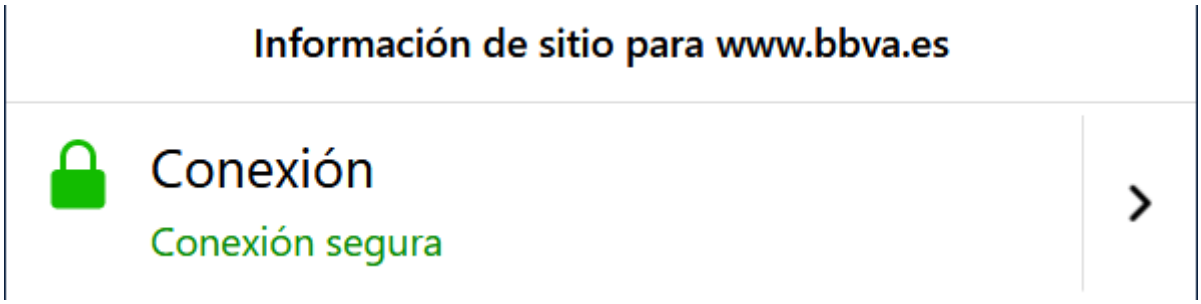
Hoja02_Apache_05

El objetivo de esta práctica es analizar las características de un certificado en una web real.

Para esta práctica vamos a utilizar el navegador Mozilla Firefox. Inícialo y conéctate a https://www.bbva.es. Observa que se trata del protocolo HTTPS. Una vez cargado, a la izquierda de la URL verás un candado y un símbolo de información como en la imagen:

Al hacer clic en el símbolo de información aparecerá un desplegable que informa de que la conexión es segura. A continuación, hacer clic en la flecha de la derecha.



Haz clic en "Más información" para ver información al respecto del certificado.

1. ¿Qué empresa ha verificado el certificado?
2. ¿Qué algoritmo de clave privada se ha utilizado para cifrar la página?

Haz clic en "Ver Certificado" y a continuación en la pestaña "Detalles".

3. ¿Cuál es el algoritmo que se ha usado para el cifrado de la firma?
4. ¿Cuáles son las fechas de validez del certificado?
5. ¿Qué sistema criptográfico se ha usado para generar la clave pública y de cuantos bits es?

A continuación, vamos a ver los certificados guardados en Firefox. Para ello, hacemos clic en el menú de Firefox, Opciones, Privacidad & Seguridad, y en la parte baja de la página en "Ver Certificados". Buscar en la lista de certificados el expedido en la página de BBVA.

6. Busca una web que utilice https pero cuyo certificado no esté verificado.