Clave simétrica:

Se usa la misma clave para cifrar la información que para descifrarla. Esto es poco seguro porque tenemos que transmitir la clave con la que tenemos que cifrar

Clave pública o asimétrica:

La clave para cifrar (clave pública), es distinta que la usada para descifrar, esta clave solo la conoce el usuario que debe conocer los mensajes.

Este usuario hace pública la clave para cifrar, por lo tanto cualquiera la puede tener, pero solo puede descifrarlo el destinatario que tiene la clave privada para descifrar.

Este último mecanismo permite crear lo que se viene llamando **infraestructuras de claves públicas X509** (norma ITU), donde:

* Se definen Autoridades Certificadoras (ACs) que garantizan la autenticidad de un sujeto, emiten un certificado **Certificado X509** que lleva una clave pública de un usuario determinado que permiten comprobar su autenticidad.
* La configuración de la clave pública necesita de 3 ficheros:
  + **Clave**: la clave privada para cifrar y firmar, debe estar muy guardada por el sujeto o por la AC. Es un archivo “*.pem*” que es el formato de las claves (quiz-2015-key.pem).
  + **CSR**: (Certificate signing request) Solicitud a AC de un certificado X509 temporal firmado. (quiz-2015-csr.pem).
  + **Certificado X509**: Certificado con clave pública emitido por AC o “auto-firmado”. (quiz-2015-cert.pem). Sirve para cifrar mensajes enviado al emisor y autenticar los mensajes firmados por el emisor que es el proceso inverso
* En el proyecto usaremos un **certificado “auto-firmado”** de 1 año de validez. Los navegadores mostraran un mensaje de error como que el servidor no está autenticado ni validado por ninguna autoridad.

HTTPS: Conexiones seguras

* HTTPS introduce el nivel SSL de cifrado entre HTTP y Sockets
  + Este nivel cifra la información que intercambian cliente y servidor, HTTP se activa automáticamente si el URL lo indica: **https:\\**

Las conexiones seguras utilizan un encriptación entre el protocolo HTTP y el TCP, el cual establece el circuito virtual.

Para que la solicitud http no vaya en claro se introduce entre HTTP y TCP el protocolo SSL (Secure Sockets layers) en el cual se cifran las solicitudes y las respuestas para que lo que llegue sea un texto ilegible y solo lo puedan entender el servidor y el cliente.

La clave simétrica aleatoria creada por el cliente solo es útil para esa sesión, y se crea porque es más eficiente, y la clave asimétrica pública se usa para enviarse esta clave simétrica, y solo el servidor puede leer la clave simétrica porque tiene la clave adecuada para leer los mensajes.

A continuación se envían los mensajes http cifrados con la clave simétrica.

OpenSSL

Herramienta criptográfica muy potente para crear las claves, implementa SSL y TSL además de crear claves y otras herramientas criptográficas