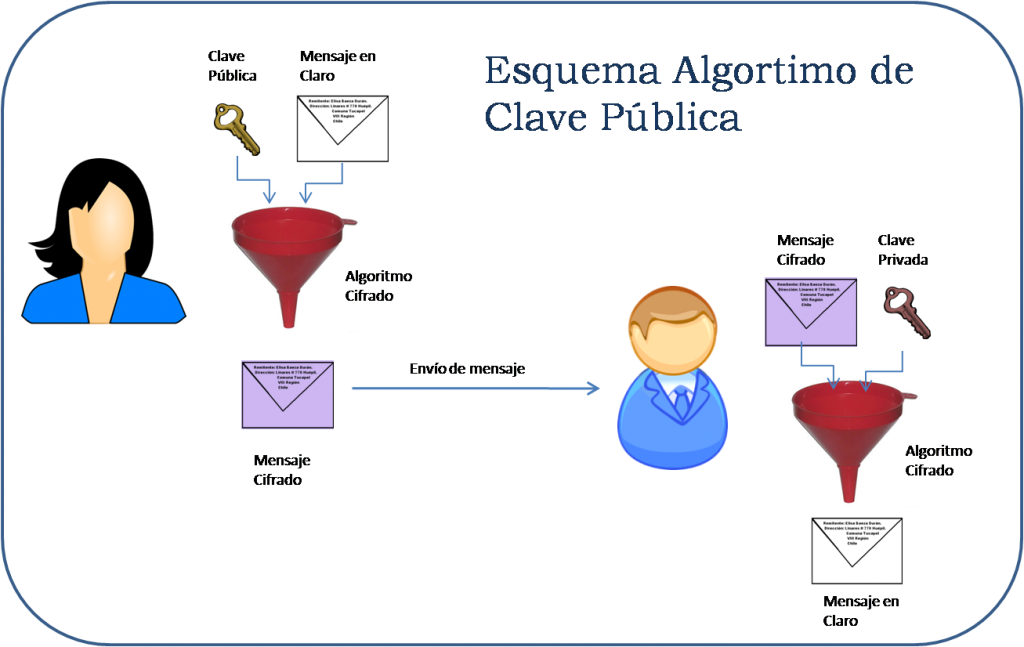
**Certificados SSL: Conceptos Básicos**

* Protocolos Seguros. TLS (Transport Layer Security) y SSL (Secure Socket Layer) son dos protocolos criptográficos que proporcionan comunicaciones seguras por red. Ejemplos de protocolos de red que usan estos protocolos son HTTPS, SSH o LDAPS. El uso de estos protocolos aseguran:
  + La confidencialidad de la comunicación. Nadie salvo los interlocutores puede saber el contenido del mensaje.
  + La integridad de los datos. Asegura que los datos no han sido modificados.
  + Autenticación del interlocutor: Permite identificar al interlocutor de forma inequívoca, basándose en la relación de confianza con un tercero.

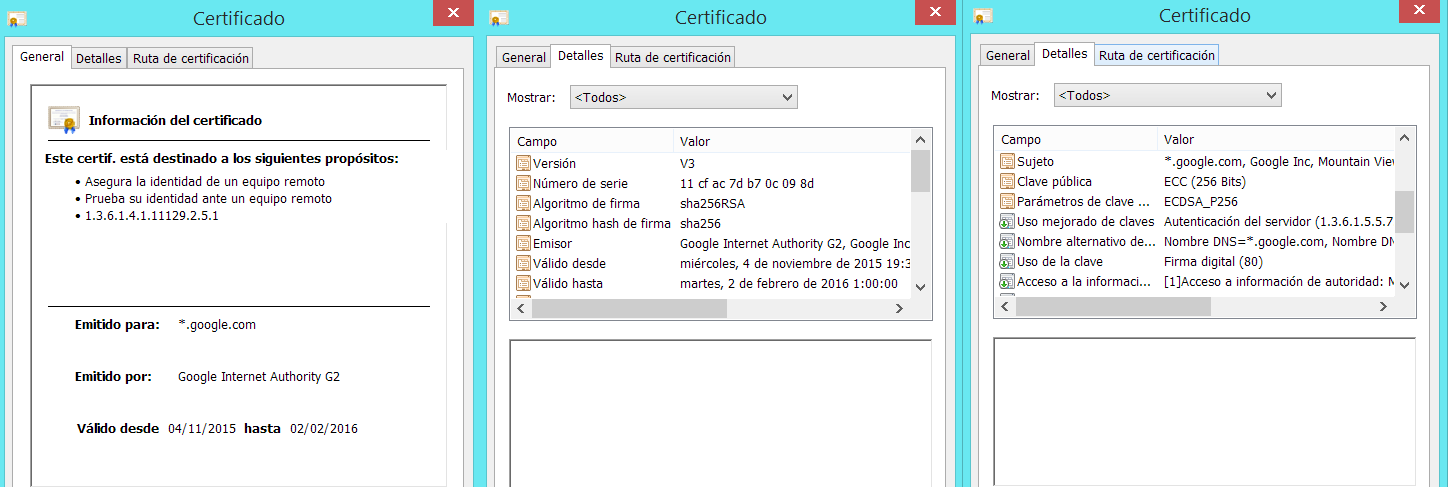
TLS es una evolución de SSL, pero es lo suficientemente grande como para hacer que no sean compatibles y se identifiquen como distintos, aunque las bases teóricas son las mismas. En este protocolo entran en juego diferentes algortimos, que los interlocutores deben acordar en la primera fase de establecimiento de conexión o negociación. Estos algoritmos son (los enumero a modo de que simplemente os suenen):  
– Algoritimos de clave asimétrica: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.  
– Algoritmos de clave simétrica: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard).  
– Funciones HASH: MD5 o de la familia SHA.

* Criptografía asimétrica o de clave pública. Se trata de un método criptográfico que utiliza un par de claves (llamadas pública y privada) que pueden utilizarse tanto para cifrar y descrifrar un mensaje. La clave privada la mantiene guardada y en secreto uno de los interlocutores mientras que la pública se envía a cualquier interlocutor que desee comunicarse con el primero. El funcionamiento es sencillo:
  1. “A” cifra un mensaje con la clave pública de B
  2. El mensaje llega cifrado a B y usa su clave privada para descifrar el mensaje.
  3. B puede estar seguro que ese mensaje no ha sido modificado porque sólo la clave privada puede descifrar el mensaje y sólo la tiene B. Esto garantiza la Confidencialidad.
  4. B redacta una respuesta y la cifra con su clave privada y la envía a A.
  5. A usa la clave pública de B para descifrarlo. A está seguro que el mensaje es de B, porque sólo B puede cifrar ese mensaje. Esto garantiza la identificación y autenticación del emisor. Esto es lo que se conoce como Firma Digital.



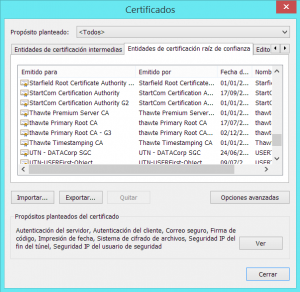
La fortaleza de este sistema es que el método criptográfico (una serie de funciones matemáticas) es público y conocido. En las claves radica la confidencialidad, sobretodo en la privada. Además, las claves son creadas con algotimos que utilizan las propiedades de los números primos para asegurar que la probabilidad de generar 2 parejas de claves iguales es mínima.

* Certificado. Es un fichero con información del emisor y su clave pública validado por una tercera parte de confianza, llamada Certificate Authority (CA). Podemos ver un certificado de cualquier sitio web, si se pulsa sobre el icono del candado que muestran la mayoría de navegadores. Por ejemplo, este es el de www.google.es



En él puede verse la información que comento: para quien se ha emitido el certificado, quién lo ha emitido (que es la Certificate Authority) y el tiempo de validez. Hay más información en el certificado que puede verse pulsando sobre detalles. Además de estos datos, se encuentra la clave pública del servidor web que usará el navegador para cifrar la clave simétrica de comunicación (ver protocolo https más abajo).

Toda esta información del certificado está validada por una CA (la CA ha firmado con su clave privada el certificado).

* Certificate Authority (CA). Es una tercera parte en la que nosotros (nuestro navegador) confía. Las CA son empresas públicas y privadas reguladas según legislaciones internacionales las cuales establecen que son de confianza. Ejemplos de CA son [Verisign](https://www.symantec.com/es/es/ssl-certificates/) (ahora Symantec) y [Thawte](https://www.thawte.com/) a nivel global o la [FNMT](http://www.cert.fnmt.es/catalogo-de-servicios/certificados-electronicos/certificado-servidor) y la Cámara de Comercio a través de [Camerfirma](http://www.camerfirma.com/) a nivel nacional.  
    
  La forma en la que la CA valida el certificado que nos muestra un servidor web, es que lo firma con su clave privada. Por tanto, nuestro navegador tiene que tener la clave pública de la CA para poder ver el certificado. Todos los sistemas informáticos: sistemas operativos y aplicaciones, capaces de comunicarse con protocolos seguros, llevan preinstalados las claves públicas de la mayoría de CAs internacionales y principales nacionales. A estos certificados se les llama certificados raíz o ROOT. En Internet Explorer, pueden verse desde el menú Opciones de Internet -> Contenido -> Certificados -> Entidades de certificación raíz de confianza.

En caso de que el navegador no tenga la clave pública de la CA preinstalada, es cuando nos saldrá el error típico de navegador que nos dice que el sitio al que vamos a acceder es peligroso o no es de confianza (en función del navegador, el mensaje es diferente). En este caso, nos ofrece siempre una opción de continuar. Lo que pasa cuando continuamos, es que el navegador se añade una excepción de seguridad para que las futuras veces que visitemos el sitio, no aparezca el error y entremos (aún cuando no confiemos).

* Protocolo HTTPS. Es el protocolo HTTP seguro, que utiliza SSL/TLS para cifrar la comunicación entre el navegador y el servidor web. Hasta aquí hemos explicado los cifrados de clave pública, pero éstos no se usan para cifrar/descifrar todo el intercambio de mensajes en una comunicación HTTPS, si no que se usa sólo en la primera fase. Realmente se utiliza un cifrado basado en un algortimo de clave simétrica, que es aquel en el que ambos interlocutores tienen la misma clave para cifrar y descifrar. Esta clave debe compartirse entre los interlocutores de forma segura, para garantizar la confidencialidad de la comunicación. Aquí entra en juego el algoritmo asimétrico y los certificados. El establecimiento de una conexión HTTPS (handshake) se compone de 3 fases: Hello, Certificate Exchange, Key Exchange. Este es el detalle:

1. Hola: El navegador envía una solicitud de conexión segura. En ella, envía una propuesta de algoritmos de cifrado, los protocolos y versión máxima que soporta de ellos. El servidor al recibir la propuesta, selecciona de los algortimos de cifrado y protocolo que soporta el cliente y le contesta con un SERVER Hola en el que le envía esta información. En este paso, se han negociado los protocolos de cifrado a utilizar, entre otras cosas.
2. CERTIFICATE EXCHANGE: El servidor envía al cliente su identificación, mediante la presentación de su certificado SSL. Hemos visto que información relevante lleva el certificado: datos de identidad (sitio, país, empresa, caducidad…), la clave pública del servidor web y todo viene firmado (cifrado) con la clave privada de una CA. Nuestro navegador confirmará que confía en la CA, viendo si tiene el certificado raíz de ésta. Si confía, extraerá la información y obtendrá la clave pública del servidor.
3. KEY EXCHANGE: En este último paso, el navegador generará una clave simétrica privada y la cifrará con la clave pública del servidor (que ha obtenido del certificado) y se la enviará al servidor. El servidor usando su clave privada, descifrará la clave simétrica. En este punto, ambos interlocutores tienen la clave simétrica privada y pueden empezar a intercambiarse información. Ha concluido la negociación, se ha establecido la conexión HTTPS y a partir de este momento, todos los datos intercambiados se cifrarán con la clave simétrica.

El motivo de usar clave simétrica, básicamente es porque es un proceso mucho más rápido y menos costoso a nivel de recursos que cifrar/descifrar con los algoritmos de clave pública/privada.

Hasta aquí los conceptos básicos para entender de forma general, el funcionamiento de los certificados SSL.