El empleo es de todos

Mintrabajo

GC-F-004v.03

Seguridad Informática:
Criptografía.

SENA



Temáticas a tratar:

- Teoría Criptográfica
- Sistemas de Cifrado
- Certificados Digitales
- SSL / TLS

Presentación:

INSTRUCTOR:
Rodrigo Ebrat Carr

Correo:
rebratc@sena.edu.co



Introducción.

Entre el Antiguo Egipto e Internet, los criptogramas (los mensajes cifrados) han protagonizado buena parte de los grandes episodios históricos y un sinfín de anécdotas. Existen mensajes cifrados entre los artículos del Kamasutra, se usaron por gobernantes y militares ya en los primeros estados como Egipto, Babilonia y Roma.

Hoy en día, con las nuevas tecnologías el uso de la criptografía se ha extendido más allá de su tradicional esfera estatal o política, y es vital también para la actividad diaria de las empresas y ciudadanos particulares.

Introducción.

A través de la criptografía la información puede ser protegida contra el acceso no autorizado, su interceptación, su modificación y la inserción de información extra.

También puede ser usada para prevenir el acceso y uso no autorizado de los recursos de una red o sistema informático y para prevenir a los usuarios la denegación de los servicios a los que sí están permitidos.

Modernamente, la criptografía es la metodología para proveer la seguridad de las redes telemáticas, incluyendo la identificación de entidades y autenticación, el control de acceso a los recursos, la confidencialidad de los mensajes transmitidos, la integridad de los mensajes y su no repudio.



Teoría Criptográfica

Conceptos y Generalidades.

Criptografía.

Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

La criptografía es parte de un campo de estudios que trata las comunicaciones secretas, usadas, entre otras finalidades, para:

- ✓ Autentificar la identidad de usuarios.
- ✓ Autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias.
- ✓ Proteger la integridad de transferencias electrónicas de fondos.

Criptoanálisis.

Técnica consistente en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la clave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada para su codificación.

Es el arte y la ciencia de transgredir las claves de acceso, es decir la que se encarga de descifrar los mensajes. Cuando se diseña un sistema para cifrar información, hay que tener muy presente su posible criptoanálisis, ya que en caso contrario podríamos llevarnos desagradables sorpresas.

Esteganografía.

Consiste en ocultar – empleo de canales subliminales – en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no). Este método ha cobrado bastante importancia últimamente debido a que permite burlar diferentes sistemas de control.

Para ello, se utilizan dos elementos, el mensaje (la información que queremos ocultar) y el camuflaje o tapadera (el elemento que hará de tapadera), una función estego (algún tipo de técnica para que el elemento oculto pase desapercibido dentro del camuflaje) y quizás algún tipo de clave necesaria para descifrarla.

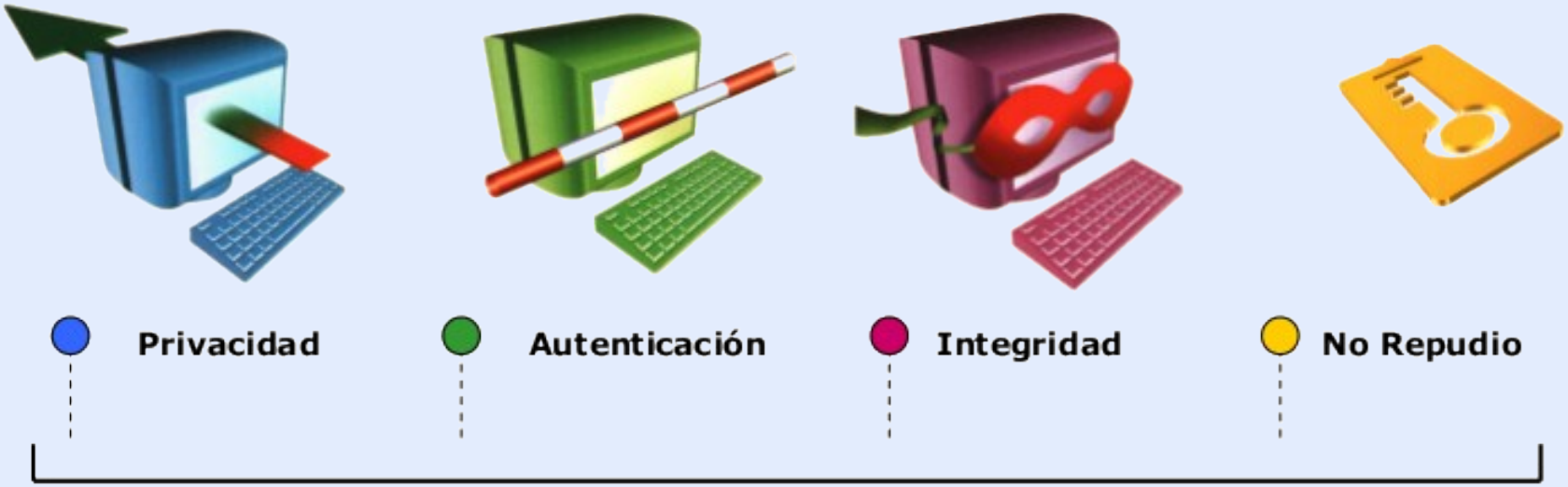
Seguridad Computacional.

Un sistema se considera computacionalmente seguro si cumple alguna de las condiciones siguientes:

- ✓ El coste del criptoanálisis excede el valor de la información obtenida.
- ✓ El tiempo necesario para el criptoanálisis excede el tiempo de vida útil de la información.

La seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

Los principios de la seguridad computacional:



- Autenticación.
- Confidencialidad (o Privacidad).
- Disponibilidad.
- Integridad.
- No Repudio.

Autenticación:



- Permite verificar la identidad.
- Una firma digital es un mecanismo que asegura la identidad del firmante del mensaje y por tanto su autenticidad.

Confidencialidad:



- Permite proteger la información de personal no autorizado.
- El cifrado es un mecanismo que aporta esta característica a un mensaje.

Integridad:



- Permite comprobar que no se ha producido manipulación alguna en el mensaje original.
- La integridad de un mensaje se obtiene adjuntando al mismo otro conjunto de datos de comprobación de la integridad.
- Una función hash que genere una huella digital asociada a un mensaje es un mecanismo que aporta esta característica.

Disponibilidad:



- Es clave que el informático garantice que se pueda acceder tanto a estos datos como a procesos en sí en cualquier momento de forma rápida y sencilla y solucionar posibles problemas cuando puedan surgir.

No repudio:



- Permite probar la participación de las partes en una comunicación. Existirán por tanto dos posibilidades:
- No repudio en origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío.
- No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Ataques contra un sistema de comunicaciones.

- **Interrupción**: algún elemento del sistema es puesto fuera de servicio.
- **Interceptación**: alguien no autorizado accede a cierta información o a cualquier elemento de la red.
- **Modificación**: alguien no autorizado, tras haber accedido a cualquier información de la red, altera su contenido.
- **Fabricación**: alguien no autorizado, falsificando su identidad, inserta cierta información en el sistema.

Los ataques por interrupción, modificación y fabricación se consideran “activos”; la interceptación como “pasivo”.



Sistemas de Cifrado

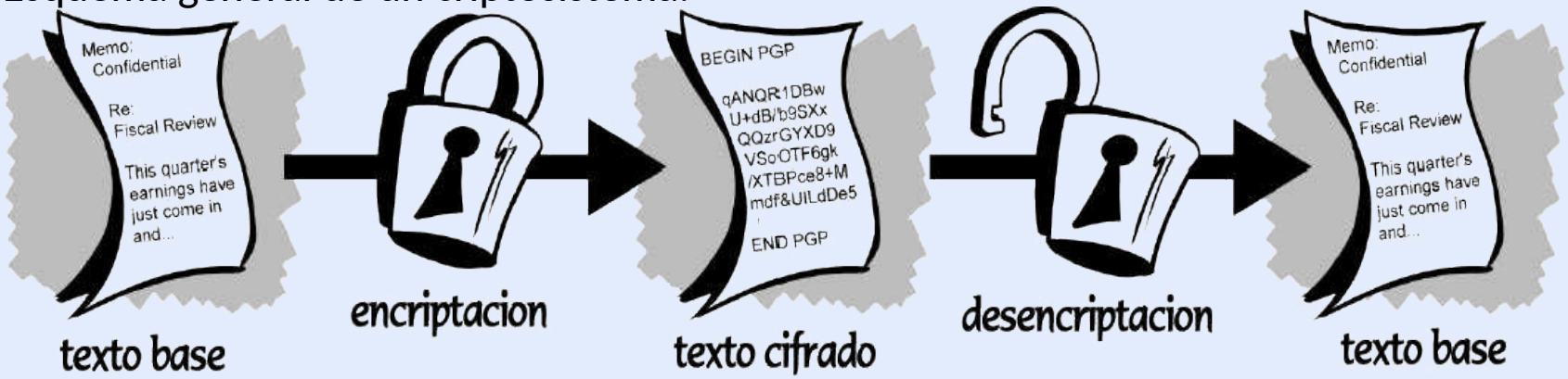
Cifrado, Criptosistemas y Firma Digital.

Cifrado o Cifra.

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica o secreto, no será posible descifrarlo o recuperarlo.

Las claves de cifrado y de descifrado pueden ser iguales (*criptografía simétrica*), distintas (*criptografía asimétrica*) o de ambos tipos (*criptografía híbrida*).

Esquema general de un criptosistema:



Esquema de un criptosistema usando llaves.



Clasificación de Criptosistemas.

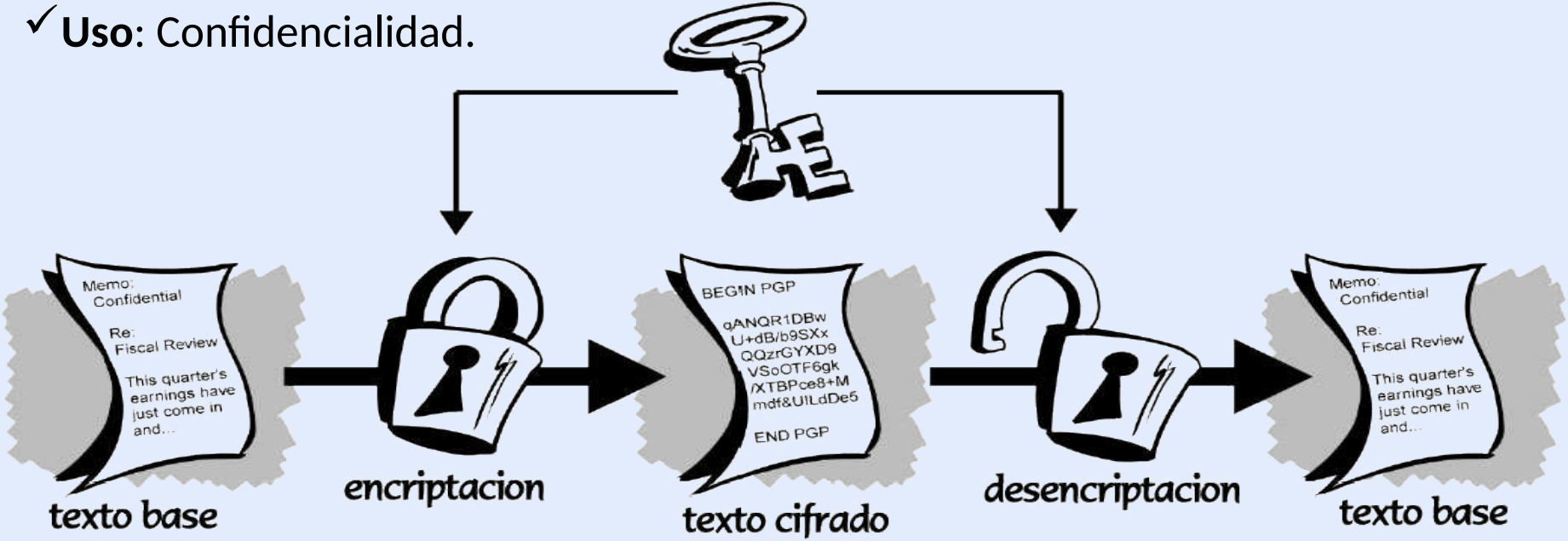
- ✓ **Criptografía Clásica:**
- ✘ Sustitución.
- ✘ Transposición.

- ✓ **Criptografía Moderna:**
- ✘ Clave Única (Simétricos: DES, IDEA, RC5, ...)
- ✘ Claves Pública y Privada (Asimétricos: RSA, DSS, DSA, ...)
- ✘ Firma Digital (MD5, SHA-1, ...)

Cifrado con Llave Única.

La criptografía de llave única ***utiliza la misma llave tanto para codificar como para decodificar mensajes***. A pesar de que este método es bastante eficiente en relación al tiempo de procesamiento, o sea, el tiempo que gasta para codificar y decodificar mensajes, tiene como principal desventaja la necesidad de utilización de un medio seguro para que la llave pueda ser compartida entre personas o entidades que deseen intercambiar información criptografiada.

- ✓Sistema de criptografía más antiguo.
- ✓Con la misma clave se cifra y se descifra.
- ✓Clave única (secreta) compartida por emisor y receptor.
- ✓**La seguridad**, mantener la clave en secreto.
- ✓**Problema**: distribución de claves.
- ✓**Uso**: Confidencialidad.

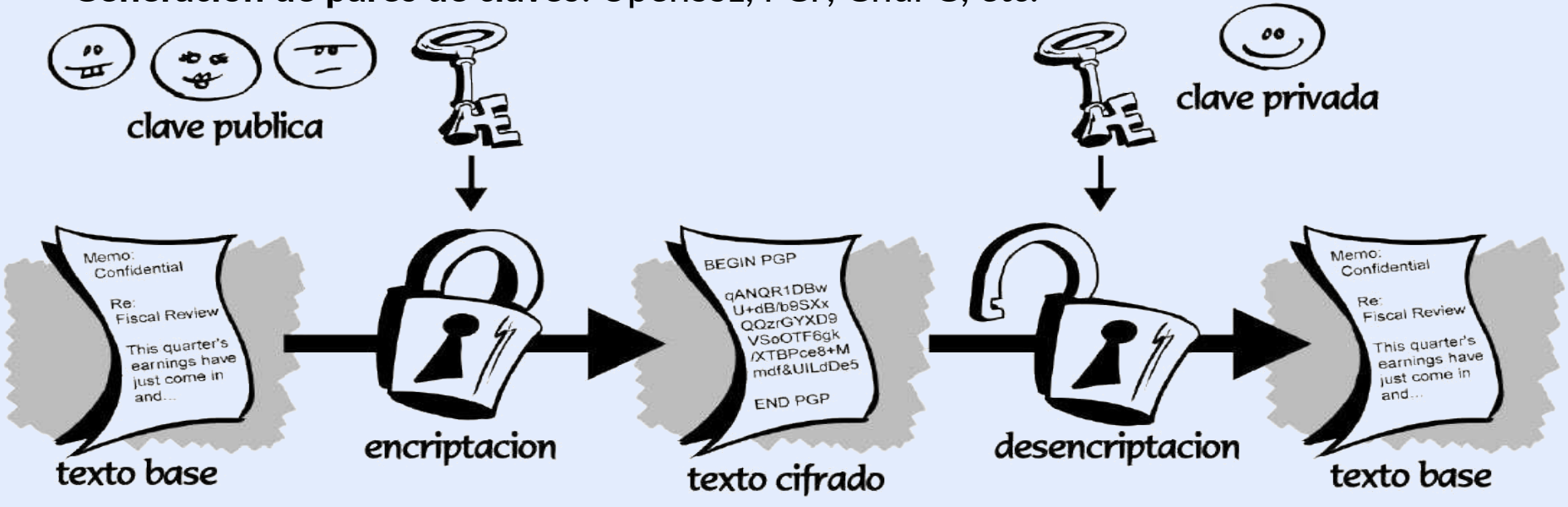


Cifrado con Llaves Privada y Pública.

La criptografía de llaves pública y privada utiliza dos llaves distintas, ***una para codificar y otra para decodificar mensajes***. Con este método cada persona o entidad mantiene dos llaves: una pública, que puede ser divulgada libremente, y otra privada, que debe ser mantenida en secreto por su dueño.

Los mensajes codificados con la llave pública solo pueden ser decodificados con la llave privada correspondiente.

- ✓ Utiliza claves distintas para encriptar/desencriptar, una pública y otra privada.
- ✓ **La seguridad**: dificultad computacional de descubrir la clave privada a partir de la pública.
- ✓ Soluciona el problema de distribución de claves.
- ✓ **Usos**: Confidencialidad, Autenticación, Firma Digital.
- ✓ **Generación de pares de claves**: OpenSSL, PGP, GnuPG, etc.



Algoritmos Usados.

- ✓ **RSA** (*Rivest*, *Shamir*, *Adleman*):
- ✘ Permite cifrado y descifrado.
- ✘ Longitudes de clave variables (512 bits).
- ✘ Usos:
  - Cifrado (Confidencialidad y Autenticación).
  - Firma digital.
  - Usado en el SSH (Secure Shell Client).

- ✓ **Diffie-Hellman**:
- ✘ Distribución de claves simétricas.
- ✘ Primer algoritmo asimétrico.
- ✘ Muy extendido en Internet (VPN, SSL, etc.).

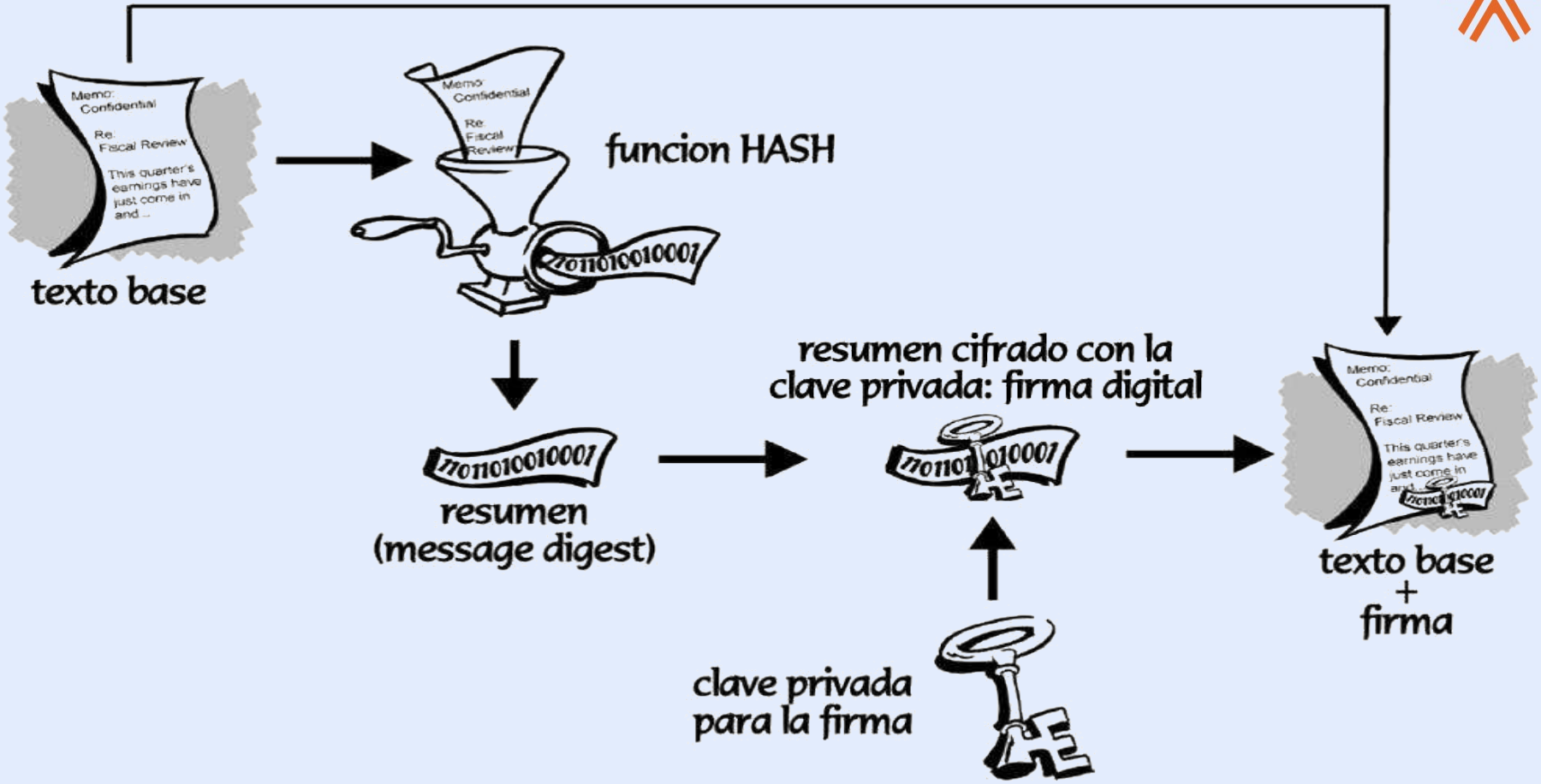
- ✓ **DSS** (*Digital Signature Standard*):
- ✘ Firma Digital.
- ✘ Adoptado como estándar por el NIST en 1994.

Firma Digital.

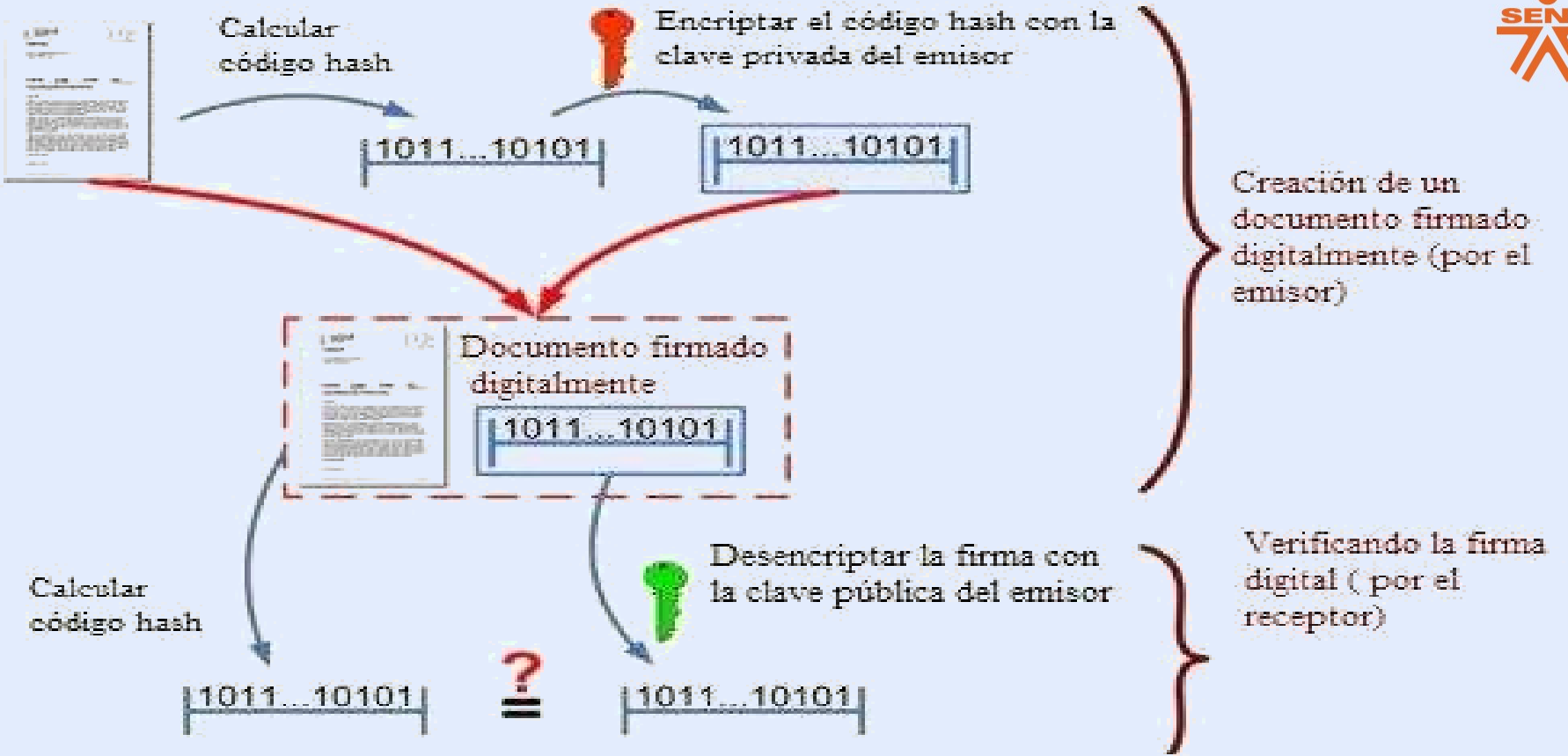
La firma digital consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda verificar si el remitente es quien dice ser e identificar cualquier mensaje que pueda haber sido modificado. Lo anterior permite...

- ✓ Que el receptor puede acreditar la identidad del emisor.
- ✓ Que el transmisor no pueda repudiar después el contenido del mensaje.
- ✓ Que el receptor no pueda suplantar al emisor y falsificar el mensaje.

Como se firma digitalmente...



Creando y verificando una firma digital...



Si el código hash calculado no concuerda con el resultado de la firma digital desencriptada, o el documento fue modificado después de hacer la firma, o la firma no fue generada por la clave privada del emisor del documento

Firma Digital.

- El proceso de firma digital lo realiza un programa (por ejemplo PGP, un cliente de correo, etc.) que aplica un algoritmo de resumen (MD5 o SHA) sobre el texto a firmar, obteniendo el extracto.

- Éste, cuya longitud suele oscilar entre 128 y 160 bits, se somete a continuación al cifrado (RSA o DSS) mediante la clave privada del autor.



Certificados Digitales.

Certificado Digital, Autoridad de Certificación y SSL/TLS.

¿Cómo asegurar que una clave pública es confiable?

Autoridades Certificadoras.

Las **Autoridades de Certificación** o **Certificadoras**, a veces abreviadas como ***AC*** o ***CA*** (por las siglas del término inglés *Certification Authority*), son entidades de confianza que emiten certificados digitales.

En efecto, las autoridades de certificación son uno de los pilares de la confianza en el mundo digital, razón por la que tienen una gran responsabilidad.

Para garantizar que las dos partes que realizan una transacción son quienes dicen ser, las AC hacen uso de una **Infraestructura de Clave Pública** (o ***PKI***, por el inglés *Public Key Infrastructure*), lo que en el ámbito de la criptografía se refiere a una combinación de elementos operativos, hardware, software, políticas y procedimientos de seguridad y auditoría que hace posible llevar a cabo operaciones criptográficas (como ***cifrado*** o ***firma digital***) de forma segura.

Autoridades Certificadoras.

Una autoridad de certificación puede ser pública o privada. Entre los proveedores más prestigiosos del ámbito privado encontramos empresas como **Thawte** o **GeoTrust**, del grupo *Symantec*, o **DigiCert**, que ofrecen certificados de seguridad **SSL** con cifrado de hasta 2048 bits.

- *Fábrica Nacional de Moneda y Timbre: www.fnmt.es*
- *VeriSign: www.verisign.com*
- *EUnetInternational: www.eunet.com*
- *Microsoft: www.microsoft.com*
- *Agencia de Certificación Electrónica: www.ace.es*
- *Global TrustAuthority: www.gta.multicert.org*

Autoridades Certificadoras.

Las AC asumen el papel de fedatarios públicos verificando la identidad de usuarios y entidades. Para ello proporcionan un certificado digital. En la actualidad la certificación en Internet usa el estándar **X.509 v3**, que permite:

- ✓ Firmar digitalmente los mensajes de tal forma que sólo el receptor puede descifrarlos y tener acceso a su contenido, garantizando la autenticidad y el no repudio.
- ✓ Cifrar la información del certificado de tal forma que sólo el receptor pueda descifrarlo y tener acceso a su contenido garantizando su integridad y confidencialidad.
- ✓ Autenticar la identidad de acceso de los usuarios de redes.

Certificados.

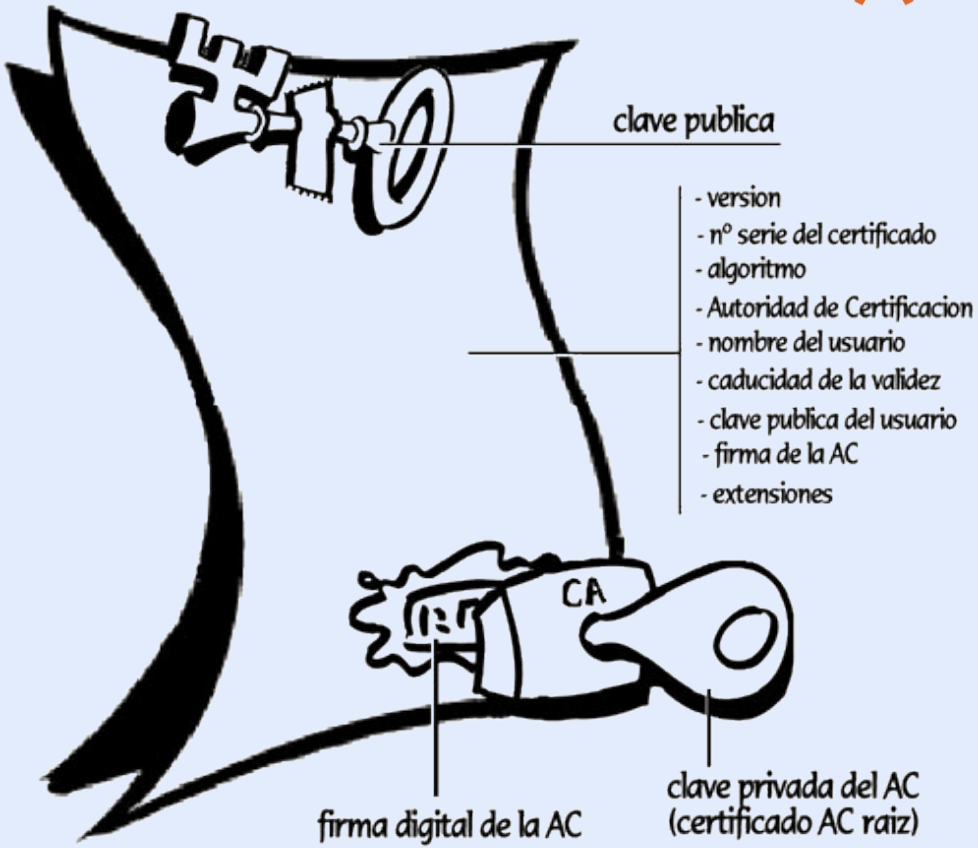
Un certificado digital es un vínculo entre una clave pública y una identidad de usuario, que se consigue mediante una firma digital por una tercera parte o autoridad de certificación (AC) que publica su clave pública en la que TODOS confían.

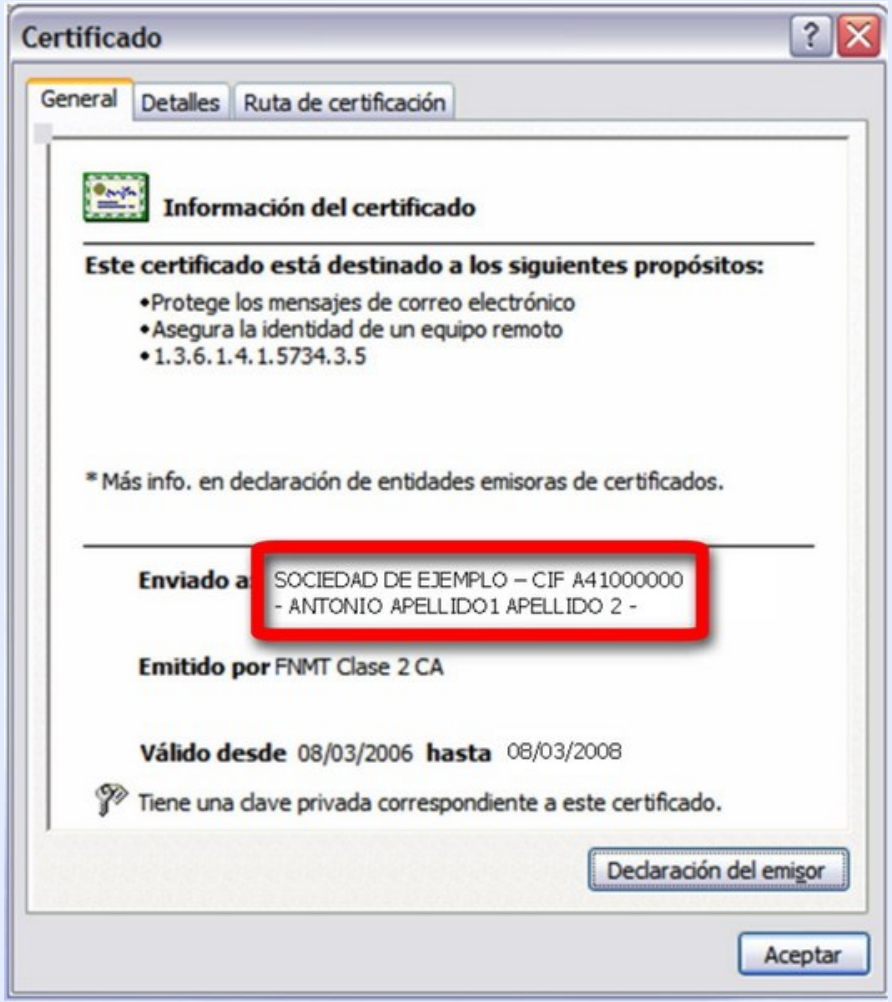
Por tanto, el certificado se considera como un objeto firmado con la clave privada de la autoridad de certificación (AC), e incluyendo: identidad del usuario, clave, periodo de validez, identidad emisor, …

El Certificado Digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona (*organización*) en Internet. Se trata de un requisito indispensable para que las instituciones puedan **ofrecer servicios seguros a través de Internet**.

Certificado X.509 v3

- RFC 3280.
- X.509 v3 es el protocolo que se utiliza para certificar las claves públicas, con lo que los usuarios pueden intercambiar datos de manera segura.
- Está basado en criptografía asimétrica y firma digital.
- Se emplea para autentificar la información en redes externas e internas y en el correo electrónico.
- Para que una clave pública se pueda considerar válida y asociada a un usuario determinado debe tener un certificado que así lo demuestre.





Ejemplo de un certificado digital, el cual es un documento (archivo) que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado (con la clave privada) por una Autoridad de Certificación (AC).

SSL.

SSL es el acrónimo de ***Secure Sockets Layer*** (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

SSL (Secure Socket Layer)

- Desarrollado por Netscape en 1995 para dotar de seguridad a las comunicaciones sobre Internet.
- Última versión SSL-v3.
- SSL proporciona autentificación para servidores y navegadores, así como confidencialidad e integridad de los datos para comunicaciones entre un servidor web y un navegador.



TLS.

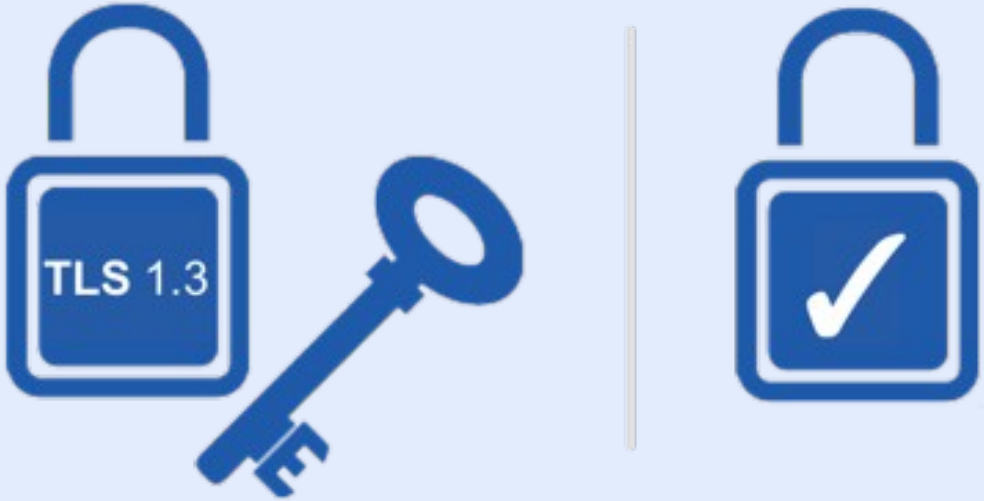
El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL.

Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL en Symantec, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

TLS (Transport Layer Security)

- TLS es una mejora del protocolo SSL; es una generalización de SSL para ser un estándar no dependiente de un solo fabricante (Netscape).

- Última versión TLS v1.3.

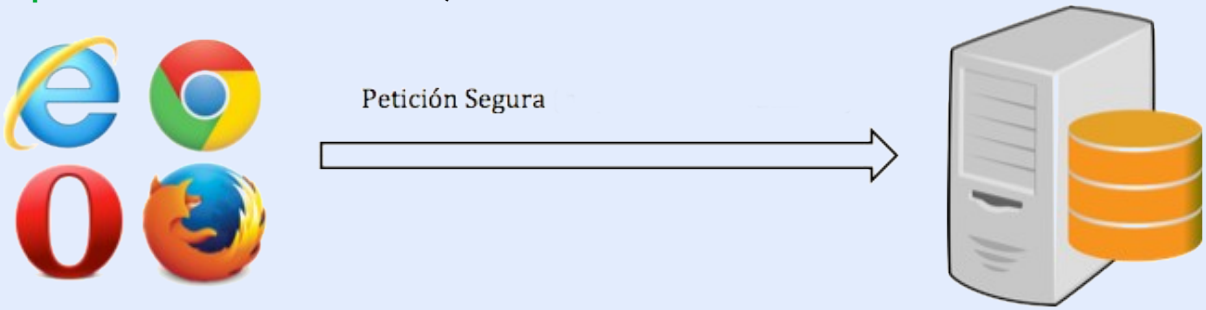


Encriptado Web: HTTPS.

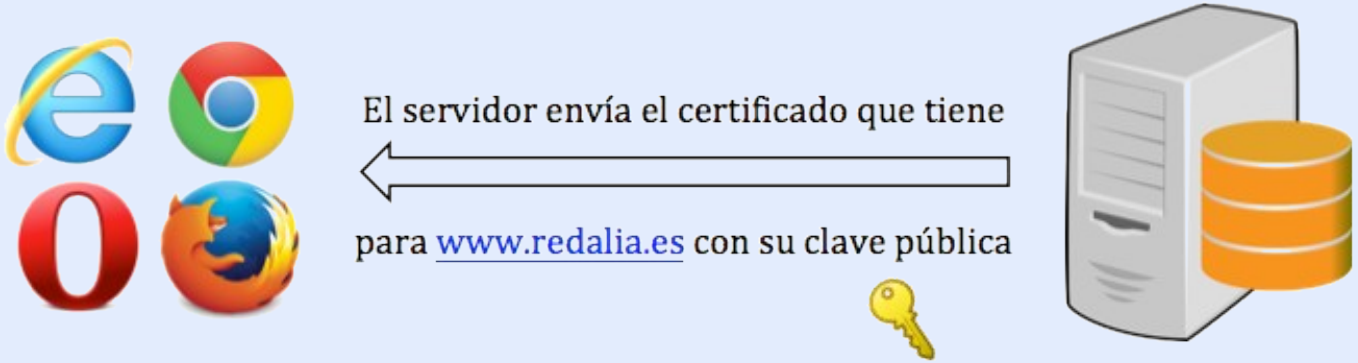
Mediante un ejemplo concreto, vamos e explicar cómo funciona el protocolo SSL/TLS combinado con HTTP, para dar lugar a la versión segura de HTTP o HTTPS.

Para ello, vamos a pasar a detallar paso a paso, lo que sucede cuando un cliente accede a un sitio web de un servidor con un certificado SSL a través del protocolo HTTPS:

Un usuario realiza una petición HTTP segura a través de un navegador a un sitio web (https://www.redalia.es/).

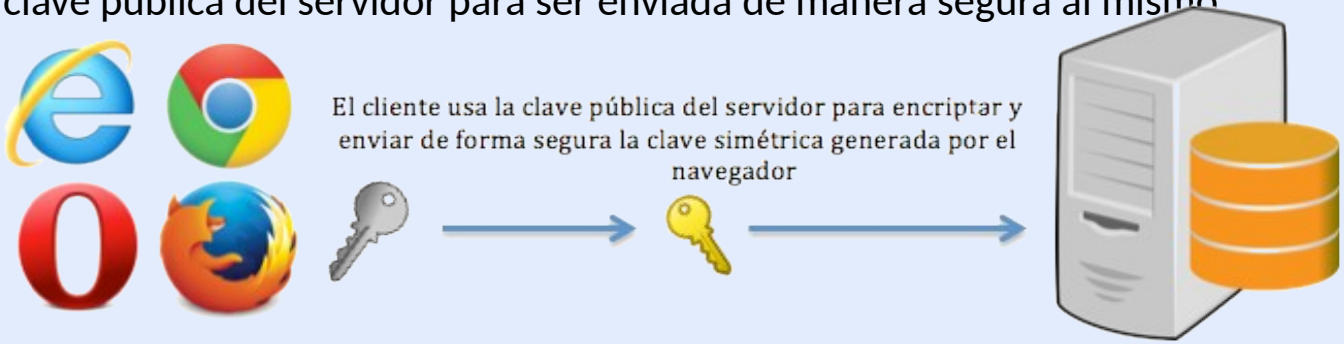


El servidor donde está alojado el sitio web, envía (si lo tiene) el certificado que incluye la clave pública del servidor. En caso de no tener certificado SSL, se producirá un error.

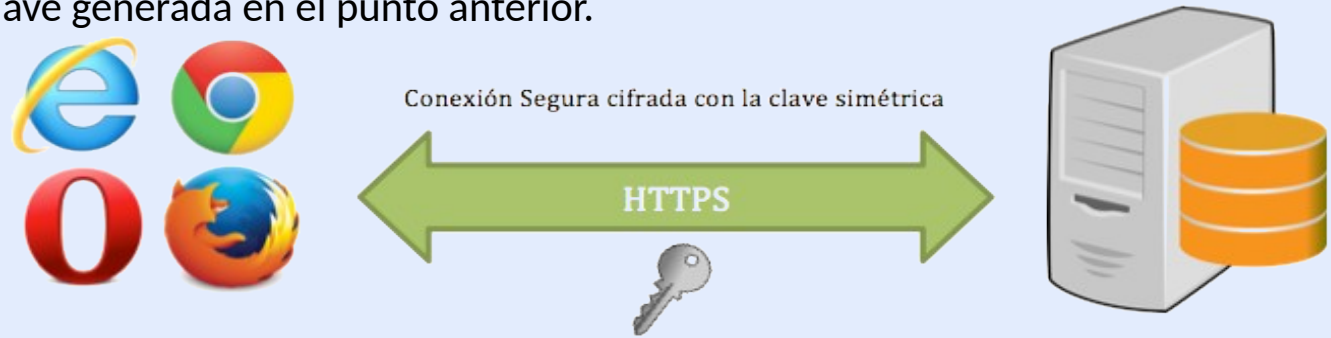


El navegador comprueba que la entidad emisora del certificado o CA sea de confianza. En caso contrario, pedirá al usuario que acepte el certificado bajo su responsabilidad.

Llegados a este punto, el navegador generará una clave simétrica, que será cifrada mediante la clave pública del servidor para ser enviada de manera segura al mismo



De esta forma, la comunicación ya se ha establecido de manera segura, y será cifrada en ambos sentidos mediante la clave generada en el punto anterior.



Bibliografía.

- http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html
- https://www.pabloyglesias.com/mundohacker-esteganografia/
- https://www.escueladeinternet.com/funcionan-las-autoridades-certifican-los-ssl/
- https://www.upv.es/contenidos/CD/info/711545normalc.html
- https://tecnologia-informatica.com/que-es-la-criptografia/
- https://www.redalia.es/ssl/protocolo-ssl/

El empleo es de todos

Mintrabajo

GC-F-004v.03

Realizado por:

Rodrigo Ebrat Carr

rebratc@sena.edu.co

Gracias

SENA