

Unidad 4: Criptografía

Resultados de Aprendizaje a trabajar en esta Unidad:
RA1: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. **RA2:** Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
Contenidos a trabajar en esta Unidad:
• Principios de criptografía • Tipos de algoritmos de cifrado • Criptografía simétrica • Criptografía asimétrica • Criptografía híbrida • Firma digital • Certificados digitales • DNI electrónico

Contenidos de la Unidad

1. INTRODUCCIÓN 2
2. PRINCIPIOS DE LA CRIPTOGRAFÍA 2
3. TIPOS DE ALGORITMO DE CIFRADO 4
4. APLICACIONES DE LA CRIPTOGRAFÍA 7
5. SSL Y TSL 13
6. BIBLIOGRAFÍA 13

1. INTRODUCCIÓN

El término criptografía proviene de las palabras griegas "cripto", que significa escondido, y "grafía", que significa escritura.

Por tanto, la **criptografía** es la técnica cuyo objetivo es la escritura oculta. Esto aplica se aplica, por ejemplo, al envío de mensajes cifrados con el propósito de asegurar la privacidad de su contenido. Sólo el receptor válido tendrá la clave para poder entender el contenido del mensaje enviado.

Los **objetivos** de la criptografía son:

- Asegurar la **privacidad** del mensaje. Los intrusos que logren interceptar el mensaje solo verán un texto sin sentido.
- Asegurar la **integridad** del mensaje. Un intruso puede interceptar el mensaje y provocar cambios en el mismo, pero el receptor dispone de los medios para detectar cualquier alteración sufrida por el mensaje durante su envío.
- Asegurar la **autenticidad** del mensaje. El propio mensaje debe contener algún medio para demostrar la identidad del emisor. El receptor obtiene en el propio mensaje una prueba inequívoca de la autoría del mismo, con la que se demuestra que el emisor es quien dice ser.

Cifrando los mensajes garantizaremos la confidencialidad de la información. Esto será importante cuando estemos trabajando en redes compartidas con personas ajenas a nuestra organización, de forma que la información enviada sólo pueda ser accesible por la persona destinataria.

Para conocer un poco sobre la historia de la criptografía, se puede consultar el artículo disponible en este enlace.

2. PRINCIPIOS DE LA CRIPTOGRAFÍA

Se suele conocer a la criptografía como el arte de cifrar y descifrar información mediante técnicas especiales de forma que esté oculta a quien no sepa la clave de cifrado.

Tiene utilidad en el intercambio de mensajes para mantener la privacidad de la información, aunque también se usa en el almacenamiento cifrado de la información para garantizar la privacidad de la misma.

Para ser exactos, habría que hablar de la criptología como la ciencia que engloba la criptografía y el criptoanálisis, entendido este último como el estudio de los métodos para recuperar la información original en ausencia de las claves de cifrado/descifrado.

La criptografía se considera una rama de las matemáticas que hace uso de técnicas de esta ciencia para el cifrado de mensajes o archivos mediante algoritmos, utilizando una o más claves.

En términos de criptografía, podemos destacar los siguientes conceptos:

- **Texto en claro o texto plano**: es la información original a proteger, sin cifrar.
- **Cifrado**: es el proceso de obtener un **texto ilegible (cifrado)** a partir de un texto en claro.
- El cifrado se basa en la aplicación de un algoritmo que modifica el texto en claro basándose en una **clave de cifrado** para obtener el **texto ilegible o criptograma.**
- **Descifrado:** es el proceso inverso al cifrado. Se obtiene el texto original a partir del texto cifrado y la clave de cifrado.



Existen dos grandes tipos de algoritmos de cifrado:

- **Cifrados en bloque**: divide el texto de origen en bloques de bits de un tamaño fijo. Estos bloques son cifrados de forma independiente. Posteriormente se construye el documento cifrado.
- **Cifrados de flujo**: no atiende a bloques, si no que el texto en plano se va cifrando bit a bit, byte a byte o carácter a carácter. Son muy útiles cuando tenemos que transmitir información cifrada según se va creando.

En criptografía básica, las dos técnicas de cifrado más sencilla son:

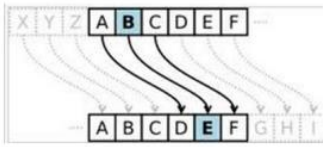
- **Sustitución**: es el cambio de los elementos básicos del mensaje (letras, símbolos, dígitos…).
- **Transposición**: es la reordenación de los elementos básicos del mensaje, sin la modificación de ninguno de ellos.

3. TIPOS DE ALGORITMO DE CIFRADO

Ya en las antiguas civilizaciones se usaban códigos secretos para enviar mensajes en las guerras para garantizar que, aunque el mensaje y el mensajero fueran interceptados, la información quedará a salvo.

Hay documentos de la antigua Grecia que documentan un sistema de cifrado basado en las posiciones de las letras en una tabla. También los romanos utilizaron este método, conocido como César.

El sistema de cifrado de César desplazaba en tres posiciones cada letra y, por tanto, el proceso inverso para descifrar el mensaje. Era un algoritmo de ***cifrado simétrico****.*



Alfabeto llano a b c d e f g h ı j k l m n o p q r s t u v w x y z
Alfab. cifrado D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Texto llano v e n i, v i d i, v i c i
Texto cifrado Y H Q L, Y L G L, Y L F L

En la actualidad, diferenciamos dos grandes grupos de algoritmos de cifrado:

- **Simétricos, o de clave simétrica**. Estos algoritmos utilizan la misma clave para cifrar el mensaje que para descifrarlo.
- **Asimétricos, o de clave asimétrica**. Los algoritmos utilizan una clave diferente para cifrar el mensaje y para descifrarlo. Son los algoritmos de cifrado que se usan en la actualidad, al resultar más seguros.

Según el **principio de Kerckhoffs,** la fortaleza de un sistema de cifrado debe recaer en la clave, y no en el algoritmo cuyos principios de funcionamiento suelen ser conocidos.

3.1. Criptografía simétrica

La **criptografía simétrica** es un método en el que se utiliza una única clave secreta (conocida de antemano por las dos partes) tanto para cifrar como para descifrar un mensaje.

- **Importancia de la clave**: La seguridad del sistema depende principalmente de que la clave sea difícil de descubrir. El algoritmo de cifrado puede ser conocido públicamente; lo importante es que la clave permanezca protegida.
- **Características de la clave**: Su seguridad depende, entre otros factores, de su longitud (número de caracteres o bits) y del conjunto de caracteres que pueden utilizarse para generarla. Cuanto mayor sea el número de combinaciones posibles, más difícil será descubrirla mediante un ataque de fuerza bruta.

Aunque los sistemas que utilizan este tipo de criptografía pueden ofrecer un nivel de seguridad muy elevado, presentan dos **dificultades** importantes:

- Intercambio de claves: El emisor y el receptor necesitan compartir la clave secreta antes de comenzar a comunicarse. Este intercambio debe realizarse de forma segura, ya que, si alguien consigue interceptar la clave, podrá descifrar los mensajes. En ocasiones, resulta más sencillo robar la clave durante su transmisión que intentar romper el propio cifrado.
- Gestión del número de claves: Cada pareja de usuarios que quiera comunicarse de forma privada necesita disponer de una clave secreta diferente. Por ejemplo, si tenemos 4 personas que quieren comunicarse entre sí, necesitaremos 6 claves distintas. En general, para N usuarios, el número de claves necesarias es N(N-1)/2 . Esto hace que la gestión de claves será complicada cuando el número de usuarios es elevado.

Algunos ejemplos de algoritmos de cifrado simétrico:

- **DES**: usa claves de 56 bits. Aunque esto supone un número de 256 de posibilidades (muy alto), los actuales ordenadores pueden atacar sin problemas esa cantidad.
- **3DES, Blowfish o IDEA** son algoritmos que usan claves de 128 bits. Mucho más seguros. Los usan tarjetas de crédito y medios de pago electrónicos.
- Otros muy usados son **RC5 y AES** (Advanced Encryption Standard) también llamada Rijndael, estándar de cifrado del gobierno USA. Actualmente es el algoritmo más utilizado en cifrado simétrico. Usado para IPSEC en conexiones VPN. Usado en WAP2.

3.2. Criptografía asimétrica

Los sistemas de criptografía asimétrica se basan en el uso de dos claves diferentes pero relacionadas matemáticamente

- **Clave privada**, custodiada por su propietario, y no se le dará a conocer a nadie más.
- **Clave pública**, conocida por todos los usuarios que quieran ponerse en contacto con el propietario o que quieran autentificar sus mensajes.

En estas parejas de claves, lo que cifra una sólo lo puede descifrar la otra y viceversa. Es imposible obtener una clave a partir de la otra.

Su funcionamiento se apoya en problemas matemáticos que son fáciles de resolver en un sentido, pero muy difíciles de invertir. Es decir, resulta sencillo realizar una operación, pero prácticamente imposible recuperar los datos originales a partir del resultado si no se dispone de la información adecuada.

Las claves en algoritmos de clave asimétrica requieren mayores tamaños, siendo necesario un mínimo de 1024 bits para las claves públicas.

La mayor ventaja de la criptografía asimétrica es que lo que se cifra con una clave sólo se puede descifrar con la otra, sin embargo existen algunos inconvenientes:

- A mayor longitud de clave, el sistema requiere mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que en sistemas simétricos.
- El mensaje cifrado ocupa más espacio que el mensaje original.

Algunos algoritmos de clave asimétrica son Diffie-Hellman, RSA, DSA.

Algunos protocolos y software que usan esos algoritmos son: DSS, PGP, GPG, SSH, SSL, TLS...

3.3. Funciones hash o funciones resumen

Las **funciones hash** o funciones resumen, son algoritmos que permiten comprobar la integridad de un documento o mensaje, es decir, verificar que su contenido no ha sido modificado.

Estos algoritmos reciben un mensaje de una longitud determinada y devuelven una cadena de caracteres que representan el resumen, hash, huella digital o checksum, es decir, una suma de verificación del original. Se diferencia de los sistemas de cifrado principalmente porque no es posible descifrarlos y volver al original.

La función hash se envía junto con el documento cifrado. Permitirá al receptor si se ha producido una alteración malintencionada sobre el mensaje original. El receptor separa el mensaje cifrado de la función hash. Al desencriptar el cifrado, deberá calcular su función hash, y esta deberá coincidir con la que ha recibido. En caso contrario, se confirma que ha habido alguna alteración de la información.

Algunos ejemplos de algoritmos hash son:

- MD5 (Message Digest 5). Acepta una entrada de cualquier longitud y devuelve una cadena de 128 bits.
- SHA (Secure Hash Algoritm). Acepta como entrada hasta 264 bits y devuelve una cadena de 160 bits.
- CRC (Cyclic Redundancy Check). Códigos de redundancia cíclica, muy utilizado en detección de errores, recibe un flujo de datos e independientemente de su longitud, devuelve un número fijo de caracteres.

3.4. Criptografía híbrida

El uso de claves asimétricas ralentiza el proceso de cifrado y descifrado de mensajes, mientras que las simétricas tienen el inconveniente de necesitar compartir previamente una clave secreta.

Para solventarlo, una práctica sencilla puede ser utilizar criptografía híbrida. La **criptografía híbrida** combina la criptografía asimétrica y la simétrica en un mismo proceso de comunicación.

En primer lugar, para establecer la comunicación, se utiliza la criptografía asimétrica para intercambiar de forma segura una clave simétrica entre el emisor y el receptor. Una vez ambos conocen la clave simétrica, la utilizan para cifrar y descifrar los mensajes que intercambiar, siendo este un proceso mucho más rápido. La clave simétrica puede cambiarse periódicamente para reducir el impacto de una posible filtración de la criptografía simétrica.

Un ejemplo es el **protocolo SSH** (Secure Shell) que permite cifrar la conversación de extremo a extremo, utilizando técnicas criptográficas para establecer conexiones seguras entre equipos a través de una red. Durante el establecimiento de la conexión se negocian los algoritmos y las claves de sesión, que posteriormente permiten proteger la comunicación.

GNU Privacy Guard (GnuPG o GPG) es una herramienta de software libre que permite cifrar y firmar digitalmente archivos y mensajes. GnuPG utiliza criptografía híbrida, combinando algoritmos simétricos y asimétricos para aprovechar las ventajas de ambos. Permite el cifrado híbrido, la gestión de claves para cada usuario, añadir una firma digital criptográfica a un mensaje, etc.

4. APLICACIONES DE LA CRIPTOGRAFÍA

4.1. Firma digital

Una ventaja de la criptografía de clave pública (o criptografía asimétrica) es que ofrece un método para la firma digital.

Las **firmas digitales** permiten al receptor del mensaje verificar la autenticidad del origen de la información, así como verificar que dicha información no ha sido modificada desde su generación. Estas características nos ofrecen soporte para la **autenticación** y la integridad de los datos, así como el **no repudio** en origen.

La firma digital tiene el mismo propósito que la manuscrita, pero es más difícil de falsificar. La firma digital es el resultado de cifrar, con clave privada, el resumen de los datos a firmar, haciendo uso de funciones hash. Al cifrar solo parte del mensaje (el

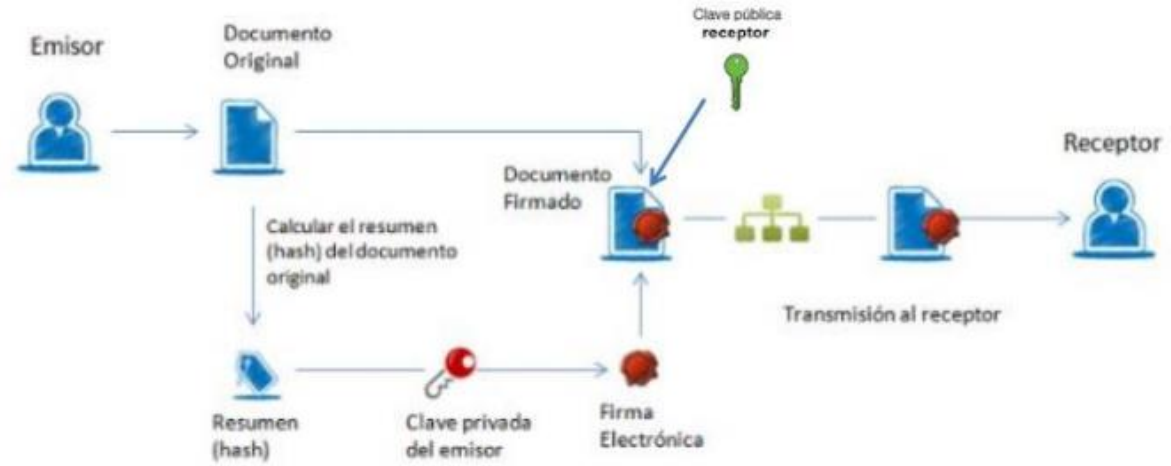
resumen), no estamos perjudicados por la lentitud del proceso de cifrado con clave asimétrica.

Por tanto, con el sistema de firma digital se consigue:

- Autenticación: verificación de la persona que firma el documento (equivalente al a la firma física de un documento).
- Integridad: la firma digital nos permite verificar que el documento no ha sido modificado desde su creación.
- No repudio en origen: el emisor no puede negar el haber enviado el mensaje.

El proceso que ocurre **en el emisor** es el siguiente:

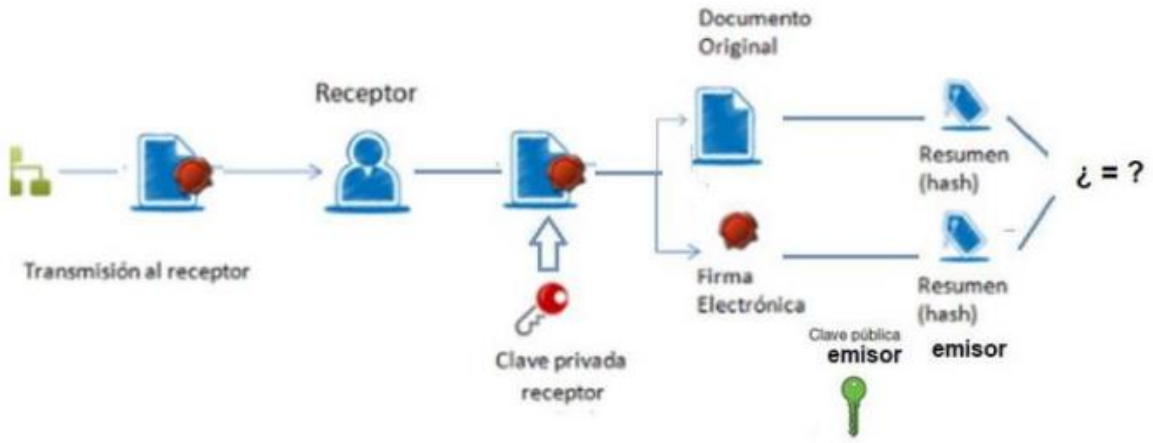
1) Se genera un valor resumen del documento usando una función hash. Este valor se cifra con la clave privada del emisor (esto permite asegurar que la única persona que ha podido firmar el documento es el propietario del documento). El resultado es lo que se conoce como firma digital del documento.
2) El emisor toma la clave pública del receptor para aplicar el algoritmo simétrico al documento y a la función resumen.
3) El resultado es un documento conjunto cifrado que se envía al receptor.
4) Por lo tanto, dos documentos distintos firmados digitalmente por una misma persona tendrán firmas digitales distinta, ya que los valores resumen nunca serán iguales.



El proceso que ocurre **en el receptor** es el siguiente:

1) Para verificar la firma del documento recibido utilizará su clave cifrada para descifrar los documentos, y la clave pública del emisor para comprobar la firma usando la función resumen (cifrada con la clave privada del emisor).
2) El receptor, con su clave privada, obtiene el documento y la función resumen enviada por el emisor.

3) Con el documento descifrado, calcula el valor resumen (1).
4) Con la clave pública del emisor, aplicándola a la función resumen enviada por el receptor cifrada con su clave privada (firma digital) obtenemos el valor resumen (2) que fue cifrado por el autor del mensaje.
5) Comprueba si ambos valores (1 y 2) son iguales. Si efectivamente son iguales, hay una evidencia de que el autor del mensaje es quien dice ser, porque solo él posee la clave privada capaz de expresar el valor resumen del documento cifrado con dicha clave. Además, se garantiza la integridad del mensaje (no ha sido manipulado por terceros).



4.2. Certificados digitales

Un certificado digital es un documento que contiene los datos de una persona (nombre, dirección, DNI...) o entidad, y una clave pública asignada a esa persona o entidad.

Está firmado digitalmente por una entidad certificadora que tiene autoridad para asegurar la veracidad de los datos contenidos en el certificado. En España, es la Casa de la Moneda y Timbre la que firma la mayoría de los certificados digitales.

El certificado digital permite el acceso a servicios públicos a través de Internet, y con ello, realizar tramitaciones importantes donde es necesario demostrar la identidad del usuario. Por ejemplo: trámites como el acceso a la Agencia Tributaria para ver los datos fiscales de uno mismo y realizar la declaración de la renta, gestionar multas, obtener la vida laboral, etc.

El archivo del certificado digital puede ser utilizado por un software para firmar digitalmente archivos y mensajes, en los que se podrá verificar la identidad del firmante.

Los certificados digitales identifican a personas y organizaciones. Contienen información sobre una persona o entidad: nombre, dirección, correo, ámbito de uso de

la clave pública, fechas de validez del certificado, firma digital de una autoridad de certificación...

Al igual que existen multitud de formatos para guardar una imagen (jpg, bmp, png...), también existen multitud de formatos para los archivos que almacenan los certificados digitales. El formato estándar de los certificados digitales es el X.509 y se pueden distribuir:

- Con clave privada (extensión .pfx o .p12) destinado a uso privado de exportación e importación posterior como copia de seguridad.
- Sólo con clave pública (extensión .cer o .crt) destinado a la distribución no segura, para que otras entidades o usuarios puedan verificar la identidad en archivos o mensajes firmados.

Existen diferentes tipos de certificados digitales:

- **Certificado personal**, que acredita la identidad del titular.
- **Certificado de pertenencia a empresa**, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- **Certificado de representante**, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- **Certificado de persona jurídica**, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- **Certificado de atributo**, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal, por ejemplo, médico, director, apoderado de...

Además, en entornos más técnicos, existen otros tipos de certificados digitales:

- **Certificado de servidor seguro**, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- **Certificado de firma de código**, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

Ahora bien, ¿cómo podemos saber si un certificado digital es válido? La única forma de validar un certificado digital de un usuario desconocido es por una **tercera parte de confianza**. Dos usuarios podrán confiar entre sí, si ambos confían en una tercera parte común que pueda dar fe de la fiabilidad de los dos. Además, la mejor forma de permitir la distribución de claves públicas (o certificados digitales) entre los usuarios, es que algún agente (en quien todos los usuarios confíen) se encargue de su publicación en algún repositorio al que todos tengan acceso.

A modo de resumen:

- Se podrá tener confianza en el certificado digital de un usuario desconocido si su certificado está avalado por una tercera parte en la que sí confiamos.
- La forma en la que esa tercera parte avala un certificado es mediante la firma digital.
- Podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos.
- Esta tercera parte se conoce como **Autoridad de Certificación**.

4.3. PKI (Public Key Infraestructure)

El modelo de confianza basado en terceras partes es la base de la definición de **infraestructuras de clave pública (PKI).**

Este modelo está formado por:

- **Autoridad de certificación (CA)**: emite y elimina certificados digitales.
- **Autoridad de registro (RA):** controla la generación de certificados, procesa peticiones y comprueba la identidad de los usuarios.
- **Autoridad de repositorio**: almacena certificados emitidos.
- Software para el uso de certificados.
- Política de seguridad en las comunicaciones relacionadas con la gestión de certificados.

La tecnología PKI permite a los usuarios:

- Autenticarse frente a otros usuarios.
- Usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío…

Se compone de hardware, software y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital y el no repudio de transacciones electrónicas.

En la PKI también existen **vulnerabilidades**. Las principales son:

- Si entra un virus en nuestro ordenador, puede alterar el depósito de claves e importar claves públicas, sin nosotros darnos cuenta, de CA fraudulentas.
- Un ataque a los servidores de una CA podría robar su clave privada y el atacante podría firmar las claves públicas de servidores peligrosos. Los internautas, pensando que es un sitio de confianza, se conectarían a ellos.



4.4. El DNI Electrónico (DNIe)

El Documento Nacional de Identidad (DNI) emitido por el Ministerio del Interior, acredita, desde hace más de 70 años, la identidad y datos personales de su titular.

En la actual sociedad de la información, se hace necesario adecuar los mecanismos de identificación personal a las nuevas tecnologías, surgiendo así el **DNI electrónico (DNIe).**

El DNIe permite:

- Acreditar electrónicamente, sin posibilidad de duda, la identidad de una persona.
- Firmar documentos electrónicos, otorgándoles validez jurídica equivalente al a de la firma manual.

Incorpora un pequeño circuito integrado capaz de almacenar:

- Certificado electrónico del ciudadano.
- Certificado electrónico para firmar digitalmente de igual validez legal a la firma manuscrita.
- Certificado de Autoridad de Certificación emisora.
- Claves para su utilización.
- Plantilla biométrica de la huella digital.

Para usar el DNIe es necesario:

- Hardware específico: lector de tarjetas inteligentes.
- Software específico: controladores o módulos criptográficos especializados.

En agosto de 2021 se implantó el DNI 4.0 que permite acceder al DNI a través de una aplicación gratuita “DNIe en el móvil”, así como utilizar la firma electrónica desde el smartphone.

5. SSL Y TSL

SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos que proporcionan comunicaciones seguras en una red, como Internet.

Ambos son protocolos de cifrado para la capa de transporte de Internet. Su función es cifrar el tráfico de datos entre el cliente y el servidor.

Una de las principales aplicaciones prácticas de estos protocolos es formar https junto a http garantizando el envío y recepción de información de forma segura en un navegador web.

TLS es el protocolo sucesor de SSL. Es más seguro, flexible y eficiente que su antecesor. Sin embargo, como las siglas SSL siguen siendo más conocidas, muchos proveedores de software de cliente o enrutadores usan el térmico SSL o alternativamente el doble término SSL/TSL.

6. BIBLIOGRAFÍA

Breve historia de la criptografía. El Diario. Disponible en: https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html

Principios de Kerckhoffs. Wikipedia. Disponible en: https://es.wikipedia.org/wiki/Principios_de_Kerckhoffs

Seguridad Informática. Alfonso García-Cervigón, María del Pilar Alegre. Paraninfo.

Seguridad Informática. José Fabián Roa Buendía. McGraw Hill.

Seguridad y alta disponibilidad. Ignacio Triviño Mosquera. Síntesis.