1. INTRODUCCIÓN

A lo largo de la historia el ser humano siempre ha desarrollado sistemas de seguridad que le han permitido comprobar en una comunicación la identidad del interlocutor (ej. tarjetas de identificación, firma), asegurarse de que sólo obtendrá la información el destinatario seleccionado (ej. correo certificado), que además ésta no podrá ser modificada (ej. notariado) e incluso que ninguna de las dos partes podrá negar el hecho (ej. Notariado, firma) ni cuándo se produjo (ej. fechado de documentos). En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad. Actualmente cada vez mayor número de actividades se está trasladando al mundo electrónico a través de Internet. Después de haber estudiado todas las amenazas que se ciernen sobre nosotros y nuestros ordenadores cada vez que navegamos por Internet, puede que tengáis la impresión de que la red es un lugar tremendamente inseguro, en que es delicado realizar operaciones bancarias, administrativas,… sin correr el riesgo de caer presa de los piratas informáticos. Por suerte esto no es así. Fruto del trabajo y la imaginación de matemáticos e informáticos, se han generado sistemas de protección y certificación de contenidos que permiten a Entidades Bancarias, Administraciones y Empresas, realizar de forma segura operaciones de todo tipo (incluso las que implican el envío de información estrictamente personal y confidencial).

Se han trasladado los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas. Necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el plus de ofrecer garantías aún sin presencia física. ¿Cómo se resuelve este problema?

En este último apartado de la unidad vamos a estudiar qué recursos existen para garantizar la seguridad de estas operaciones en la red global.

2. CRIPTOGRAFÍA.

La criptografía (*kryptos* = oculto + *graphe* = escritura) es el arte de escribir en clave o de forma enigmática. En principio se puede expresar como el conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido. En la actualidad estas técnicas permiten además, asegurar que el mensaje no se ha modificado, reconocer al emisor del mensaje, probar la emisión y recepción del mensaje, etc.

Para comprender correctamente conceptos como firma electrónica y certificado digital es necesario partir de los conceptos más básicos sobre criptografía.
Como ya hemos dicho, a lo largo de la historia siempre ha habido necesidad de proteger la información. Así, la criptografía tiene su origen durante el Imperio Romano, en la época del Emperador Julio César. César utilizó un esquema

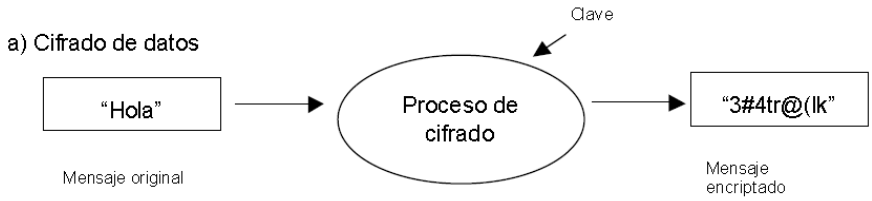
criptográfico simple pero efectivo para comunicarse con sus generales. El esquema de César consistía en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo, la letra "A" podría ser codificada
como "M", la "B" como "N", la "C" como "O" ... así sucesivamente. En este caso, el número que se sumaría a cada letra para realizar la codificación sería el 13.
Así pues, el mensaje "ATAQUEN HOY AL ENEMIGO" podría transformarse en "MFMCGQZ TAK MX QZQYUSA", sin poder ser reconocido por el enemigo.
El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica".
El "desplazamiento de 13 letras" es la clave que se utiliza por César para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un criptosistema de *clave simétrica* en el que se utiliza la misma clave para cifrar y descifrar el mensaje.

Por supuesto hoy en día los sistemas criptográficos que se emplean en Internet son mucho más complicados, aunque la base es la misma. No lo olvide: una clave cifra el mensaje. A continuación veremos su aplicación al mundo de las telecomunicaciones.

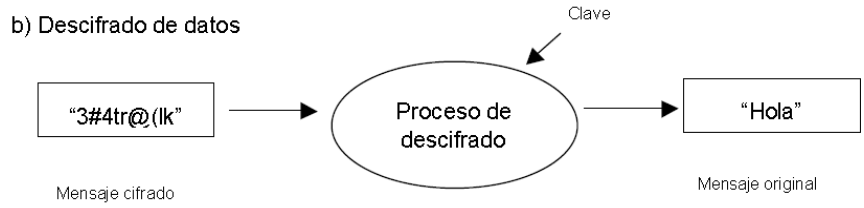
3. LA ENCRIPTACIÓN

La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado permitirá hacer legible un mensaje que estaba cifrado.
A grandes rasgos, la criptografía es una rama de las matemáticas que se ocupa del proceso de encriptación de información. El encriptación o cifrado de datos es una técnica que permite transformar cierta información en una serie de datos ininteligibles o "datos cifrados", como se muestra a continuación:

a) Cifrado de datos



b) Descifrado de datos



Como se observa en la figura, para poder ejecutar ambos procesos de cifrado y descifrado, se necesita utilizar un clave secreta, de manera de sólo quien la conoce puede efectuar dichas operaciones.
De esta manera, por ejemplo, si dos personas se ponen de acuerdo en el valor de una clave secreta, y la mantienen privadamente sólo entre ambos, pueden intercambiar información cifrada. Esto permite que si un agente externo intercepta las comunicaciones, no podrá conocer el contenido original de los mensajes, pues sólo observara datos ininteligibles o cifrados. Para descifrar se necesita conocer la clave.
A las claves usadas para encriptar también se les denomina comúnmente "llaves criptográficas".
En el ejemplo anterior, se uso la misma clave para encriptar y desencriptar. A ésta técnica se le llama "criptografía simétrica", y es una técnica limitada porque no permite asegurar la identidad de quién genera el mensaje, puesto que la clave la conocen, al menos, 2 personas.

3.1. Criptografía Asimétrica: El concepto de clave pública

El concepto de criptografía de clave pública o "asimétrica" fue introducido por W. Diffie y M. Hellman en el año 1976. Está basada en el uso de un par de claves que cumplen, entre otros requisitos, que lo que somos capaces de cifrar con una de ellas, somos capaces de descifrarlo con la otra y sólo con ella.
Una de las claves solo está en poder del propietario, que debe conservarla de forma segura, y se denomina clave privada.
La otra clave es publicada para que la conozcan todos aquellos que quieran comunicarse de modo seguro con el propietario mencionado, a esta última se la denomina clave pública.
La ventaja de estos sistemas criptográficos es que la denominada clave pública puede ser usada por cualquier persona para encriptar mensajes (transformarlos a texto ininteligible) bajo la premisa que solo quien posea la clave privada podrá desencriptar (ver en forma legible) dichos mensajes.
Supóngase que dos personas deseasen intercambiar información confidencial; digamos, Bernardo y Carolina.
1.- Si Bernardo envía a Carolina un mensaje cifrado usando su propia llave privada, Carolina lo puede recuperar usando la llave pública de Bernardo, la cual es conocida.
Carolina esta segura que el mensaje venía de Bernardo, pues solo él lo pudo cifrar usando su llave privada. Esto garantiza la **autenticidad.**
2.- Asimismo, si Bernardo enviase a Carolina un mensaje cifrado usando la llave pública de Carolina, esta seguro que sólo Carolina puede recuperar o leer el mensaje, pues solo ella tiene el otro par de la llave necesario para descifrar (la llave privada de Carolina). Esto garantiza **confidencialidad.**

La idea básica de un sistema de clave pública radica en que es infactible (aun utilizando el mejor computador disponible) determinar la clave privada a partir de la clave pública. Además, una vez encriptado un mensaje, para cualquier persona que no sea el enviador o el receptor es computacionalmente infactible encontrar el mensaje que lo generó.

3.2. El concepto de Firmas Digitales

La criptografia de clave pública también permite disponer de una herramienta análoga a las firmas convencionales: las 'firmas electrónicas o digitales'. Así, de la misma manera en que una firma manuscrita 'convencional' puede ser utilizada en cartas o cheques para especificar la persona responsable por el documento, una firma digital permite enlazar unívocamente a un documento almacenado digitalmente con una persona específica y verificar la autenticidad del contenido del documento.
En particular, un sistema de firmas electrónicas establece un esquema por el cual un 'firmante' puede acompañar un documento por cierta información (una 'firma digital'), generada a partir del contenido del documento y de la clave privada del firmante tal que permita al receptor comprobar que el autor del documento es quien dice ser y que el documento no ha sido alterado.

3.3. El concepto de Certificados de Identidad Digital

En los ejemplos mencionados, un aspecto fundamental es poder garantizar que la llave pública de Carolina que tiene Bernardo sea la que le corresponde a Carolina realmente, y no de una impostora (lo mismo para el caso de Carolina). Esta garantía es la que brindan los certificados digitales de identidad emitidos por Autoridades Certificadoras (AC). Una Autoridad de Certificación (AC, en inglés CA) es una entidad de confianza del emisor y del receptor del mensaje.
Para garantizar que una llave pública le pertenece a cierta entidad, una AC emite un documento electrónico denominado “certificado digital” en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, su llave pública, el periodo de validez de dicho certificado, mas otros datos como el e-mail, restricciones de uso, etc. La autenticidad de estos datos es asegurada pues la AC anexa en el mismo certificado su propia “firma digital”, tal como se mencionó anteriormente.
En resumen, podría decirse que el certificado digital es una especie de “pasaporte electrónico”, que luego puede utilizar la entidad para identificarse (por ejemplo, en el contexto de una transacción electrónica, envió de e-mail, etc). Así, los certificados digitales permiten efectuar comunicaciones electrónicas seguras, garantizando:

- La **autenticidad** de las personas y entidades que intervienen en el intercambio de información.
- **Confidencialidad**: que solo el emisor y el receptor vean la información.
- La **integridad** de la información intercambiada, asegurando que no se produce ninguna manipulación.
- El **no repudio**, que garantiza al titular del certificado que nadie más que él puede generar una firma vinculada a su certificado y le imposibilita a negar su titularidad en los mensajes que haya firmado.

Para el formato de los certificados digitales, existe un estándar internacional ampliamente reconocido, denominado “X.509”. El uso de un estándar permite que un

certificado sea reconocido y compatible con distintas aplicaciones de software y en variados ambientes.
Por último, cabe señalar que la tecnología de certificados de identidad digital ya viene incorporada en aplicaciones usadas en Internet, como son el correo electrónico y los navegadores. Por ejemplo, Microsoft Outlook 2000 permite enviar e-mails firmados digitalmente, y transmitir e-mails encriptados. Para ello basta con tener previamente instalado un "certificado digital" de identidad. Asimismo, con los populares navegadores Internet Explorer o Netscape Navigator, reconocen y manejan íntegramente certificados de identidad digital.

Los ejemplos más típicos de certificados electrónicos son:

- DNI electrónico: DNIe.
- Fábrica Nacional de Moneda y Timbre: Certificado de clase 2 (persona física).

3.3.1. ¿Cómo obtener un Certificado Electrónico?

Las gestiones para la obtención de un certificado electrónico deben realizarse ante una Autoridad de Certificación, reconocida oficialmente.

En particular, para obtener el Certificado de Clase 2 de la Fábrica Nacional de Moneda y Timbre, una vez realizada la solicitud vía internet, deberá acreditar su identidad en una oficina de registro.

3.3.2. Aplicaciones prácticas de los Certificados Electrónicos

Con los certificados electrónicos, es posible realizar consultas y efectuar gestiones a través de la webs de Administración Electrónica o Banca On-Line, permitiendo:

- **Autentificar** la identidad del usuario, de forma electrónica, ante terceros.
- **Firmar** electrónicamente de forma que se garantice la integridad de los datos trasmitidos y su procedencia.
- **Cifrar** datos para que sólo el destinatario del documento pueda acceder a su contenido.

3.4. El protocolo HTTPS

Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP. El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.
La idea principal de https es la de crear un canal seguro sobre una red insegura. Esto proporciona una protección razonable contra ataques *eavesdropping* y *man-in-the-middle*, siempre que se empleen métodos de cifrado adecuados y que el certificado del servidor sea verificado y resulte de confianza.
La confianza inherente en HTTPS está basada en una Autoridad de certificación superior que viene preinstalada en el software del navegador (Es el equivalente a decir "Confío en la autoridad de certificación (p.e. VeriSign/Microsoft/etc.) para decirme en quien debería confiar"). Los protocolos HTTPS son utilizados por navegadores como: Safari, Internet Explorer, Mozilla Firefox, Opera y Google Chrome, entre otros.
Algunos navegadores utilizan un icono (generalmente un candado) en la parte derecha de la barra de direcciones para indicar la existencia de un protocolo de comunicaciones seguro e incluso cambian el color del fondo de la barra de direcciones para identificar páginas web seguras.
Para conocer si una página web que estamos visitando utiliza el protocolo https y es, por tanto, segura en cuanto a la trasmisión de los datos que estamos transcribiendo, debemos observar si en la barra de direcciones de nuestro navegador aparece https al comienzo, en lugar de http.