Sistemas de Identificación. Criptografía.

Caso Práctico

Uno de los principales fines de la seguridad informática es proteger la información. Proteger la información, entre otras cosas, implica que los usuarios y usuarias de una empresa puedan confiar en la misma y que la información sea accesible solo por el personal autorizado.

Precisamente algunos de los problemas a los que se tiene que enfrentar la empresa de Juan en esta ocasión, están muy estrechamente relacionados con la confiabilidad y confidencialidad.

Actualmente, el phishing, es uno de los delitos informáticos más utilizados por los estafadores en la red. Este hecho, entre otros, afecta al departamento de comercio electrónico de la empresa de Juan. Después de realizar algunos estudios con encuestas, los encargados del estudio han llegado a la conclusión de que la empresa está perdiendo un sector importante de su clientela potencial, porque no confían en realizar los trámites de compra a través de la web.

Estando en una sesión de trabajo en la que se analiza este hecho, el ponente determina:

-Estamos ante un problema de confiabilidad.

-Esto se traduce en cuantiosas pérdidas económicas -Intervino rápidamente el director-.

-Por otra parte, se deduce que existen algunos problemas relacionados con la confidencialidad de la información. Existen muchos datos estrictamente confidenciales a los que solo pueden tener acceso determinadas personas. Por ejemplo, en la empresa se está elaborando un nuevo plan de marketing y una reestructuración económica –Puntualizó el jefe del departamento de marketing-. Ignacio sabrá más que yo sobre el tema, pero creo que se debería proteger esta información cuando viaja por la red.

-Es cierto, mucha información al respecto, viaja continuamente por la red. En caso de ser interceptada y de llegar a mano de quien no debería, como por ejemplo alguna empresa de la competencia, podría suponer echar por tierra meses de trabajo –advierte Ignacio-, sin contar con los efectos económicos que implicaría. Existen programas que rastrean el tráfico en la red, por tanto no sería algo descabellado.

-Además de todo ello, que no es poco, la ley exige que determinados datos de los clientes se almacenen de forma ilegible para incrementar el nivel de seguridad y asegurar que nadie pueda tener acceso a información –Intervino Juan, que cada vez se encuentra en una posición más activa en la empresa-.

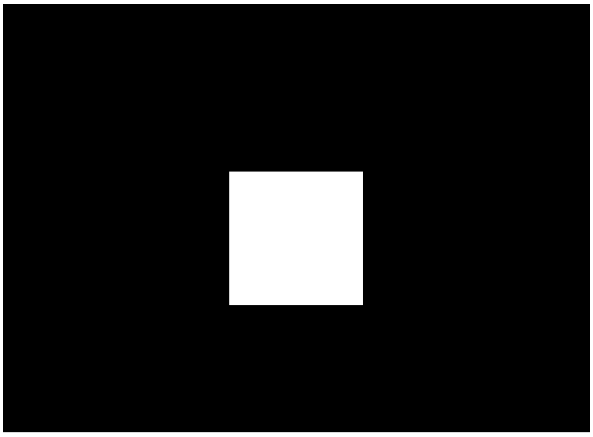
La respuesta a muchos de estos problemas está en el cifrado de la información.

Reflexiona

Como sabes, existen programas que pueden rastrear el tráfico en la red. Cuando entramos en un sitio Web con nuestro usuario y contraseña, esos datos suelen viajar por la red hasta el servidor para comprobar que el usuario está dado de alta y que la contraseña es correcta. ¿Te imaginas qué podría pasar si cuando introducimos nuestro usuario y contraseña en un sitio se envía al servidor "en claro" (sin cifrar)?

Debes conocer

Ésta es una presentación sobre los contenidos fundamentales que se tratarán a lo largo de todo el tema. Es interesante que veas esta presentación para hacerte una idea de lo que vas a aprender en la presente unidad:



00:00 00:48

Introducción a la Criptografía.

Caso Práctico

Ha llegado la hora de hacer la copia de seguridad de uno de los servidores de la empresa. En dicho servidor, se encuentran bases de datos con datos personales de la clientela, documentos de gestión económica de la empresa y otros documentos confidenciales, a los que solamente deberían tener acceso personas muy concretas de la empresa.

-Recuerdo -dice Ignacio- que unos años atrás, un empleado que tenía un negocio de forma paralela a su trabajo en la empresa, obtuvo datos personales de clientes en beneficio de su negocio.

-Naturalmente, se supone –responde Juan -, que dicho empleado no debería tener acceso a dichos datos y mucho menos utilizarlos para su negocio.

Por este tipo de cosas, a la hora de realizar la copia se seguridad, habrá que proteger de alguna manera la información, ya que en el servidor destino se almacenan otros datos a los que sí tienen acceso muchos empleados y empleadas de diversos departamentos.

Juan propone proteger con contraseña los ficheros confidenciales, pero Ignacio cree que no será suficiente:

-¿Por qué no protegemos con contraseña los ficheros que sean confidenciales? –propone Juan.

-Es una buena idea, pero no es suficiente –determina Ignacio-. Además de no ser efectiva al 100%, en muchos casos, no todos los tipos de ficheros son susceptibles de ser protegidos con contraseñas por sí solos.

-Entonces, ¿Qué podemos hacer? –Pregunta Juan.

-Debemos cifrar la información más relevante. Además, en el caso de algunos datos personales, lo exige la propia ley –confirma Ignacio.

Es a partir de este momento cuando Juan e Ignacio de ponen a investigar sobre criptografía y sus diferentes técnicas.

Reflexiona

Seguramente alguna vez habrás visto, o incluso habrás empleado en la infancia, un peculiar lenguaje que consiste en añadir una nueva sílaba detrás de cada sílaba de la palabra, compuesta por una consonante y la vocal de la sílaba que le precede. De esta forma y utilizando la letra 'p' como consonante, la palabra 'casa' pasaría a ser 'capasapa'. Cuando los niños y niñas emplean este lenguaje, lo hacen con el objetivo de que otras personas que escuchan la conversación no sean capaces de entenderla, quedando restringida al emisor y el receptor del mensaje.

Dicho lenguaje no deja de ser una técnica de cifrado cuyo objetivo, como en tantas otras ocasiones, es conseguir la confidencialidad de la información.

Aspectos de Seguridad.

En la primera unidad conociste algunos de los aspectos deseables en un sistema seguro. Vamos a volver a verlos y a añadir alguno que no mencionamos en esa primera toma de contacto. De esta forma, en los siguientes epígrafes podrás relacionar las diferentes técnicas criptográficas con dichos aspectos.

Vamos a definir los siguientes aspectos:

- **Integridad**: Se refiere a la capacidad de asegurar que la información transmitida a través de la red o almacenada en algún medio, no ha sido alterada por algún desconocido.
- **No repudio**: Permite garantizar que los participantes en una transacción no nieguen haber realizado una acción "en línea". Por ejemplo, que hagamos una compra y posteriormente nos neguemos a pagarla alegando que no fuimos nosotros.
- **Autenticidad**: Hace alusión a la capacidad de conocer la identidad de la persona o entidad con la que estamos tratando a través de Internet. Va a repercutir en la confianza del usuario o usuaria hacia la empresa que ofrece el servicio y viceversa: ¿Cómo sabemos que determinado sitio Web es de la empresa que aparenta ser? ¿Cómo sabe el empresario que un cliente es quien dice ser?
- **Confidencialidad**: Garantiza que la información sólo puedan ser leída por aquellas personas autorizadas a hacerlo.
- **Privacidad**: Se refiere al control que debemos tener sobre el uso que se haga de la información que proporcionamos como clientes o clientas a una empresa.

En lo sucesivo, haremos alusión especialmente al cifrado de la información en el envío de mensajes. En cualquier caso, el cifrado, no se limita a dicho ámbito, sino que también se aplica a información almacenada.

Autoevaluación

Relaciona cada aspecto de seguridad con la situación descrita, escribiendo el número asociado al aspecto de seguridad que le corresponda en el hueco correspondiente.

Ejercicio de relacionar.

Situación	Relación	Característica
Una persona no autorizada consigue leer el contenido de un mensaje.	☐	1. Integridad.
Negativa a pagar un artículo comprado por Internet alegando que fue otra persona la que hizo la compra.	☐	2. Repudio.
Un mensaje es interceptado y alterado antes de que llegue a su destino.	☐	3. Autenticidad.
Una página falsa se hace pasar por otra existente para recabar contraseñas.	☐	4. Confidencialidad.

Enviar

Cuando una persona que no es su destinatario accede a un mensaje se está violando la confidencialidad de dicho mensaje.

Por otra parte, repudiar, es sinónimo de rechazar y está relacionado con la negativa al pago después de una transacción económica. Por último, la alteración de la información antes de que llegue a su destino, supone violar la integridad de dicha información y la incapacidad para verificar la identidad de un sitio, como ocurre en el último caso, hace referencia a la autenticidad.

Concepto de Criptografía.

Las distintas técnicas criptográficas te ofrecen un modo de proteger los datos almacenados o intercambiados a través de la red. Del mismo modo, logran algún otro de los requisitos de seguridad antes mencionados.

> El cifrado es el proceso de transformar un mensaje de forma que no pueda ser leído por nadie más que el remitente y el destinatario

Como hemos dicho en el anterior epígrafe, la criptografía es muy útil para incrementar la seguridad en la información transmitida a través de la red, pero no se limita a este contexto. La criptografía te permite proteger tanto la **información almacenada** como la **transmisión de dicha información**.

Mediante la criptografía podemos conseguir:

- Integridad del mensaje.
- No repudio.
- Autenticación.
- Confidencialidad.

Veremos con qué técnicas logramos cada uno de estos aspectos.

Como acabas de ver, el cifrado consiste en la **trasformación** del texto o datos originales en otros ininteligibles. Para realizar este proceso, es necesario algún tipo de **clave**.

Ejercicio resuelto

Muestra algún ejemplo de métodos de cifrado sencillos especificando la clave que utilizas para cifrar la información.

Mostrar retroalimentación

Algunos métodos muy simples son:

- El **cifrado por sustitución**: Consiste en reemplazar una letra por otra diferente.

  Por ejemplo, si usamos la clave "la letra más dos", la palabra "Hola" se transformaría en "Jqnc"
- El **cifrado por transposición**: Consiste en cambiar el orden de dos letras de la misma palabra.

  Leonardo Da Vinci escribía sus notas en orden inverso, de forma que sólo pudieran leerse usando un espejo.
  Así, "Hola" se transformaría "aloH"

Historia.

Conocer algunos hechos acerca de la historia de la criptografía y sus inicios, además de resultar interesante, te ayudará a comprender cómo empezando por métodos muy simples, se llegó a los sofisticados algoritmos que se utilizan hoy en día.

Si bien las técnicas criptográficas más utilizadas hoy en día tienen escasas décadas, existen indicios de mensajes criptográficos en multitud de civilizaciones desde hace cientos de años, como los egipcios, los hebreos o los babilonios.

Desde el inicio de los años 1920, se comenzó a utilizar en Europa una máquina llamada **Enigma**. Se trata de una máquina cuyo mecanismo utilizaba tanto la **sustitución** como **transposición** de caracteres. **Cada día** se generaba una **nueva clave**, de forma que en caso de que el enemigo interceptase alguno de los mensajes cifrados, no resultaría fácil de descifrar, al menos en un tiempo razonable como para poder actuar en consecuencia.

Para descifrar los mensajes en el destino se utilizaba otra máquina igual, ya que todas las máquinas del mundo tenían la misma configuración. Precisamente este hecho, provocó que con la captura de algunas de estas máquinas por parte de los aliados, éstos pudieran llegar a comprender su funcionamiento y, con ello, descifrar los mensajes alemanes.

Para saber más

En el siguiente enlace podrás ampliar la información respecto a la historia y evolución de la criptografía desde sus comienzos.

Historia de la Criptografía en Wikipedia.

Primeros Métodos de Cifrado.

Como has visto, las técnicas criptográficas se han ido perfeccionando poco a poco y haciéndose más sofisticadas, desde que se cifraron los primeros mensajes hace más de 2000 años hasta los tiempos actuales.

Uno de los primeros métodos utilizados fue el método de la escítala. Este método era utilizado por los espartanos y consistía en enrollar una cinta en un bastón de forma que, posteriormente, se escribía el mensaje a lo largo del bastón. De esta forma, cuando se desenrollaba la cinta, el mensaje quedaba ilegible. Para descifrarlo, había que volver a enrollar la cinta a un bastón del mismo grosor, para que las letras quedasen colocadas en el orden adecuado.

Otro método utilizado habitualmente, fue el **Polybios**, que inventado por el escritor griego del mismo nombre. Polybios colocó las letras del alfabeto en una tabla a partir de la cual se sustituyen los caracteres correspondientes. De esta forma, cada letra del alfabeto, se sustituye por un par de letras que indican la fila y la columna en la cual aquella se encuentra.

Ejercicio resuelto

Cifra en siguiente mensaje con el método Polybios. Para ello debes utilizar la tabla que ves a continuación. Mensaje: "Polybios fue un escritor griego."

Método Polybios

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
L	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Mostrar retroalimentación

Debemos sustituir cada letra, por las 2 letras correspondientes a la fila y la columna donde se encuentra. "**LELDEDABBDLDDC BADEAE DELC AEDCACDBBDDDLDDB BBDBBDAEBBLD**"

Otro método clásico de cifrado por sustitución es el conocido como cifrado del César. Este método fue empleado en los tiempos de la Roma Imperial y es llamado así porque es el procedimiento que empleaba Julio César para enviar mensajes secretos a sus legiones. Consistía simplemente en sustituir una letra por la situada tres lugares adelante en el alfabeto. Esto es:

- La A se transformaba en D.
- La B en E.
- La C en F.
- Y así sucesivamente, hasta que la Z se convertía en C.

Debido a la correspondencia entre el alfabeto original y el de cifrado, era un método bastante vulnerable.

Autoevaluación

Utilizando las técnica del César, la frase "mas vale pajaro en mano que ciento volando" quedaría como "sgy bgrk vgpgxu _____ " utilizando un desplazamiento de ☐ caracteres (sin contar la ñ).

Enviar

El cifrado del César, consiste simplemente en sustituir cada letra por la que está n puestos detrás en el alfabeto

Técnicas Criptográficas.

Caso Práctico

Pedro trabaja en el departamento de administración y quiere enviarle a Ignacio un correo con información confidencial. El contenido del mensaje consiste en una serie de propuestas que le envía de cara a tomar decisiones de inversión económica. Ignacio por su parte, dará su punto de vista técnico.

-¡Ringgg! -Suena el teléfono-.

-¿Digame? -Pregunta Pedro-.

-Hola Ignacio, soy Pedro del departamento de Administración. Mira, hemos estado estudiando algunos aspectos que podríamos mejorar para aumentar los beneficios. Algunos de ellos incluyen elementos técnicos, por eso me gustaría que le echases un vistazo para que me des tu opinión y para que hables con algunos proveedores y proveedoras en el caso de que estés de acuerdo en algunos puntos concretos. Bueno, en el correo que te envío ya te explico todo con detalle.

-De acuerdo, pero antes de que me lo envíes, te recomiendo que me lo mandes a través de una cuenta de correo seguro. Por ejemplo, una cuenta gmail de Google. De esa forma la información viajará encriptada y nos cubrimos las espaldas en el caso de que algún hacker trate de rastrear la red con un sniffer.

-De acuerdo, lo mandaré a través de una cuenta segura, descuida.

-Muy bien Pedro, pues ya estoy al tanto de tu correo -le confirma Ignacio-.

-Gracias Ignacio, espero tu respuesta.

Es muy importante asegurarse de que solamente el destinatario, en este caso Ignacio, va a poder acceder a dicha información.

Si no se toman las medidas adecuadas y un hacker rastrease la red con un sniffer, podría obtener parte de la información incluida en el mensaje. De ocurrir esto, se echarían por tierra meses de trabajo, por no hablar de la repercusión económica que podría acarrear si llegase a manos de una empresa de la competencia.

Pero los problemas no terminan aquí. Como sabes, hoy en día se puede suplantar la identidad en el correo electrónico. Si otra persona le envía un correo a Ignacio con información falsa haciéndose pasar por éste e Ignacio toma alguna decisión en base a ello, podría llegar a acarrear graves consecuencias. Por otra parte, el mensaje también es susceptible de modificación durante el tráfico. Si el mensaje fuese manipulado se podrían tomar decisiones erróneas.

Llegado a este punto, ya sabes en qué cosiste la criptografía de forma general, pero todavía no hemos visto las técnicas que se utilizan hoy en día. Existen multitud de técnicas criptográficas.

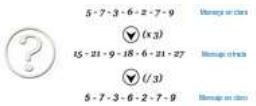
Vamos a ver que, dependiendo de qué técnicas utilicemos para cifrar la información, conseguiremos unos objetivos de seguridad u otros como, por ejemplo, confidencialidad, integridad o autenticación (que está directamente relacionada con los sistemas de identificación).

Criptografía Simétrica.

Si buscas la palabra simetría en el diccionario de la Real Academia, la primera definición que encontrarás será la siguiente: "*Correspondencia exacta en forma, tamaño y posición de las partes de un todo.*"

Como sabes, la mayoría de los primeros métodos de cifrado, utilizaban la misma clave para cifrar y descifrar el mensaje, aplicada de forma inversa. Esto significa que son métodos de **cifrado simétricos**.

Del mismo modo, si aplicamos dichas definiciones al cifrado digital, un cifrado simétrico es aquel que aplica la misma clave para cifrar y descifrar (aunque generalmente de forma inversa). Imagina cifrar la combinación de una caja fuerte multiplicando cada una de sus cifras por un número. Para descifrar dicho número, solo tendríamos que dividir cada una de las cifras por ese mismo número para volver a obtener la combinación.



Hoy en día, se utilizan claves digitales. El algoritmo de cifrado simétrico más usado hoy en día es el DES (Acrónimo. DES= Data Encryption Standard) que comenzó utilizando una clave **de 56 bits.** Debido al incremento de la capacidad de cómputo de los ordenadores, una clave se 56 bits se acabó quedando escasa y se pasó a utilizar el triple DES, que consiste en cifrar tres veces el mensaje con otras tantas claves. Otros ejemplos de sistemas simétricos son RC2, RC4 o RC5 con claves de hasta **2048 bits.**

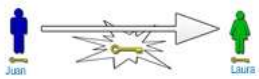
La seguridad, tanto en un cifrado simétrico como en otras técnicas que verás posteriormente, irá en función de la longitud de la clave.

Reflexiona

En una ocasión, una organización propuso un reto que consistía en descifrar un mensaje cifrado con una clave RSA de 64 bits, para lo cual se emplearon 5 años en el año 2002.

Inconvenientes de la Criptografía Simétrica.

Hasta aquí no parece haber problemas más allá de la complejidad de la propia clave, pero vamos a ver que no es el único problema. En un contexto en el que queremos enviar un mensaje a otro destinatario y si partimos de la base de que el destinatario tiene que conocer la clave para poder descifrar el mensaje, ¿cómo hacemos llegar a éste la clave? Si enviamos la clave junto al mensaje, corremos el riesgo de que dicho mensaje sea interceptado con la clave, de forma que podrá ser descifrado.



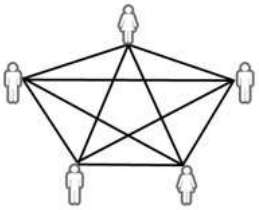
Por lo tanto, tenemos un primer problema, que es enviar la clave se forma segura al destinatario, pero aún hay otro problema más. Necesitaríamos una clave diferente para cada uno de los destinatarios, ya que, si utilizásemos siempre la misma clave, sería conocida por todos y se perdería la confidencialidad deseada. En la práctica, utilizar una clave para cada uno de los destinatarios en inviable.

Ejercicio resuelto

Si tenemos un grupo de 5 personas. ¿Cuántas claves serían necesarias para comunicarse mediante cifrado simétrico entre todas ellas?

Mostrar retroalimentación

Veamos la solución mediante un sencillo esquema:



Como puedes ver, cada arista representa el envío de un mensaje entre 2 personas. Teniendo en cuenta que necesitaremos una clave diferente para cada una de las personas con las que tratemos, existe una arista que parte de cada una de las personas a todas las demás. Ahora solo nos queda contar el número de aristas, que serían 10.

Pero… ¿qué pasaría si en vez de 5 personas fuesen 100? En este caso, el método del dibujo se haría más complicado. Por esta razón conviene calcular el caso general. Una forma fácil de verlo es comprobar la sucesión de los primeros números:

- Para 2 personas: 1.
- Para 3 personas: 3.
- Para 4 personas 6.
- Para 5 personas: 10.
- …

Por tanto, tenemos el siguiente caso general: **n(n-1)/2**

Criptografía de Clave Pública.

Como vas a ver, el cifrado de clave pública, supuso un gran avance en lo referente a técnicas criptográficas. En 1976, Whitfield Diffie y Martin Hellman crearon una técnica totalmente nueva para cifrar mensajes, denominada criptografía de clave pública.

Dicho método tiene las siguientes características:

- Cada persona tendrá dos claves digitales relacionadas matemáticamente entre sí.
- Una clave es pública y la otra privada.
- Ambas sirven para cifrar y descifrar, pero lo que se cifra con una, sólo se podrá descifrar con la otra.
- Las funciones matemáticas usadas para generar las claves garantizan que no se puede averiguar una clave a partir de la otra.

Al utilizar una clave diferente para cifrar y descifrar el mensaje, no existe el problema del intercambio de claves que tenía el cifrado de clave simétrica.

Ejemplo:

¿Qué ventajas tiene este método?

- Nos garantiza la confidencialidad del mensaje, evitando los inconvenientes que tiene el cifrado simétrico.

¿Con dicho método conseguimos cubrir todos los aspectos de seguridad?

- No, sigue sin existir garantía de que el emisor sea quien dice ser (autenticación). Por tanto, éste podría negar haber enviado el mensaje (no repudio). Tampoco garantiza que el mensaje no haya sido alterado durante la transmisión (integridad).

Autoevaluación

Ignacio, quiere enviarle al gerente de la empresa un correo confidencial. Señala cuál de las siguientes opciones sería la más adecuada para mantener dicha confidencialidad.

- ○ Cifrar el mensaje con la clave privada de Ignacio
- ○ Cifrar el mensaje con la clave privada del gerente
- ○ Cifrar el mensaje con la clave pública del director.
- ○ Cifrar el mensaje con una clave simétrica que deberán conocer ambos.

Incorrecto, si se cifra con la clave privada de Ignacio, se descifrará con su clave pública, a la que podría tener acceso todo el mundo. Por tanto, no garantizaría la confidencialidad.

No es correcto. Ignacio no podría utilizar la clave privada del gerente, ya que no puede tener acceso a ella.

Muy bien, has captado la idea…

No es la opción correcta. El hecho de cifrar con una clave simétrica supone tener que compartir la clave, con el riesgo que entraña. Además, si utilizase cifrado simétrico necesitaría otra clave diferente cada vez que enviase algo a otro destinatario.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Firmas Digitales.

Al igual que la firma manuscrita tradicional, permite identificar a la persona que, en este caso, está realizando una transacción electrónica. Por tanto, logra la **autenticación** del usuario, cosa que no era posible a través de la criptografía de clave pública por sí sola.

Dicho de otro modo, permite identificar al emisor, certificando que es quien dice ser, es decir, que no se trata de ningún impostor o impostora, lo que implica evitar el **repudio**. Esta firma compromete al emisor, actuando como prueba, de la misma forma que nos compromete la firma manuscrita cuando firmamos un documento, con la ventaja de que, en este caso, al ser una firma digital es mucho más fácil de verificar y contiene mucha más información.

Desde el punto de vista técnico, es el proceso inverso al de la clave pública. En este caso, el emisor cifra el mensaje original empleando su clave privada. El receptor, para descifrarlo, usará la clave pública del emisor.
Lógicamente, hay que usarlo en combinación con la clave pública para seguir garantizando la confidencialidad. De lo contrario, al utilizar como clave de descifrado una clave pública, cualquier persona podría tener acceso al mensaje.

Autoevaluación

Señala la opción correcta:

- ○ Si envío una información encriptada con la clave pública de mi destinatario, éste o ésta podrá desencriptarla solamente con mi clave pública.
- ○ Si encripto un mensaje con la clave pública de mi destinatario aseguro la confidencialidad del mensaje.
- ○ Si yo encripto un mensaje con la clave privada de mi destinatario, éste ó ésta podrá desencriptar el mensaje con mi clave Pública.
- ○ Si encripto un mensaje con mi clave publica, aseguro que el mensaje es mío, es decir, autentifico el mensaje.

Incorrecto, cuando se cifra con la clave pública de una persona solamente se puede descifrar con la privada de dicha persona y viceversa.

Correcto, así es…solamente se podrá descifrar con la clave privada del destinatario, a la cual solo él ó ella tiene acceso. Por tanto, asegura la confidencialidad.

No es correcto, un usuario solamente tiene acceso a su propia clave privada, nunca a la de otro destinatario.

No es la opción correcta. A mi clave pública podría tener acceso cualquier persona. Por lo tanto, no existe la manera de demostrar que he sido yo quien cifró el mensaje.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

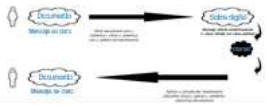
Sobres Digitales.

Has visto que el cifrado de clave pública es un método efectivo de cara a mantener la confidencialidad y combinado con la firma electrónica se pueden lograr otros aspectos como la autenticación y el no repudio. Uno de los problemas que puedes notar en este tipo de cifrado es que es **computacionalmente lento**.

Es decir, si usamos claves de 256 o 512 bits para cifrar un documento de gran tamaño podría llegar a tardar bastante tiempo en realizar la operación. La criptografía de clave simétrica es mucho más rápida pero tiene el problema del envío de la clave.

Como solución intermedia al problema del que hablamos se propuso: usar criptografía simétrica para cifrar documentos grandes y enviar la clave cifrada mediante criptografía de clave pública.

Este método es lo que se conoce como **sobre digital**. En el siguiente esquema puedes ver su funcionamiento.



Autoevaluación

La técnica conocida como sobre digital, consiste en:

- ○ Cifrar un documento extenso con la clave privada del destinatario y posteriormente con su clave pública.
- ○ Cifrar el documento con la clave privada del emisor para posteriormente cifrar la propia clave con cifrado simétrico.
- ○ Cifrar el documento con una clave simétrica y posteriormente cifrar la clave simétrica con la clave pública del emisor
- ○ Cifrar el documento con una clave simétrica y posteriormente encriptar dicha clave simétrica con la clave pública del emisor

Incorrecto, el sobre digital no consiste en dicho proceso. Además, no sería posible que utilizásemos la clave privada del destinatario.

No es correcto, no tendría sentido utilizar un cifrado simétrico para cifrar una clave privada. Además de no ser un método seguro, la clave privada nunca va a ser enviada.

Muy bien, has captado la idea. En eso consiste un sobre digital. De esta forma ciframos el documento en un tiempo razonable y aseguramos la confidencialidad encriptando la clave simétrica con la clave pública del destinatario.

No es la opción correcta. Si utilizamos la clave pública del emisor para cifrar la clave simétrica, solamente se podrá descifrar con la privada de éste. Por lo tanto, no tendría sentido hacer algo así.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Certificados Digitales.

Caso Práctico

Recientemente se ha realizado un estudio a través de una serie de encuestas a clientela potencial del portal de comercio electrónico de la empresa. Después de dicho estudio, ha quedado de manifiesto que la principal razón por la que gran parte de esa clientela potencial no compra es la desconfianza. Es decir, tienen miedo a sufrir estafas mediante delitos informáticos como, por ejemplo, el famoso Phishing.

Una vez más, Juan e Ignacio proponen una solución al problema en una reunión con el equipo directivo y personal de diversos departamentos. En este caso, la solución propuesta consiste en utilizar certificados digitales:

-La solución puede estar en los certificados digitales –propone Ignacio- ¿Alguien sabe lo que es un certificado digital?

-Un certificado digital es un documento que contiene una serie de información de un usuario tal como: nombre, dirección de correo electrónico, una clave pública del usuario, una fecha de caducidad y la firma de una autoridad de certificación –respondió, a su vez, otro miembro de la mesa.

-¡Sí! Yo tengo uno y me ahorra mucho tiempo haciendo gestiones por Internet. Lo solicité hace tiempo y ahora mismo puedo consultar información y hacer "papeleos" sin tener que hacer colas -responde Juan con entusiasmo.

-¿Y habrá peligro de que alguien se haga pasar por nosotros? Es decir, ¿qué pasaría si yo solicito un certificado dando tus datos?-pregunta otro compañero.

-Tranquilo, eso está previsto. Para eso están las autoridades de certificación. Nuestro certificado, estará firmado por una autoridad competente que habrá comprobado anteriormente la correspondencia de identidad entre la persona física y el certificado. Entonces siempre que el certificado esté firmado por una de estas autoridades, podemos estar seguros de la autenticidad del certificado.

-Pero… ¿Cómo podemos emplear un certificado digital para resolver este problema? –interviene su compañera Sandra.

-Pues sería algo similar. Lo que tú tienes es un certificado personal, pero también existen certificados para servidor -explica Juan una vez más.

-Y… ¿cómo llevarlo a la práctica? –preguntó Sandra con interés.

-Lo que necesitamos en este caso, es establecer una conexión SSL.

-Ya estamos con las siglas... -dijo Sandra un poco impaciente.

-Es el acrónimo de Secure Socket Layer –aclaró Ignacio-. Mediante una conexión de este tipo los datos viajan encriptadas y, además, proporcionaremos un certificado en el servidor. En el cliente sería opcional. De esta manera cualquiera podrá comprobar la veracidad del portal.

El certificado digital, puede tener diferentes formatos. También existen varias formas de utilizarlo, pero la más común, es instalarlo en el navegador web de nuestro ordenador. De esta forma, cuando entramos en un sitio que requiere nuestra identificación mediante certificado digital, el certificado será detectado y una vez comprobados nuestros datos podremos acceder al sitio.

Mediante el proceso citado, podríamos hacer multitud de gestiones por Internet evitando tener que acudir físicamente a los sitios, hacer colas y demás inconvenientes que conlleva el método tradicional. Algunos ejemplos son: consultar la vida laboral, entregar la declaración de la renta, etc.

En cualquier caso, este no es el único fin de los certificados digitales. La otra cara de la moneda está en verificar la identidad de los sitios web. Como sabes, hoy en día, uno de los delitos más típicos en la red es el Phishing. Una de las principales formas de evitarlo es comprobar la identidad de los sitios mediante los certificados digitales.

Autoridades de Certificación.

Llegado a este punto ya sabes lo que es un certificado digital, pero aún hace falta tener en cuenta otra cuestión: ¿cómo se verifica la asociación entre el certificado digital y una persona física? Es decir, si descargásemos el certificado por Internet necesitaríamos algo precisamente similar al propio certificado para verificar quien somos y así poder descargarlo. Como esto no es posible ya que todavía no tenemos el certificado, hará falta que **una tercera parte de confianza**, verifique nuestra identidad. Aquí es donde entran las llamadas **autoridades de certificación**.

Es posible que todavía no te haya quedado del todo claro en qué consisten y por qué son necesarias las autoridades de certificación. Pues bien, pongamos un ejemplo: cuando vas a sacar o renovar el **DNI** (Acrónimo. DNI = Documento Nacional de Identidad), no es posible comunicarte con una autoridad emisora directamente para que te envíen el DNI sin ningún trámite adicional. Tendrás que acudir físicamente a las oficinas de los organismos competentes para que un funcionario o funcionaria verifique que realmente eres la persona física a la que se asocia la identidad, comprobar la huella dactilar, la fotografía, etc. De lo contrario, alguien podría hacerse pasar por ti. Es por esta razón por la que podemos confiar en que un DNI se corresponde con la persona física, porque está **avalado por una tercera** parte de confianza, en este caso la policía.

Con un certificado digital pasa lo mismo. Necesitamos que esté avalado por una tercera parte de confianza, en este caso, una autoridad de certificación. Por lo tanto una **autoridad de certificación es una institución que garantiza que un certificado digital pertenece a una persona física concreta.**

¿Recuerdas que en el anterior epígrafe decíamos que el certificado digital contiene, entre otras cosas, la firma digital de una autoridad de certificación? Pues precisamente esa es la manera de dejar constancia de que dicho certificado está avalado por la autoridad de certificación que lo firma (digitalmente).

Existe una especie de jerarquía de autoridades de certificación, de forma que, grandes autoridades certifican a otras para poder emitir certificados. De todos modos, en última instancia quien emite los certificados en España, es la Fábrica Nacional de Moneda y Timbre. Otro ejemplo de autoridad muy conocida, en este caso Americana, es Digicert.

Para saber más

En el siguiente enlace podrás ampliar la información respecto a las autoridades de certificación.

Autoridades de certificación (Wikipedia).

Obtener un Certificado Digital en España.

Ahora que ya sabes lo que es un certificado digital pasemos a la práctica. Vamos a ver los pasos que debemos seguir para **solicitar** un certificado digital **personal**.

En primer lugar vamos a ver los pasos a seguir para **solicitar un certificado digital** personal:

1. Conectarse a la página de CERES e introducir nuestro DNI. Posteriormente se nos **proporcionará un código.**
2. Ir con el código recibido y nuestro DNI a una **oficina de registro autorizada**, por ejemplo, la seguridad social. Una vez comprobada nuestra identidad deberemos **firmar la solicitud.**
3. Una vez realizados los dos pasos anteriores podemos volver a acceder a la página para **descargar el certificado.**

Debes conocer

En el siguiente enlace puedes ver un vídeo de CERES acerca del certificado digital.

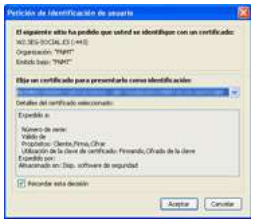
http://www.youtube.com/embed/p19J0TOplks

En el siguiente enlace verás un tutorial donde se explica paso a paso como importar tu certificado digital en Windows 10 en Google Chrome.

Instalar el certificado digital en tu ordenador

http://www.youtube.com/embed/gFLppbP-2Ks

Cuando tenemos el certificado de usuario instalado y entramos en un sitio que lo requiere, automáticamente será detectado por el navegador. Veremos una ventana similar a la siguiente:



Otra opción que existe para almacenar un certificado digital, son las tarjetas criptográficas. Dicha tarjeta no es más que una tarjeta que incluye un chip donde se almacenará nuestro certificado. Lógicamente, si tenemos el certificado almacenado en dicho soporte, necesitaremos un lector de tarjetas similar al de la siguiente imagen para emplearlo.

Herramienta GPG en Linux.

Caso Práctico

En el departamento de marketing es frecuente intercambiar propuestas, ideas y proyectos, tanto a nivel interno como con la dirección de la empresa u otros departamentos.

Desgraciadamente, en dicho departamento no reina un buen ambiente debido a la gran afluencia de empleados y empleadas, a las nuevas incorporaciones y también a la alta competividad que genera trabajar por comisiones. Últimamente, se han dado varios casos de falsificación de documentos y suplantación de identidad.

José García, como portavoz de dicho departamento, se reúne con Ignacio para tratar de buscar una solución:

-Como sabes, en nuestro departamento ya se han dado casos en los que se ha suplantado la identidad de otro empleado. Este hecho es realmente grave y, además, el mal ambiente que se está creando no ayuda en absoluto al buen funcionamiento del departamento –explica José.

-Entiendo –Asiente Ignacio- En vuestro departamento trabajáis con Linux, ¿verdad?

-Sí, efectivamente. ¿Será un problema para llevar a cabo una solución? –Pregunta José preocupado.

-No, en absoluto. Os propongo que utilicéis GPG que es una herramienta gratuita.

-Me hablas en chino Ignacio… ¿eso va a solucionar nuestro problema?

-Sí, no te preocupes. Podemos organizar un pequeño seminario para formar a los empleados y empleadas del departamento en el manejo de la herramienta.

-Genial, yo soy el primero que no tengo ni idea del tema, así que perfecto.

-No te preocupes, verás como es más sencillo de lo que parece. A través de esta herramienta, tendréis un sistema de claves mediante el cual podréis firmar documentos asegurando la identidad de la persona que envía dicho documento. También podréis mandar la información confidencial cifrada, etc.

-Pues perfecto, ya nos explicarás con más calma entonces.

-Está hecho.

-Muchas gracias Ignacio, me dejas más tranquilo.

-No hay de qué.

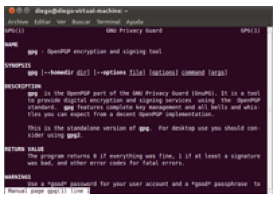
GnuPG, en un sistema de clave pública de código abierto y gratuito. En este caso vamos a ver cómo utilizar algunas de su instrucciones sobre una distribución GNU/Linux, pero también podríamos utilizarlo sobre Microsoft Windows.

Comandos para el Cifrado Simétrico.

A lo largo de este epígrafe conocerás las principales instrucciones de la herramienta GPG de Linux. Para abrir el terminal de línea de comandos en Ubuntu, vamos a Aplicaciones > Accesorios > Terminal.

En primer lugar, es conveniente que conozcas como consultar la ayuda. Un comando muy útil es:

```
man gpg: ayuda
```



- Para **cifrar** un documento con clave simétrica se introduce el comando y posteriormente nos pide una cadena de texto que utilizará como clave simétrica. El resultado será un fichero cifrado cuyo nombre será el mismo que el fichero fuente, pero con extensión **gpg**.

```
gpg -c Documento
```

Debes tener en cuenta que si tu **directorio activo** no es el directorio del documento, debes escribir la ruta completa (por ejemplo, Escritorio/Documento.txt).

Si bien el cifrado simétrico es menos seguro que el cifrado asimétrico, en ocasiones, puede resultar útil cuando necesitamos compartir un documento con un gran número de personas, a las cuales puede incluso que no conozcamos. En estos casos es importante compartir la clave utilizando un método seguro.

Añadiendo el parámetro **–a** la salida será ASCII (archivo extensión .asc).

- Para **descifra** un documento con clave simétrica, lógicamente, tendremos que introducir la clave con la que fue cifrado. Debes fijarte en que, en este caso, el nombre del documento no es el mismo que en el caso anterior. En este caso, el documento que queremos descifrar, será el documento que está cifrado y, por lo tanto, tendrá extensión gpg.

```
gpg -d Documento
```

Si se ejecuta con éxito, se mostrará el contenido del fichero.

Ejercicio resuelto

Vamos a poner en práctica lo que acabamos de ver. El ejercicio consiste en cifrar y descifrar un fichero de texto con clave simétrica en Ubuntu.

Mostrar retroalimentación

En primer lugar creamos un fichero de texto llamado Documento.txt en el Escritorio. Abrimos el documento y escribiremos cualquier cosa para dotarlo de contenido. Guardamos el documento.

Abrimos el terminal de línea de comandos y tecleamos la siguiente instrucción: gpg -c Escritorio/Documento.txt

Nos pide una contraseña, tecleamos cualquier contraseña que recordemos fácilmente (para probar el ejercicio no es necesario que sea complicada), por ejemplo “hola”.

Si todo ha ido correctamente, podemos ver que se ha generado en el escritorio un fichero llamado **Documento.txt.gpg.**

Ahora solamente nos queda descifrar el documento. Para esto, tecleamos la siguiente instrucción: **gpg -d Escritorio/Documento.txt.gpg**

Por último, nos pedirá la contraseña que introducimos cuando ciframos el documento. Después de introducirla, se mostrará el contenido.

Comandos para el Cifrado Asimétrico (de Clave Pública).

Para obtener un par de claves (pública y privada, utilizamos la siguiente instrucción:

```
gpg --gen-key
```

Tras introducir la instrucción, nos pedirá los siguientes parámetros: tipo de clave (podemos elegir la RSA por ejemplo), tamaño de la clave (ten en cuenta que cuanto mayor sea, será más segura, pero también tardará más tiempo la operación), periodo de validez, identificador de usuario, un comentario (opcional) y contraseña para proteger la propia clave. Aunque en los ejercicios de prueba no será algo importante, esta clave no debe ser tan trivial como, por ejemplo, tu nombre ya que es la única forma de asegurarte que nadie utilizará tu clave privada para hacerse pasar por ti, en caso de que llegue a manos no deseadas.

Es recomendable no utilizar tildes en el identificador ni en el comentario opcional que podemos hacer.

Añadiendo el parámetro **"–a"** la salida será ASCII (archivo extensión **.asc**)

La siguiente orden, muestra un listado de las claves del usuario, lo que se conoce como **anillo de claves**.

```
gpg -k
```

En este caso, vamos a exportar la clave pública al archivo salida.gpg (utilizando la orden output podríamos darle el nombre que quisiéramos). De esta forma, la clave pública puede ser compartida con otros usuarios.

```
gpg --output salida.gpg --export Usuario
```

El fichero salida.gpg con la clave se guardará por defecto en la carpeta del usuario.

Para compartir posteriormente esta clave pública tenemos varias posibilidades: enviarla por correo electrónico, subirla a un servidor de claves, "colgarla" en una página Web, etc.

Si exportamos la clave y la compartimos con otro usuario, éste tendrá que importarla para incluirla en su anillo de claves. El siguiente comando importa la clave pública de un archivo (salida.gpg). De esta forma se añade dicha clave al anillo de claves del usuario.

```
gpg --import salida.gpg
```

Ahora crearemos un documento firmado digitalmente a partir del documento fuente (el documento a firmar no es cifrado). Necesitaremos introducir la clave para **desbloquear la clave**. Genera un fichero con extensión .gpg que no será directamente legible. Para restaurarlo necesitaremos la clave pública de la persona que lo ha firmado.

```
gpg --sign Documento
```

Cuando el destinatario recibe el documento firmado, solamente tendrá que ejecutar el siguiente comando sin parámetros para restaurar el documento original y comprobar la firma. De esta forma se asegura que el mensaje no ha sido alterado desde que se firmó, de lo contrario, no sería posible su restauración

```
gpg Documento
```

Para saber más

A continuación dispones de un manual de GPG donde podrás ampliar la información al respecto y encontrar muchas más instrucciones.

Manual GnuPG.

Tambien en este enlace puedes encontrar las recomendaciones del Centro Criptográfico Nacional para cifrar y firmar mensajes de forma correcta, empleando GnuPG y una variante gráfica para Ubuntu y Windows.

Recomendación CCN-Cert sobre Firma y Cifrado

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: Plan de Alfabetización Tecnológica Extremadura Licencia: cc by-nc-nd Procedencia: http://www.flickr.com/photos/patextremadura/4643852621/		Autoría: nearsoft Licencia: CC BY-NC-SA Procedencia: http://www.flickr.com/photos/nearsoft/3704855174
	Autoría: 24gotham Licencia: CC BY-NC-ND Procedencia: http://www.flickr.com/photos/iconeon/2419133069/		Autoría: Iago A.R. Licencia: CC BY-NC-ND Procedencia: http://www.flickr.com/photos/eseartista/1101947771/
	Autoría: anvica Licencia: CC BY-NC-ND Procedencia: http://www.flickr.com/photos/anvica/2947233762/		Autoría: Frandj Licencia: CC BY-NC Procedencia: http://www.flickr.com/photos/frandj/19783051/
	Autoría: KingRobertII Licencia: CC BY-SA Procedencia: http://www.flickr.com/photos/photobyrk/5705842096		Autoría: tonyhall Licencia: CC BY-NC-SA Procedencia: http://www.flickr.com/photos/anotherphotograph/295590995
	Autoría: Diego Méndez Licencia: GPL Procedencia: Captura de pantalla de Firefox		Autoría: Rickydavid Licencia: cc by-nc-nd Procedencia: http://www.flickr.com/photos/cuppini/4476516098/
	Autoría: driusan Licencia: CC BY-NC Procedencia: http://www.flickr.com/photos/driusan/2472706272/		Autoría: Diego Méndez Licencia: GPL Procedencia: Captura de pantalla en Ubuntu
	Autoría: Die Stimme der freien Welt Licencia: CC BY-SA Procedencia: http://www.flickr.com/photos/dsdfw/382736757		

Funciones ‘hash’.

Como sabes, hasta ahora hemos visto como podemos conseguir confidencialidad, autenticación y no repudio. Aún queda un paso más que lograr: la **integridad del mensaje**. Con integridad nos referimos a la capacidad de asegurar que el mensaje no sea alterado durante su transmisión.

Esto es posible mediante las **funciones hash**, también llamadas funciones resumen. Una función hash, es un algoritmo que se aplica sobre el mensaje y **produce un código** de longitud fija que es un **“resumen”** del mismo.

La función puede ser tan simple como contar el número de unos del mensaje o mucho más compleja y producir un número de 128 bits resultado de contar el número de 0, el de 1, el de 00, el de 11, y así sucesivamente. En cualquier caso, una función hash, debe tener al menos **dos características** deseables:

- Que existan pocas probabilidades de que varios documentos generen el mismo valor resumen.
- Debería ser prácticamente imposible generar un documento que genere un valor resumen determinado.

Por todo ello, los algoritmos que se utilizan en la práctica son bastante complejos desde el punto de vista matemático. Hay funciones estándar, como MD4 (Acrónimo. MD= Message-Digest Algorithm 4) y MD5 (Acrónimo. MD= Message-Digest Algorithm 5), que producen números de 128 y 160 bits respectivamente.

Su funcionamiento cuando enviamos un mensaje cifrado es el siguiente: antes de cifrar el mensaje, se le añade el número obtenido de aplicarle este algoritmo. El receptor, tras descifrar el mensaje original, le volverá a aplicar la función y comprobará que el número obtenido coincide con el que recibió. Esto garantiza que el mensaje no ha sido alterado.

Otro uso típico de las funciones resumen es utilizarlas para **almacenar los valores resumen de las contraseñas**. Lo que se pretende con esto, es evitar guardar los valores en claro por seguridad. Además, de esta forma tenemos una solución para comprobar las contraseñas. Por ejemplo, en Linux, se almacenan los valores resumen de las contraseñas en el fichero **etc/passwd.**

Cuando **se firma digitalmente** un documento, se utiliza una función **resumen** del documento firmado en la firma electrónica. Gracias a dicho valor resumen, la firma, no sólo permite identificar a un individuo, sino que la firma será única para cada documento concreto que éste firme.

Para lograr todos los aspectos de seguridad mencionados al principio (salvo el de privacidad), se usará conjuntamente **criptografía de clave pública**, **funciones resumen** y **firmas digitales**.

Debes conocer

En el siguiente vídeo puedes ver un vídeo en el que se ve de forma muy gráfica todo el proceso de la firma digital que acabamos de ver.

Vídeo sobre la firma electrónica.

PKI.

PKI son las siglas de las palabras en inglés Public Key **I**nfraestructure, que podemos traducir como "**I**nfraestructura de Clave Pública". Cuando hablamos de infraestructura de clave pública, nos referimos a todo el conjunto de protocolos, servicios y estándares necesarios para utilizar los diferentes sistemas basados en criptografía de clave pública como los certificados y las firmas digitales.

Teniendo esto en cuenta, las PK**I**, están compuestas por:

- Autoridades de **certificación**.
- Autoridades de **registro**.
- **Otro** tipo de autoridades como las de los repositorios donde se almacenan los certificados emitidos, las autoridades de fechado digital, etc.
- Todo el **software asociado**, así como las políticas de seguridad utilizadas en estos sistemas.

Para saber más

En el siguiente enlace podrás ampliar la información acerca de la infraestructura de clave pública. Dicho enlace corresponde a la entrada al respecto de la Wikipedia.

Entrada en Wikipedia sobre PKI.

En el siguiente vídeo verás como instalar un certificado digital de servidor en un **I**nternet **I**nformation Server. Una vez instalado se podría comprobar a través de la página Web que muestra de ejemplo.

Vídeo-tutorial.