Diseño web funcional.Prevención y buenas prácticas: Principios de la seguridad informática

En este tema te presentamos algunos conceptos básicos acerca de la seguridad informática.

Es importante que importante que te empieces a familiarizar con algunas de las principales amenazas y con distintos mecanismos para implementar la seguridad de los datos y de los sistemas.

Recuerda que si quieres ser un buen informático debes saber proteger el sistema del que eres responsable de fallos y ataques.

1. ¿Qué es la seguridad informática?

Imagen en flickrcc de www.elbpresse.de bajo licenciaAlgunos derechos reservados

Hoy en día es difícil concebir una empresa que no posea ordenadores y una conexión a Internet. Y no solo empresas, sino también a nivel particular como herramienta de ocio o trabajo. Las empresas basan gran parte de su actividad en datos almacenados en equipos informáticos o en datos e información que viaja por la red.

Por un lado será importante garantizar que la información almacenada no se pierda,se degrade o se altere de forma incorrecta (**seguridad**) y por otro, el garantizar que datos de carácter personal o privados por la actividad de la empresa sean accesibles por personas no autorizadas (**privacidad**).

Ofrecer protección frente a estos dos tipos de vulnerabilidad es de suma importancia, tanto para la actividad y funcionamiento de organismos y empresas como para individuos particulares.

¿Qué sientes cuándo se te estropea el disco duro de tu equipo y pierdes todas tus fotos de los últimos 5 años?, ¿y si alguien suplanta tu identidad y accede a tus datos bancarios? , ¿y si tu empresa rival accede a tus datos con los diseños de los últimos prototipos que aún no habéis lanzado?.

Para saber más

El acceso a datos privados y la suplantación de identidad son delitos penados por la ley.

Todo este tipo de delitos que se realizan contra sistemas informáticos o a través de ellos , se conocen como cibercrimen y existe una unidad de la Guardia Civil encargada de su investigación.

Grupo de Delitos Telemáticos (G.D.T): si tienes curiosidad en esta página se describe su actividad, así como algunas normas básicas de seguridad y se proporcionan una serie de formularios para denunciar o informar de posibles delitos telemáticos.

2. Objetivos de la seguridad informática

Imagen en Flickrcc de Avi Dolgin

bajo licencia Algunos derechos reservados

Según el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC):

"La **seguridad informática** consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la **confidencialidad**, la **integridad** y la **disponibilidad** de la información, pudiendo, además, abarcar otras propiedades, como la **autenticidad**, la **responsabilidad**, la **fiabilidad** y el **no repudio**."

El principal objetivo será garantizar:

- La **confidencialidad** de la información: que nadie no autorizado pueda verla.
- La **integridad** de la información: que nadie no autorizado pueda modificarla y alterarla.
- La **disponibilidad** de la información: que quien esté autorizado pueda acceder a ella siempre y consultarla.

2.1. Confidencialidad

Según la Real Academia de la Lengua Española, se dice que algo es confidencial cuando "se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho".

El objetivo de la confidencialidad es pues impedir la divulgación no autorizada de la información.

Si pensamos en nuestros datos personales o los datos que enviamos por la red al realizar una operación bancaria, está claro que deseamos que esos datos solo sean vistos por nosotros y el receptor autorizado (p.ej. aplicación web de nuestro banco online), pero por nadie más, no deseamos que está información que viaja por la red o que está almacenada en una base de datos, sea interceptada por alguien no autorizado y que sea capaz de acceder a la información.

De la misma forma las empresas guardan y transmiten información sensible, por ejemplo, de nuevos productos que aún no han salido a la venta, que en el caso de caer en casos de la competencia, podría arruinar a la empresa.

Más delicada incluso puede ser la información militar que en caso de caer en manos de otros países podría poner en peligro la seguridad de toda una nación.

La **criptografía** es una técnica que nos permite cifrar o encriptar la información, de forma que si alguien accede a ella no sea capaz de descifrarla. Sin embargo aquí nos encontramos con el problema de la clave criptográfica, que habrá que proteger, puesto que si alguien la obtiene, podrá descifrar y entender los datos interceptados.

2.2. Integridad

Imagen en Flickrcc de RaHuL Rodriguez bajo licencia algunos derechos reservados

Para garantizar la **integridad** de la información, la seguridad informática debe buscar la forma de mantener los datos libres de modificaciones no autorizadas. Si alguien no autorizado, por error, accidente o con mala intención, modifica o borra parte o la totalidad de la información, se habrá producido un fallo en la seguridad.

Las modificaciones solo deben poderse realizar por parte de personal autorizado, y serán registradas para asegurar la confiabilidad de los datos.

Una mecanismo para garantizar la integridad es añadir al mensaje o datos de origen un conjunto adicional de datos de comprobación, de forma que si durante la transmisión del mensaje alguien no autorizado lo modifica, en el destino lo sabremos gracias a esos datos adicionales. Es lo que se conoce como **firma digital**.

2.3. Disponibilidad

La **disponibilidad** debe garantizar que los usuarios autorizados tengan acceso a los datos siempre que lo requieran. Deben de poder acceder al sistema para consultar, modificar o insertar información (según tipo de autorización y permisos).

Para ello los sistemas deben mantenerse funcionando de forma correcta y que se recuperen de forma eficiente ante posibles fallos.

Cuando un usuario autorizado no pueda acceder al sistema, diremos que este no está disponible.

Existen sistemas críticos que si dejan de funcionar pueden ocasionar pérdidas muy importantes. Para este tipo de sistemas se desarrollan mecanismos que garanticen que estarán operativos en porcentajes cercanos al 100%. Se diseñan y configuran de forma que el tiempo en que están parados o caídos sea mínimo. Es lo que se conoce como **alta disponibilidad**.

La disponibilidad se mide por el indice de disponibilidad que es el tiempo en que el sistema está totalmente operativo dividido entre el tiempo total. Los índices cercanos al 100% indicarán que los sistemas y sus datos y procesos han estado disponibles casi de forma continua.

Imagen en flickrcc de TNS Sofres bajo licencia Algunos derechos reservados

- **Autenticación:** permite validar la identidad del emisor. Verificando que es quien dice ser. El método más conocido es el de controlar el acceso mediante usuario y contraseña. Existen otros métodos más seguros como el certificado digital, tarjetas magnéticas, huella dactilar, reconocimiento facial, etc..
- **Autorización**: controla el acceso de los usuarios a información, equipos o procesos restringidos, tras pasar un proceso de autenticación. Deberemos definir sobre qué puede actuar, cuándo puede actuar y cómo puede hacerlo (p.ej. acceso a ficheros en modo de solo lectura o lectura/escritura, acceso a bases de datos con permisos de inserción, borrado o modificación, etc.) Siempre será más recomendable dar autorizaciones más restringidas y abrirlas cuando sea necesario, que dar autorizaciones muy abiertas que pueden comprometer la seguridad del sistema en caso de accesos con permisos inadecuados, bien intencionadamente o bien por error.
- **Auditoría**: debemos llevar un control sobre los sistemas y servicios que nos permita determinar qué acciones se han llevado a cabo y quién y cuándo las ha llevado a cabo. Periódicamente se revisará está información para analizarla y sacar conclusiones que permitan detectar posibles fallos de seguridad o mejorar los procedimientos.
- **No repudio**: mecanismo para asegurar que nadie pueda decir que él no fue. El emisor no podrá negar que fue él quien envió el mensaje, puesto que el receptor tendrá pruebas de ello o el receptor no podrá negar que recibió el mensaje porque el receptor tendrá información que lo confirma.

3. Seguridad activa y pasiva

En un vehículo nos encontramos con dos tipos de seguridad:

- La seguridad activa, que es la que trata de evitar que se produzca un accidente, como pude ser el sistema de frenado o la adherencia de los neumáticos.
- Y la seguridad pasiva, que trata de minimizar los daños una vez que el accidente ya se ha producido o es inevitable, como pueden ser los cinturones de seguridad o airbags.

En seguridad informática nos encontramos con algo parecido. Por un lado la **seguridad activa**, que tratará de prevenir y evitar que ocurran daños en los sistemas informáticos, y por otro lado, la **seguridad pasiva** que tratará de minimizar los efectos causados por un accidente, un error o un ataque.

3.1. Técnicas de seguridad activa

Estas técnicas intentan evitar y prevenir los daños en sistemas informáticos. Algunas de ellas son:

Técnicas	¿Qué previenen o evitan?
Contraseñas seguras	Previene el acceso a recursos a personas no autorizadas
Encriptación	Los datos a proteger se cifran usando una clave de cifrado, de forma que las personas que no conozcan la clave no puedan interpretar esos datos.
Software específico (antivirus, antiespías, cortafuegos, etc.)	Previenen frente a los virus informáticos y entradas indeseadas al sistema.
Firma digital y certificado digital	Permiten verificar el origen de los datos, su integridad y su autenticidad

3.2. Técnicas de seguridad pasiva

Estas técnicas intentan minimizar los daños causados por un percance, error o ataque sobre el sistema informático. Algunas de estas técnicas son:

Técnicas	¿Cómo minimizan?
Instalaciones adecuadas (conexiones eléctricas, refrigeración del sistema, etc.)	Minimizan posibles fallos en el hardware por calentamiento, por sobrecarga en la línea eléctrica, etc.
SAI (Sistema de Alimentación Ininterrumpida)	Estos dispositivos proporcionan energía eléctrica almacenada en sus baterías durante un tiempo limitado ante un apagón. Otras de sus posibles funcionalidades es la de mejorar la calidad de la energía eléctrica, filtrando frente a subidas y bajadas de tensión.
Conjunto de discos redundantes (RAID, Redundant Array of Independent Disks)	Nos permiten restaurar información que no es válida o consistente a partir de la repetición de los datos en distintos grupos de discos.
Copias de seguridad	Copias de los datos en distintos soportes físicos y en distintas ubicaciones físicas.

4. Seguridad física y lógica

Imagen en flickrcc de CEBImagery

Se pueden clasificar los mecanismos de seguridad atendiendo a si protegen el hardware o el software.
Aquellos mecanismos que protegen el hardware o medio físico en que se ubica el sistema frente a amenazas que pueden ser causadas por el hombre o por la naturaleza, se conocen como **seguridad física**.
Los mecanismos que protegen el software, es decir, aplicaciones y datos frente a posibles amenazas serán los que implementen la **seguridad lógica**.

Para saber más

- **Hardware** (Wikipedia)
- **Software** (Wikipedia)

4.1. Seguridad física

La seguridad física, como ya hemos dicho es la que trata de proteger el hardware frente a posibles amenazas. En la siguiente tabla se recogen algunas de estas amenazas:

Amenaza	Mecanismos de protección
Incendios	● Mobiliario ignífugo en CPD (centro de procesos de datos). ● Mecanismos antiincendios (detectores, extintores, etc..) ● No estar cerca de material inflamable
Inundaciones	● No ubicar los servidores en salas subterráneas con riesgo de inundación. ● Sistemas de evacuación de agua. ● Impermeabilización y sellado de posibles vías de entrada de agua
Robos	● Vigilante ● Cámaras de seguridad ● Sistemas de control de acceso
Sobrecargas y apagones	● SAI (Sistemas de alimentación ininterrumpida).
Caídas en la línea	● Línea de backup.
Otros desastres naturales (terremotos, maremotos, etc..)	● Consultar datos meteorológicos. ● En áreas con alta probabilidad de movimientos sísmicos, edificaciones preparadas para ello.

4.2. Seguridad lógica

La **seguridad lógica** trata de proteger las aplicaciones o programas y los archivos y datos frente a distintas amenazas, mediante distintas medidas de seguridad. En la siguiente tabla puedes ver algunas de estás medidas:

Amenaza	Mecanismos de protección
Modificaciones no autorizadas	• Restringir el acceso a programas y archivos mediante contraseñas. • Limitar permisos de forma que los usuarios no puedan modificar por error o intencionadamente programas ni archivos. • Listas de control de acceso. • Cifrado de la información.
Ataques desde la red (Internet o red local)	• Firewalls. • Servidores Proxys. • Sistemas de monitorización de la red. • Listas de control de acceso (por IP p por MAC).
Pérdidas de información	• Copias de seguridad. • Sistemas tolerantes a fallos. • Discos redundantes.
Virus	• Programas antivirus que eviten que estos programas malintencionados se instalen en los equipos.
Suplantación de identidad	• Contraseñas • Sistemas de reconocimiento (voz, digitales, faciales, etc.) • Certificados

5. Seguridad de contraseñas

Imagen en flickrcc de GNOME Seahorse

Es fundamental el controlar que cualquier persona que acceda al sistema esté autorizado y que solo pueda acceder a los recursos para los que tiene autorización.

Una de las formas más usuales de autorizar los accesos es mediante un usuario y contraseña (o password) y asociando a dicho usuario una serie de permisos (qué acciones podrá realizar y cuáles no y sobre qué recursos).

RECOMENDACIONES PARA LA ELECCIÓN DE CONTRASEÑA

No es recomendable elegir contraseñas que por ser fáciles de recordar, sean también fáciles de averiguar, no se recomienda nuestra fecha de nacimiento, NIF, nombre, nombre de nuestra mascota, nombre de algún familiar, etc.

Existen además ataques por diccionario o fuerza bruta que que se dificultan si se siguen algunas normas como longitud mínima o caracteres especiales.

Algunas normas básicas a la hora de elegir nuestra contraseña son:

- No elegir palabras relacionadas con nuestro entorno (NIF, nombre de nuestra mascota, fecha de nacimiento, nombre de tu hijo, etc.)
- Usar combinaciones de letras, números y caracteres especiales (no usar palabras con significado).
- Longitud mínima de 8 caracteres.
- Intentar usar contraseñas distintas para servicios distintos.
- No usar nunca la contraseña por defecto, cambiarla en el primer acceso.

Para recordar una contraseña segura (mínimo 8 caracteres que incluyan números, letras y caracteres especiales) podemos recurrir al truco de usar una frase, por ejemplo: ¿Yo nací en febrero de 1980?, y quedarnos con los dos últimos caracteres de cada palabra: Yocíenrode80?

Obviamente, ninguna de estas precauciones será de utilidad si después anotamos la contraseña en un postit y la pegamos en la pantalla de nuestro ordenador. Las contraseñas deben almacenarse de forma segura (existen programas **gestores de contraseñas**) y tener cuidado en su distribución, cómo y a quién se facilita, como norma general una contraseña es de uso privado, por lo que no se debe facilitar a nadie. En caso necesario, debemos ser cuidadosos con el medio que usamos y si es necesario cifrar la información , de forma que solo la persona que posea la clave de cifrado pueda recuperar esa contraseña.

MEDIDAS DE SEGURIDAD A IMPLEMENTAR POR EL ADMINISTRADOR DEL SISTEMA

A la hora de configurar nuestros sistemas debemos forzar a los usuarios a tomar ciertas medidas de seguridad con respecto a sus contraseñas:

- Obligar al usuario a cambiar la contraseña inicial en su primer acceso.
- Numero máximo de intentos permitidos, tras el cual el sistema se bloquea.
- Que no se admitan contraseñas de menos de 8 caracteres y que estos obligatoriamente incluyan mayúsculas, minúsculas, números y caracteres especiales.
- Que las contraseñas expiren cada cierto tiempo y haya que cambiarlas, tampoco se permitirá repetir ninguna de las tres últimas.

Para saber más

Imagen en flickrcc de www.elbpresse.de bajo licenciaAlgunos derechos reservados

Existen diversos sistemas para averiguar contraseñas. Algunos de los más conocidos son:

- **Sniffers**: programas que interceptan las comunicaciones de los equipos en una red pudiendo extraer contraseñas de las comunicaciones "escuchadas".
- **Keyloggers**: Programas que capturan las teclas pulsadas.
- **Fuerza bruta:** Programas que prueban todas las combinaciones (cuanto más larga sea la contraseña, más tiempo requieren).
- **Ataque por diccionario:** Programas que usan palabras del idioma del usuario.
- **Suplantación de identidad:** Se trata de engañar al usuario haciéndole creer que es su banco, o alguien conocido, o algún organismo público, para que se le faciliten las claves.

Para saber más

Criptografía proviene del griego, *krypto* significa oculto y *graphos* escribir, es decir, sería algo como escritura oculta.

La criptografía engloba los mecanismo por los cuales un mensaje inicial (texto en claro) se convierte en otro inteligible (texto cifrado) del que se podrá de nuevo obtener el mensaje original, pero sólo en el caso en que se posea la clave.

Los distintos métodos para ocultar o cifrar la información de partida se conocen como **algoritmos de cifrado**.

UN POCO DE HISTORIA

Los primeros mensajes cifrados datan del siglo V a.C, fueron los espartanos los primeros que usaron una técnica de ocultación de mensajes. La técnica consistía en enrollar una cinta en un bastón de un determinado grosor y escribir el mensaje longitudinalmente a bastón, de forma que en cada vuelta de la cinta se iba escribiendo una letra, repitiendo esto para varias filas. Sólo si el receptor poseía el bastón o conocía su grosor para elaborar uno igual, podría enrollar la cinta de nuevo y leer el mensaje, en caso de que el bastón fuera distinto las letras aparecían descolocadas y el texto era inteligible.

Posteriormente, griegos y romanos usaron otros métodos de cifrado. Los griegos usaban un sistema de sustitución, que consistía en substituir cada letra por un par de letras o números que indicaban su posición en una tabla (fila, columna). La tabla debía ser conocida por el receptor para poder descifrar el mensaje. El método romano consistía en substituir cada carácter por el que estaba tres posiciones más atrás en su alfabeto.

Estos métodos se fueron perfeccionando a lo largo del tiempo, cada vez con algoritmos y claves más complejos, será durante la Segunda Guerra Mundial donde se haga imprescindible el uso de máquinas para el cifrado y descifrado de mensajes, con el fin de proteger la información enviada de los enemigos.

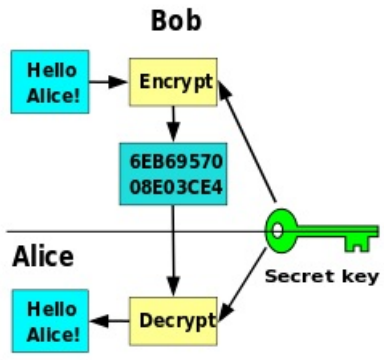
CLASIFICACIÓN

Una primera clasificación de los métodos criptográficos sería:

- **Sistemas de transposición**: los caracteres (grupos de caracteres) del mensaje original se cambian de posición. Podrán ser simples, dobles o múltiples según el número de veces que se realice la transposición.
- **Sistemas de substitución**: Se sustituyen los caracteres del mensaje original por otros (que pueden ser letras, números o incluso imágenes o sonidos).

TIPOS DE SISTEMAS DE CIFRADO

- **Criptografía simétrica:** en la que emisor y receptor comparten una misma clave para el cifrado y descifrado del mensaje.
- **Criptografía asimétrica:** emisor y receptor usan un par de claves, clave pública y clave privada, la clave pública es compartida, pero no así la privada. El emisor cifrará con la clave pública siendo sólo posible el descifrado con la clave privada del receptor.



En este tipo de sistemas el mensaje es cifrado y descifrado con la misma clave privada, que debe ser conocida por el transmisor y por el receptor.

Esto representa un problema pues es necesario encontrar un modo seguro de comunicar la clave entre en emisor y el receptor.

Si el mensaje cifrado es interceptado y no se dispone de la clave, este será inteligible, pero si por cualquier mecanismo el atacante descubre la clave, el sistema de criptografía se habrá roto.

Otro inconveniente es que el emisor debe compartir una clave privada distinta con cada receptor, por lo que si envía mensajes a muchos usuarios distintos será necesario el recordar muchas claves distintas.

VENTAJAS

Son rápidos y eficientes, por lo que resultan adecuados para cifrar grandes volúmenes de datos.

Pueden cifrar bit a bit (**cifrado de flujo**), útiles para cifrar a la vez que se envía la información o por bloques de generalmente 64 bits (**cifrado de bloque**), para volúmenes grandes de información.

INCONVENIENTES

Requieren una clave por cada emisor-receptor.

Requieren un medio seguro de transmisión de la clave.

No son robustos. Pueden romperse por ataques como el de clave relacionada (como ocurre con el cifrado WEP de redes inalámbricas), aprovechando la naturaleza del algoritmo y relaciones entre texto original y claves o por mecanismos de fuerza bruta, que prueban todas las posibles claves (cuanto más larga sea la clave más tiempo se empleará en obtenerla)

Para saber más

ALGUNOS ALGORITMOS DE CIFRADO CON CLAVE SIMÉTRICA

- **DES (Data Encryption Standard)**

Nació en los años 70, divide la información en bloques de 64 bits y los cifra con claves de 64 bits (de los que 56 son los que realmente se utilizan para el cifrado y los 8 restantes son para cálculos de paridad (comprobación de errores)). Es altamente vulnerable y se puede llegar a romper en menos de 24 horas.

- **3DES (TripleData Encryption Standard)**

Se basa en aplicar DES 3 veces. La clave es de 128 bits y se divide en dos de 64 (claves A y B). A la hora de descifrar se aplicará el algoritmo con la clave A, después la B, y de nuevo la A (el algoritmo se aplica 3 veces).

Es más seguro que DES pero más lento y consume más recursos.

- **AES (Advanced Encryption Standard)**

Es el algoritmo empleado por el WPA de las redes inalámbricas. Opera conb claves de 128, 192 o 256 bits. Opera con bloques.

- **RC5 (River Cipher)**

Opera con bloques de tamaño variable 832, 64 o 128 bits) y clave también variable. El número de iteraciones tampoco es fijo, aumentando la seguridad a mayor número de iteraciones.

- **IDEA (International Data Encryption Algorithm)**

Trabaja con bloques de 64 bits y la clave de 128 bits (todos útiles, sin paridad). Igual que DES, IDEA usa el mismo algoritmo para cifrar que para descifrar.

Los sistemas de cifrado por clave asimétrica usan un par de claves: una privada (que solo conoce el propietario) y otra pública (que es la que se intercambia).

En este caso no habrá problemas con el intercambio de la clave (tal y como ocurría en los sistemas de clave simétrica) pues el atacante no podrá hacer nada sólo con la clave pública, necesitaría también la privada (que sólo la tiene el propietario y no se ha intercambiado en ningún momento).

Estos sistemas nos serán de utilidad para dos fines principales:

- **Confidencialidad** (encriptación del mensaje de forma que solo el usuario con la clave privafa adecuada lo pordrá descodificar).
- **Autenticación** (garantizando que el mensaje ha sido emitido por quién dice ser)

Veamos estas dos posibilidades.

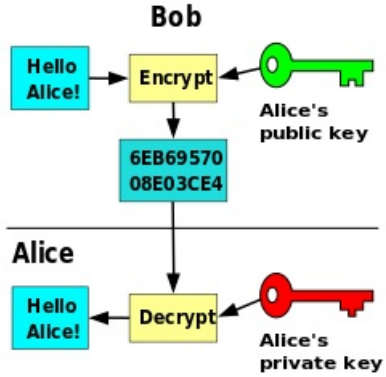


Imagen en WikimediaCommons de Davidgothberg bajo licencia public domain

ENCRIPTACIÓN CON CLAVE ASIMÉTRICA

Bob desea mandar un mensaje a Alice, Bob usará su clave pública (que es de conocimiento general) para encriptar el mensaje. Pero sólo Alice, que posee la clave privada adecuada podrá descifrarlo.

VENTAJAS

La clave privada nunca se distribuye, por lo que no existe el problema de comunicación de la clave que existía en los sistemas con clave simétrica.

Solo he de conocer dos claves (la pública, de conocimiento general, y la privada, que conozco yo exclusivamente), independientemente del número de receptores con los que vaya a intercambiar información (evitamos el problema de elevado número de claves cuando el número de receptores era grande que veíamos en los sistemas de clave simétrica).

INCONVENIENTES

Requieren mayor tiempo de cifrado, los mensajes generados son más grandes, las claves empleadas también son de mayor tamaño para garantizar la seguridad. Por lo que en general requieren más tiempo y recursos que los sistemas de clave simétrica.

Es necesario algún sistema que garantice que la clave pública, que se distribuye libremente, es auténtica (p.ej. **PKI** (Infrestructuras de clave pública) que son las usadas en los DNIe o con los certificados digitales emitidos por la Fábrica Nacional de Moneda y Timbre o las **listas de revocación de certificados**).

Para saber más

ALGUNOS ALGORITMOS DE CIFRADO CON CLAVE ASIMÉTIRCA

- **RSA (Rivest-Shamir-Adelman)**

Este algoritmo se basa en la factorización de números enteros.

Se puede emplear para firmas digitales, pero no permite cifrar la información.

Requiere equipos potentes y más tiempo de cómputo que RSA.

- **DSA (Digital Signature Algorityhm)**

Algoritmo de firma digital del Gobierno Federal de Estados Unidos. Al igual que RSA permite firmar digitalmente, pero no cifrar. Es más lento que RSA pero también más seguro.

- **ElGamal**

Algoritmo de uso libre (no está bajo ninguna patente) que permite tanto firmar como cifrar.

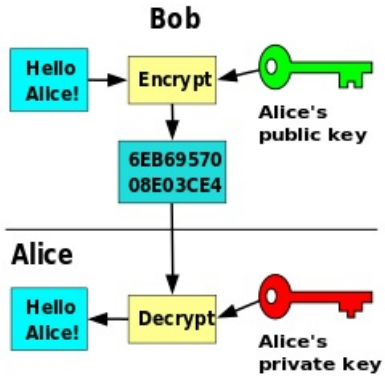
AUTENTICACIÓN CON CLAVE ASIMÉTRICA

Bob desea mandar un mensaje a Alice asegurando que es e´quién lo envía, para ello deberá firmar el mensaje (esta **firma digital**, al igual que una firma escrita, nos indicará que el mensaje es suyo).

Para esto Bob usará su clave privada (que como sólo conoce él, nos asegura que ha sido él quién ha generado la firma).

Normalmente no se cifra el mensaje completo (a menos que también deseemos asegurar su privacidad), lo que se hace es generar una **función resumen** o **hash** a partir del mensaje, y será sólo este resumen lo que encriptemos con nuestra clave privada.

Una vez Alice reciba nuestro mensaje, podrá verificar con su clave pública, mediante la obtención del resumen, que fue Bob quién envió el mensaje.



7. Para ampliar, certificado digital

En los sistemas de clave asimétrica, surge el problema de la clave pública, que está al alcance de todos, con la privada no hay problema puesto que sólo la conoce el propietario.

Hay que asegurar que la clave pública es de la persona correcta y no de un suplantador.

El certificado digital es un documento que contiene información sobre un individuo o entidad (nombre, dirección, email, fecha expiración..etc..),una clave pública, y una firma de un organismo (autoridad certificadora) que garantiza que la clave pública pertenece a quién dice el certificado.

En España el organismo certificador es la Casa de la Moneda y Timbre.

El certificado digital es una herramienta que nos permitirá realizar multitud de trámites telemáticamente (declaración de la renta, vida laboral, cita médica, etc.), gracias a qué garantiza que somos quién decimos ser.

En el siguiente enlace tienes detallado el proceso a seguir para obtener un certificado digital en España:

https://www.sede.fnmt.gob.es/certificados/persona-fisica

EXPORTACIÓN E IMPORTACIÓN DE CERTIFICADOS EN DISTINTOS NAVEGADORES
Aquí tienes una guía para exportar tu certificado del navegador y equipo en el que hiciste la petición (y en el que obligatoriamente debes instalarlo por primera vez) a otros equipos y navegadores.
Te recomiendo que siempre pongas una clave a tu certificado, así en caso de que alguién se haga con él, estarás protegido.
https://www.sede.fnmt.gob.es/preguntas-frecuentes/exp-imp-y-elim-de-certificados

Imagen de creación propia bajo licencia CC

Aviso legal

El presente texto (en adelante, el "**Aviso Legal**") regula el acceso y el uso de los contenidos desde los que se enlaza. La utilización de estos contenidos atribuye la condición de usuario del mismo (en adelante, el "**Usuario**") e implica la aceptación plena y sin reservas de todas y cada una de las disposiciones incluidas en este Aviso Legal publicado en el momento de acceso al sitio web. Tal y como se explica más adelante, la autoría de estos materiales corresponde a un trabajo de la **Comunidad Autónoma Andaluza, Consejería de Educación, Cultura y Deporte (en adelante Consejería de Educación, Cultura y Deporte Andaluza**).

Con el fin de mejorar las prestaciones de los contenidos ofrecidos, la Consejería de Educación, Cultura y Deporte Andaluza se reservan el derecho, en cualquier momento, de forma unilateral y sin previa notificación al usuario, a modificar, ampliar o suspender temporalmente la presentación, configuración, especificaciones técnicas y servicios del sitio web que da soporte a los contenidos educativos objeto del presente Aviso Legal. En consecuencia, se recomienda al Usuario que lea atentamente el presente Aviso Legal en el momento que acceda al referido sitio web, ya que dicho Aviso puede ser modificado en cualquier momento, de conformidad con lo expuesto anteriormente.

1. Régimen de Propiedad Intelectual e Industrial sobre los contenidos del sitio web

1.1. Imagen corporativa

Todas las marcas, logotipos o signos distintivos de cualquier clase, relacionados con la imagen corporativa de la Consejería de Educación, Cultura y Deporte Andaluza que ofrece el contenido, son propiedad de la misma y se distribuyen de forma particular según las especificaciones propias establecidas por la normativa existente al efecto.

1.2. Contenidos de producción propia

Descargar PDF