PROGRAMACIÓN DE SERVICIOS Y PROCESOS

Utilización de técnicas de programación segura

Criptografía. Protocolos criptográficos

Criptografía

La **criptografía** es la técnica que permite cifrar mensajes o hacerlos ininteligibles.

Su funcionamiento consiste en la **utilización de códigos** para escribir datos confidenciales que circulan por Internet o cualquier red en general. Además de lo mencionado, gracias a la criptografía conseguimos:

- ***Preservar la integridad*** *de la web.*
- ***Autenticar*** *al emisor, receptor del mensaje.*
- *Confirmar la* ***actualidad*** *del mensaje o el acceso.*

Criptografía. Protocolos criptográficos

Aplicaciones

- **Cifrar**: permite que los mensajes que se transmiten no puedan ser conocidos por terceras personas. De esta manera **se asegura la privacidad** de la información.
- **Autenticar**: para **demostrar que somos nosotros** y que **el emisor es quien dice ser**. De esta manera es posible cifrar un mensaje con una clave que solo conozcamos nosotros y el receptor podrá confirmar la autoría del mensaje descifrándolo. Para esto se utiliza un sistema de **clave simétrica** en el que el receptor conoce la clave utilizada para el cifrado.
- **Firmar**: Para esto se utiliza un sistema de **clave asimétrica** en el que se cuentan con dos claves, una **privada** y otra **pública**. El **emisor cifra con la clave privada** que solo él conoce y el **receptor utiliza una clave pública** para descifrar.

Criptografía. Protocolos criptográficos

Criptografía

Los **protocolos criptográficos** son protocolos que utilizan algoritmos o métodos criptográficos con el objetivo de conseguir algún objetivo en cuestión de seguridad.

SSL: protocolo que **cifra los mensajes** intercambiados entre emisor y receptor a través de un algoritmo de **cifrado simétrico** y la clave de sesión mediante un algoritmo de **cifrado asimétrico**. Como ventaja presenta que para cada transacción que se realice genera una **clave de sesión distinta** por lo que nos protege de que si esta ha sido obtenida por un usuario no autorizado no pueda utilizarla en transacciones posteriores. Este protocolo garantiza la **confidencialidad e integridad** de los datos intercambiados.

Criptografía. Protocolos criptográficos

Criptografía

SET: protocolo utilizado para **asegurar las transacciones de Internet** en las que se **necesita tarjeta de crédito**. Utiliza **dos pares de claves**, uno para **cifrar la información de la compra** y el otro para **cifrar la información del pago**. Este protocolo garantiza la autenticación del emisor y receptor a través del uso del certificado digital, la confidencialidad de los datos mediante el cifrado y la integridad de la información intercambiada.

PGP: protocolo que cifra el contenido del mensaje a intercambiar entre emisor y receptor. En este caso utiliza algoritmos de **clave simétrica y asimétrica**. Garantiza la integridad de la información, la confidencialidad, la autenticación y no repudio.

IPSec: se trata de un conjunto de protocolos que permiten asegurar las comunicaciones sobre el protocolo IP autenticando y / o cifrando los paquetes IP.

Criptografía. Protocolos criptográficos

Criptografía

La **encriptación de la información** consiste en codificar ésta de manera que si es interceptada por personas no autorizadas no sean capaces de descifrar y tener acceso a la información. Para descrifrar dicha información es necesario una clave que solo deben conocer el emisor y el destinatario de la información.

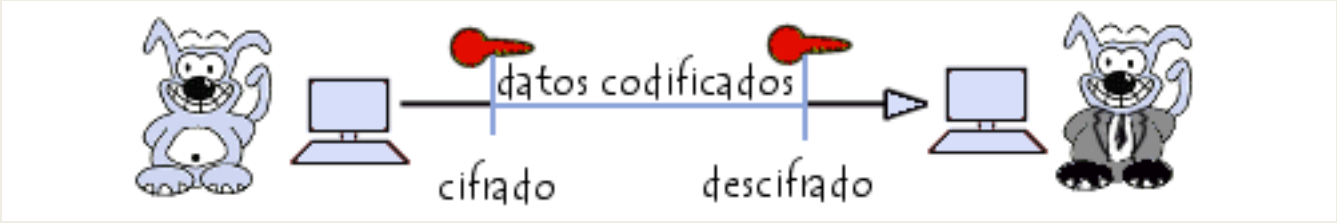
Los principales métodos de encriptación son:

- *Criptografía de* ***clave simétrica***
- *Criptografía de* ***clave asimétrica***

Criptografía. Protocolos criptográficos

Criptografía de clave simétrica

El **cifrado de clave privada o simétrica** consiste en la utilización de **una única clave** para el cifrado y descrifrado del mensaje enviado.



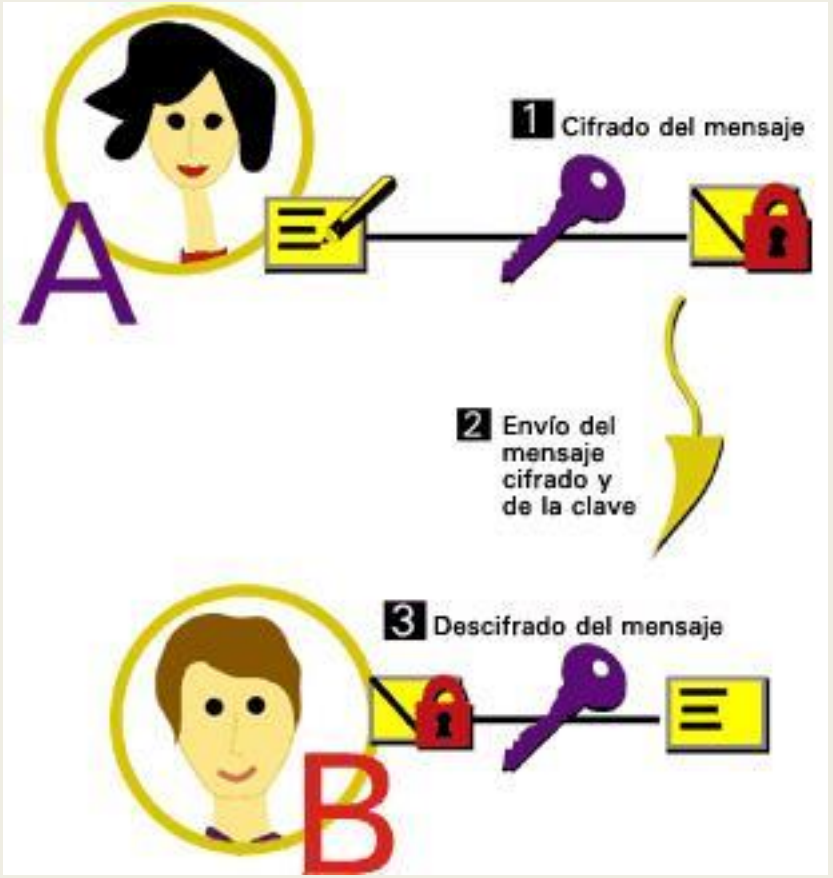
El funcionamiento consiste en aplicar un algoritmo al mensaje a enviar de manera que queda cifrado. El **problema** que se puede encontrar en este cifrado es el hecho de que es necesario el envío del mensaje mediante un **canal seguro**. Además de que si un usuario quiere comunicarse con varios usuarios necesita tener **tantas claves como usuarios destinatarios** de los mensajes.

Criptografía. Protocolos criptográficos

Criptografía de clave simétrica

PROCESO:

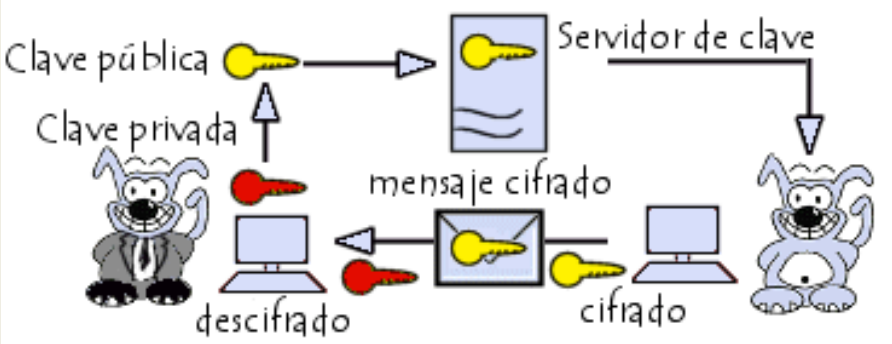
- Ana ha escrito un mensaje para Bernardo pero quiere asegurarse de que nadie más que él lo lee.
- Por esta razón ha decidido **cifrarlo con una clave**. Para que Bernardo pueda descifrar el mensaje, Ana deberá comunicarle dicha clave.
- Bernardo recibe el mensaje y la clave y realiza el descifrado.
- El **beneficio** más importante de las criptografía de clave simétrica es su **velocidad** lo cual hace que éste tipo de algoritmos sean los más apropiados para el cifrado de grandes cantidades de datos.
- El **problema** que presenta la criptografía de clave simétrica es la **necesidad de distribuir la clave que se emplea** para el cifrado por lo que si alguien consigue hacerse tanto con el mensaje como con la clave utilizada, podrá descifrar el mensaje.
- **Por esta razón** se plantea el uso de un sistema criptográfico basado en claves asimétricas, como veremos a continuación.



Criptografía. Protocolos criptográficos

Criptografía de clave asimétrica

El **cifrado de clave pública o asimétrica** consiste en la utilización de **dos claves**, una pública para el cifrado y una privada o secreta para el descifrado.



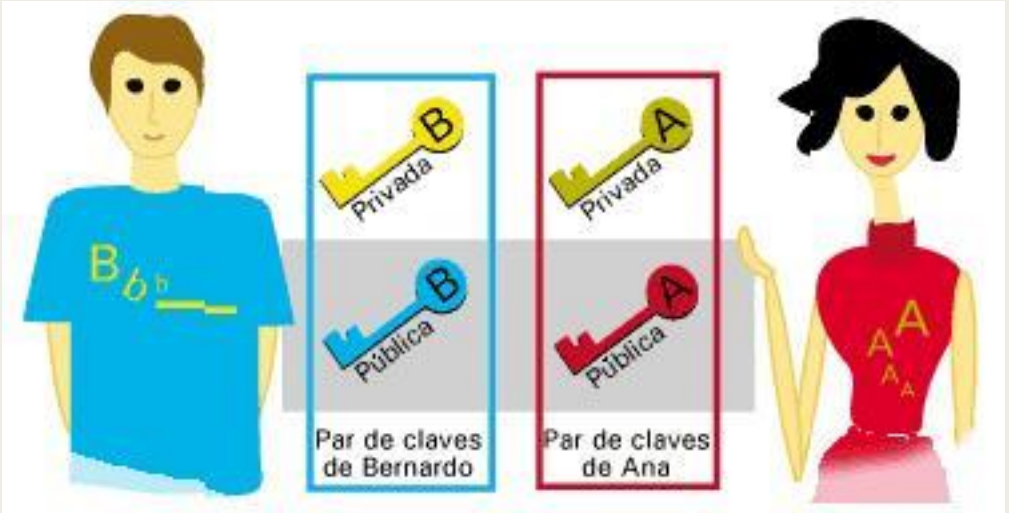
Su funcionamiento es sencillo, un usuario que quiere enviar un mensaje a otro, debe cifrar el mensaje que quiere enviar mediante el uso de la clave pública del destinatario del mensaje. Éste para conocer el mensaje debe descrifrarlo utilizando su clave privada.

Criptografía. Protocolos criptográficos

Criptografía de clave asimétrica

PROCESO:

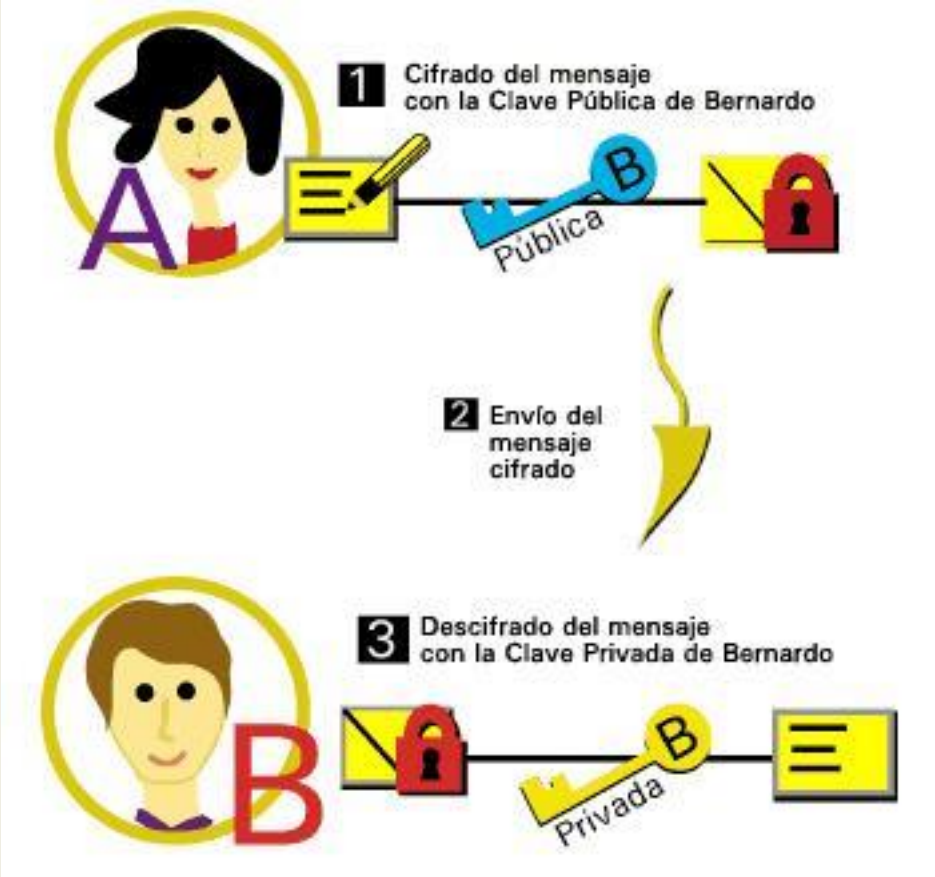
Ana y Bernardo tienen sus pares de claves respectivas: una **clave privada** que sólo ha de conocer el propietario de la misma y una **clave pública** que está disponible para todos los usuarios del sistema.



Criptografía. Protocolos criptográficos

Criptografía de clave asimétrica

- Ana escribe un mensaje a Bernardo y quiere que sólo él pueda leerlo. Por esta razón lo cifra con la clave pública de Bernardo, accesible a todos los usuarios.
- Se produce el envío del mensaje cifrado no siendo necesario el envío de la clave.
- Sólo Bernardo puede descifrar el mensaje enviado por Ana ya que sólo él conoce la clave privada correspondiente.
- El **beneficio** obtenido consiste en la **supresión de la necesidad del envío de la clave**, siendo por lo tanto un **sistema más seguro**.
- El **inconveniente** es la **lentitud de la operación**. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un **algoritmo de clave pública junto a uno de clave simétrica**.



Criptografía. Protocolos criptográficos

Algoritmo HASH

Es un método que permite **generar un número** que representa de manera única a un documento o conjunto de datos. Esta generación se realiza a través de una operación matemática. Hay que destacar que a partir del número obtenido no es posible recuperar el conjunto de los datos originales.

Los principales algoritmos HASH son:

- ***MD5****: se trata de una función hash de 128 bits.*
- ***SHA-1****: función hash de 160 bits.*

Un sistema de control de acceso basado en roles también conocido como **RBAC** por sus siglas en ingles consiste en una función de seguridad que permite controlar el acceso de usuarios a determinadas tareas normalmente restringidas.

Criptografía. Protocolos criptográficos

Control de acceso. Sistemas de control de acceso basado en roles.

Estos sistemas proporcionan las siguientes características:

Autenticación: permite **comprobar la identidad del usuario** que accede a la aplicación. Este proceso se realiza en dos pasos. Primero el usuario se identifica y a continuación se comprueba dicha identificación.

Autorización: permite **definir los privilegios de un usuario** en una aplicación. Normalmente se sigue una de estas estrategias:

- ***Denegar*** *todo desde el principio e ir otorgando permisos según se vaya queriendo.*
- ***Autorizar*** *todo desde el principio e ir denegando aquellas acciones que no queramos que tenga acceso el usuario.*

Auditoria: permite **conservar un historial** de la aplicación donde se almacene quien la ha realizado, cuando, que permisos tienen los usuarios, etc.

Criptografía. Protocolos criptográficos

Protocolos seguros de comunicaciones

Nivel de sesión

- **SSL**: protocolo utilizado para realizar **conexiones seguras** en Internet. Este protocolo cifra los mensajes intercambiados entre emisor y receptor a través de un algoritmo de **cifrado simétrico** y la clave de sesión mediante un algoritmo de **cifrado asimétrico**. Como ventaja presenta que para cada transacción que se **realice genera una clave de sesión distinta** por lo que nos protege de que si esta ha sido obtenida por un usuario no autorizado no pueda utilizarla en transacciones posteriores. Este protocolo garantiza la confidencialidad e integridad de los datos intercambiados.

Criptografía. Protocolos criptográficos

Protocolos seguros de comunicaciones

Nivel de aplicación

- **HTTPS**: protocolo seguro de transferencia de datos basado en el protocolo HTTP antes estudiado. Este protocolo crea un canal cifrado basado en SSL / TSL por lo que es más recomendable para usarlo en la transferencia de contraseñas, datos bancarios, etc que el protocolo HTTP.

- **S-HTTP o Secure HTTP**: protocolo utilizado para realizar transacciones seguras en Internet. Para esto utiliza un sistema de cifrado asimétrico. Hay que tener cuidado de no confundirlo con el protocolo HTTPS que básicamente se traduce como HTTP sobre SSL.

Criptografía. Protocolos criptográficos

Protocolos seguros de comunicaciones

- **S/MIME**: protocolo de seguridad usado para el intercambio de correo electrónico garantizando la confidencialidad y autoría de los mensajes intercambiados. Al estar basado en el protocolo MIME nos permite adjuntar cualquier tipo de archivos en nuestros correos electrónicos. Este protocolo permite cifrar el contenido del mensaje mediante algoritmos de clave pública.

Criptografía. Protocolos criptográficos

Ejercicio

En criptografía, el cifrado es el proceso que permite que los mensajes que se transmiten no puedan ser conocidos por terceras personas. De esta manera se asegura la privacidad de la información. Este proceso realiza la conversión de la representación original de la información en otra forma alternativa conocida como texto cifrado. El objetivo que se persigue es que sólo las partes autorizadas pueden descifrar un texto cifrado para convertirlo en texto plano y acceder a la información original.

Se pide **inventar un método de cifrado** que nos permita cifrar un texto y descifrarlo posteriormente. Este método inventado debe ser distinto al cifrado César. Implementar una aplicación Java que nos proporcione estos dos métodos:

```
public String cifrar(String mensaje);

public String descifrar(String mensaje);
```

Una vez realizada la tarea debes crear un único archivo zip (o rar) que contenga la carpeta del proyecto con todo el código fuente, y un vídeo demostrativo del funcionamiento del mismo.