MEDAC
Instituto Oficial de Formación Profesional

PROGRAMACIÓN DE SERVICIOS Y PROCESOS
TÉCNICO EN DESARROLLO DE APLICACIONES MULTIPLATAFORMA

La criptografía

14

ÍNDICE

© MEDAC 978-84-18864-98-8
Reservados todos los derechos. Queda rigurosamente prohibida, sin la autorización escrita de los titulares del copyright, bajo las sanciones establecidas en las leyes, la reproducción, transmisión y distribución total o parcial de esta obra por cualquier medio o procedimiento, incluidos la reprografía y el tratamiento informático.

OBJETIVOS

Adentrarnos en el mundo de la criptografía y sus principales aplicaciones.

Conocer el modelo de criptografía de clave pública y privada.

Aprender los conceptos de firmas y certificados digitales.

Realizar encriptación de la información mediante funciones HASH.

/ 1. Introducción y contextualización práctica

En esta unidad vamos a tratar el concepto de criptografía, algo muy importante cuando hablamos de la seguridad de la información de nuestras aplicaciones.

Vamos a ver cómo se realiza el proceso de encriptado de la información, además de estudiar los dos modelos más comunes de la criptografía, el modelo de clave privada y el modelo de clave pública.

Por último, vamos a aprender cómo se puede aplicar la criptografía a los programas que desarrollemos mediante las firmas digitales y los certificados digitales, mediante funciones HASH.

Escucha el siguiente audio en el que planteamos el caso práctico que iremos resolviendo a lo largo de esta unidad.

Fig. 1. Criptomonedas

Audio Intro. "La seguridad de los datos"

https://bit.ly/36KJZ9C

/ 2. Concepto de criptografía

La palabra criptografía proviene del griego "cripto", que significa secreto, y "grafía", que significa escritura, por lo que la palabra criptografía significa **escritura secreta**.

La criptografía fue creada y está siendo utilizada (entre otros usos) para poder enviar información confidencial o mensajes privados a ciertas personas u organizaciones.

Los **pasos** a seguir para poder **aplicar la criptografía** a un mensaje son los siguientes:

1. Se **escribe el mensaje 'normal'**, es decir, sin encriptar.

2. Se utilizan **técnicas de encriptado**, más o menos sofisticadas para codifica el mensaje deseado.

3. Se puede enviar el mensaje ya encriptado por **una línea de comunicaciones seguras**, o no seguras. Si estamos en el segundo caso, el mensaje enviado puede ser interceptado. Esto no entrañaría ningún peligro inicialmente, ya que estaría encriptado. No obstante, si el método de encriptación llevado a cabo es conocido o descifrado por el ente que lo intercepta, la información quedaría al descubierto.

4. Cuando el receptor reciba el mensaje, aplicará la **técnica de desencriptado** para poder ver el mensaje original.

Junto a la criptografía podemos destacar el **criptoanálisis**, que es una ciencia que se dedica a estudiar la fortaleza o robustez que tienen los sistemas criptográficos, pudiendo comprobar cómo de seguros son en realidad.

Mediante el criptoanálisis se están mejorando día a día los sistemas criptográficos.

Existen diferentes **tipos de criptografía:**

- Criptografía simétrica.
- Criptografía de clave pública o criptografía asimétrica.
- Criptografía con umbral.
- Criptografía basada en identidad.
- Criptografía basada en certificados.
- Criptografía sin certificados.
- Criptografía de clave aislada.

Los tipos de criptografía más utilizados **en un entorno profesional**, son los de criptografía **simétrica y asimétrica**, que son los que vamos a estudiar más adelante en esta unidad.

Audio 1. "Tecnologías de la seguridad de la información"
https://bit.ly/2Kgaa0c

/ 3. Aplicaciones de la criptografía

Una de las aplicaciones más emergentes de la criptografía, y sobre la que más se puede estar innovando en la actualidad, es el concepto de **la cadena de bloques** blockchain, ya que éste, **utiliza diferentes tipos de criptografía para garantizar la seguridad de las transaccione**s.

En primer lugar, se utiliza el tipo de **criptografía HASH**, mediante la cual, se pueden convertir grandes cantidades de información en una combinación de letras y números única, y muy difícil de imitar. Con esto queremos decir que básicamente se van a resumir enormes cantidades de información, pudiéndose comprobar rápida y fácilmente, que todos los procesos realizados por los nodos de la *blockchain* coincidan. Por otra parte, el usar un código HASH nos va a permitir la creación de las claves públicas y privadas, con las que se reciben y envían **criptomonedas**.

Dentro de los datos de la cadena *blockchain*, son utilizadas diferentes capas de criptografía, que solamente pueden ser resueltos por ordenadores de una potencia considerable.

Ya en otro ámbito, concretamente en la cotidianeidad de nuestro día a día, uno de los usos más comunes que tiene la criptografía está en Internet.

Cuando accedemos a un sitio web denominado como **HTTPS** (fácilmente visible en el apartado de la URL de nuestro navegador favorito), éste utiliza el **protocolo de seguridad denominado SSL** (que estudiaremos en la siguiente unidad), por sus siglas en inglés, ***Secure Sockets Layer***. Este protocolo se encargar de cifrar todos los datos que el usuario pueda enviar al servidor utilizando diferentes algoritmos criptográficos.

Fig. 2. Seguridad

Un último ejemplo del uso de la criptografía está en el uso de cualquier **sistema financiero virtual**, como puede ser PayPal.

Así que recuerda, cada vez que accedas a determinadas páginas webs, realices una compra online..., estás haciendo uso de todo el potencial que nos ofrece la criptografía.

/ 4. Caso práctico 1: "La mejor encriptación"

Planteamiento: Pilar y José acaban de recibir un encargo de un cliente que está muy interesado en que sean ellos quienes resuelvan el problema, ya que su jefe considera que son los mejores programadores de la empresa.

El problema consiste en que este cliente desea encriptar de forma segura una serie de contraseñas de sus aplicaciones, pero como no es especialista en la materia, no sabe qué tipo de algoritmo utilizar.

Según él le han comentado que existen los siguientes tipos de algoritmos para este propósito: MD2, MD5, SHA-1, SHA-256, SHA-384 y SHA-512.

Nudo: ¿Cómo podrían nuestros amigos comprobar cuál de estos algoritmos de encriptación de información sería el mejor para las contraseñas de las aplicaciones de su cliente?

Desenlace: Como primer punto cabría destacar que la implementación de cualquier algoritmo de encriptación, por básico y sencillo que sea, ya ofrece una protección mayor que no usar ninguno, ya que provoca una primera barrera al intruso, al estar la información protegida de alguna forma.

En el caso que concierne a nuestros amigos, deberían de analizar una serie de características del encriptado final, con cada uno de los algoritmos de encriptación que les propone su cliente, y el que mejor resultados ofrezca, que sea el elegido.

Concretamente, habrá que prestar especial atención a los aspectos de:

- **Longitud de la cadena**: La cadena encriptada más larga será la más complicada de revertir en caso de ataque.
- **Tipo de caracteres usados**: Una encriptación será más segura si usa diferentes tipos de caracteres, como pueden ser letras minúsculas y mayúsculas, números y símbolos especiales.
- **El tiempo de encriptado**: El tiempo que se tarda en encriptar la información también es muy importante, ya que podemos tener una información muy segura, pero tardar en encriptarse mucho tiempo, lo cual no es aconsejable.

Fig. 3. Encriptado seguro

/ 5. Encriptación de la información

Podemos definir formalmente la encriptación o el **cifrado de la información** como el proceso por el que la información o los **datos que se desean proteger son codificados**, dando lugar a un texto que parece ser aleatorio, o sin sentido para los humanos.

Igualmente, podemos definir formalmente la **desencriptación** como la operación inversa a la encriptación, mediante la cual, **los datos encriptados se transforman mediante las técnicas inversas del algoritmo utilizado, para encriptarlos en el texto original**.

Es importante conocer los siguientes **conceptos básicos** para poder hablar de criptografía y encriptación:

- **Texto plano**: Se refiere al texto original, sin aplicar ningún algoritmo de encriptación.
- **Texto cifrado**: Se refiere al texto resultado de aplicar el algoritmo de encriptación al texto original.
- **Algoritmo de cifrado o algoritmo criptográfico**: Es el algoritmo que utilizaremos para poder encriptar o cifrar el texto plano para dar lugar al texto cifrado. Junto al algoritmo de cifrado existe una clave.
- **Clave**: Cadena de caracteres que serán la base para el algoritmo de cifrado, y que permitirán pasar del texto plano al cifrado. Cada clave diferente proporcionará como salida un texto cifrado diferente. Esta clave puede ser simétrica o asimétrica.

Fig. 4. Proceso de encriptado

Como resumen podemos decir que el proceso de encriptado de la información se puede representar mediante la siguiente fórmula:

$$Cifrado \rightarrow F\_K\ (M)=C$$

Donde F es el algoritmo que vamos a utilizar para cifrar la información, K será la clave de cifrado, M será el mensaje que queremos cifrar y C será el texto ya cifrado.

Vídeo 1. "Principios de la criptografía"
https://bit.ly/3nFfLvq

/ 6. Criptografía de clave privada o simétrica

La criptografía de clave simétrica o **privada es un método de encriptado que utiliza una clave que es secreta**, la cual solo pueden **conocer el emisor y el receptor**. Este tipo de criptografía es muy apropiada si queremos garantizar la confidencialidad.

A este tipo de criptografía se la **denomina simétrica porque la clave de encriptado y desencriptado es exactamente la misma**.

Podemos decir que las principales **características** de la criptografía simétrica son:

- **La clave es secreta**, debiendo conocerla solo las partes involucradas en la comunicación, es decir, el emisor y el receptor.
- Se utiliza la **misma clave para cifrar y para descifrar** los mensajes de la comunicación.
- Estos **algoritmos de cifrado** suelen ser **muy rápidos** y no suelen aumentar el tamaño del mensaje, es debido a esto que son muy apropiados para encriptar grandes cantidades de texto.

La criptografía de clave privada también tiene una serie de **inconvenientes**, pudiendo destacar los siguientes:

- Como la clave de cifrado y descifrado es la misma, en el momento del envío de ésta por parte del emisor al receptor, **este mensaje puede ser interceptado** y una persona no deseada puede hacerse con ella.
- Como las claves se utilizan en una única comunicación, si se desean comunicar varias personas, deberá haber **una clave para cada combinación de personas diferentes** que vayan a comunicarse, generando así una enorme cantidad de claves.

Una alternativa para solucionar los problemas de distribución de claves y todo lo que se deriva de ello, pueden ser la **criptografía asimétrica y la criptografía híbrida** que estudiaremos a continuación.

Un ejemplo práctico donde se utilizaba este tipo de criptografía fue la máquina Enigma, utilizada por la Alemania Nazi en la segunda guerra mundial para cifrar sus comunicaciones.

Fig. 5. Máquina enigma

/ 7. Criptografía de clave pública o asimétrica

La criptografía de clave pública surgió para solucionar el problema de distribución de claves que sufría la criptografía de clave privada, permitiendo así tanto al emisor como al receptor poder poner en común unas claves mediante un canal (incluso no seguro) de comunicación.

A este tipo de criptografía se le denomina asimétrica porque **las claves de encriptado y desencriptado son diferentes**, a diferencia de la criptografía de clave privada.

Podemos listar las **características** más importantes de este tipo de criptografía:

- Tanto **emisor como receptor tienen en su poder un par de claves**, una que es pública, que es conocida por todo el mundo y que el hecho de conocerla no implica conocer ningún tipo de información sobre la clave privada inversa, y otra que es privada, que la conoce únicamente su poseedor.

- Todas **las parejas de claves** sirven únicamente con ellas mismas, es decir, que **son complementarias**, y el proceso no funcionará si alguna de ellas es cambiada.
- **Las claves de encriptado y desencriptado únicamente se pueden generar una vez**, de esta forma, es prácticamente imposible que dos personas obtengan las mismas claves.
- Cuando un mensaje es cifrado con la **clave pública**, únicamente se va a poder descifrar con la clave privada que sea la inversa a esa clave pública.
- Cuando ciframos un mensaje con la **clave privada**, estamos demostrando que nosotros hemos sido quienes hemos cifrado dicho mensaje.

La gran ventaja que ofrece este tipo de criptografía es que ya no existe el problema de la distribución de claves.

La criptografía de clave pública también tiene algunos **inconvenientes**:

- Estos algoritmos son algo **más lentos.**
- Hay que poder **garantizar que la clave pública** es realmente de quien dice ser.

Lo más óptimo sería utilizar una combinación de criptografía de clave pública y de clave privada, lo que se conoce como criptografía híbrida.

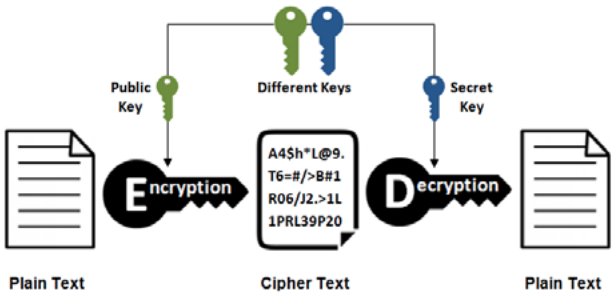

Fig. 6. Criptografía asimétrica usada en Bitcoin

/ 8. Caso práctico 2: "Accesos de usuario seguros"

Planteamiento: Pilar y José han recibido un ejercicio extra por parte de su profesor que trata sobre seguridad.

En este ejercicio nuestros amigos deben diseñar un acceso seguro de usuarios a una aplicación, es decir, realizar de forma segura su *login*.

El programa ya cuenta con un sistema de acceso, pero este no es seguro, ya que la contraseña se puede interceptar fácilmente.

Nudo: ¿Cómo crees que pueden mejorar la seguridad del acceso a la aplicación nuestros amigos? ¿Podrán utilizar alguno de los conceptos de la criptografía?

Desenlace: Una de las cosas más comunes que deben hacer los programadores de aplicaciones son los accesos de los usuarios a las mismas.

Estos accesos nunca deben implementarse en texto plano, ya que con un simple analizador de tráfico de red podríamos obtener las claves de acceso de una forma extremadamente sencilla.

La idea es que las claves de acceso estén encriptadas en la base de datos de usuarios de la aplicación, realizando así dos tareas de forma simultánea:

1. La primera sería que, al estar esas claves encriptadas en la base de datos, si alguien consigue entrar a ella no podrá obtenerlas.

2. La segunda es que estamos dotando de una alta seguridad a los accesos de los usuarios.

Para realizar estos accesos podríamos seguir los siguientes pasos:

- Obtener la clave que introduce el usuario.
- Encriptarla.
- Una vez encriptada, enviarla por petición segura HTTPS para comprobar si el *login* en correcto.

```
// Obtenemos las claves
usuario = obtenerUsuario()
clave = obtenerClave()

// Encriptamos la clave
clavesegura = encriptar(clave)

// Comprobamos si el acceso es OK
si comprobarAcceso(usuario, clavesegura)
    // entramos al sistema
sino
    // mostramos un error
```

Fig. 7. Esquema de acceso seguro

/ 9. Firma digital y certificados digitales

Las firmas digitales son el equivalente a las **firmas personales**, pero **en un entorno tecnológico**, es decir, su objetivo es identificar al firmante inequívocamente, pero en lugar de hacerlo en papel, se llevaría a cabo de forma digital. Las firmas digitales están basadas en **criptografía de clave pública y resumen de mensajes** HASH.

Un resumen de mensajes (*Message-Digest Algorithm*, en inglés) es un **algoritmo que para encriptar**, toma como entrada un **mensaje con una longitud variable y lo convierte en un resumen de una longitud fija**. Algunos algoritmos de este tipo son el MD5 y el SHA.

Otro elemento más que interviene en el proceso de criptografía son los **certificados digitales**. Éstos se diseñaron para resolver el problema de la confianza que han de depositar las dos partes involucradas en la comunicación, es decir, un certificado digital es un documento electrónico firmado por un tercero (entidad certificadora) que da fe de los datos de la firma digital empleada. De forma genérica, podemos decir que vienen a ser como el notario de la firma digital.

Una **entidad certificadora** es una organización que se responsabiliza de la veracidad de los datos de los firmantes digitales, y, por tanto, de la emisión y validez de los certificados oportunos. Creándolos y aportando mecanismos que permitan poder revocarlos, suspenderlos, y comprobar su validez.

Extrapolando todos estos conceptos a un entorno de programación, podemos destacar que en Java se usa la clase ***MessageDigest*** y los algoritmos que podemos emplear son: MD2, MD5, SHA-1, SHA-256, SHA-384 y SHA-512.

Cada vez que vayamos a encriptar un texto deberemos controlar la excepción *NoSuchAlgorithmException* mediante un bloque try-catch.

En el método *getInstance* es donde podremos indicar cualquiera de los algoritmos listados anteriormente para cifrar el mensaje con una función HASH.

```
try {
    String password = "contraseña";
    MessageDigest md = MessageDigest.getInstance("SHA-256");

    md.update(password.getBytes());
    byte byteData[] = md.digest();

    StringBuilder sb = new StringBuilder();
    for (int i = 0; i < byteData.length; i++) {
        sb.append(Integer.toString((byteData[i] & 0xff) + 0x100,
                16).substring(1));
    }

    System.out.println("Contraseña -> " + password);
    System.out.println("MD5 -> " + sb.toString());
} catch (NoSuchAlgorithmException error) {
    System.out.println("Error: " + error.toString());
}
```

Fig. 8. Código para encriptar texto con HASH

Vídeo 2. "Ejemplo de funciones HASH"
https://bit.ly/3lMDcm9

/ 10. Resumen y resolución del caso práctico de la unidad

A lo largo de esta unidad hemos conocido el concepto de **criptografía**, que como hemos podido comprobar, algo vital en seguridad de la información de nuestras aplicaciones.

Hemos aprendido a realizar el **proceso de encriptado** de la información.

También hemos estudiado los dos modelos más comunes de la criptografía, **el modelo de clave privada y el modelo de clave pública** y en qué se diferencian entre si cada uno de estos modelos criptográficos.

Por último, hemos practicado sobre cómo se puede aplicar la criptografía a las aplicaciones mediante las **firmas digitales y los certificados digitales**, además de un ejemplo de cómo se pueden usar las **funciones HASH** para ello.

Resolución del caso práctico de la unidad

Seguro que, en este momento del curso, y del ciclo, ya sabemos que la información es uno de los bienes más preciados ya no solo en la informática, porque sea vital para ésta, si no en cualquier organización, la información podría considerarse uno de los bienes más importantes a mantener y securizar. Si se pierde la información, se para la organización. Así de simple.

En el caso de la aplicación del bufete de abogados, lo más crítico, y por lo tanto lo primero que deberían mirar nuestros amigos es si la información que se almacena de los clientes, está correctamente encriptada.

Para esta tarea pueden utilizar una función de clave privada, siendo la clave de desencriptado conocida únicamente por el jefe o responsable del bufete.

Otro aspecto importante a considerar, es sobre si los usuarios se identifican en la aplicación de forma segura, y de no hacerlo, podría utilizarse un algoritmo de certificado digital, lo cual haría que esa identificación fuese totalmente fiable.

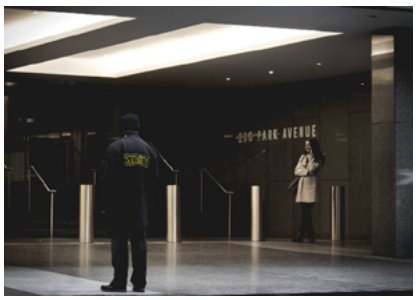

Fig. 9. Seguridad en el acceso a la información

/ 11. Bibliografía

Colaboradores de Wikipedia. (2020a, marzo 17). Criptografía simétrica. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica#:%7E:text=La%20criptograf%C3%ADa%20de%20clave%20sim%C3%A9trica,cifrar%20y%20descifrar%20mensajes%20en

Colaboradores de Wikipedia. (2020a, mayo 31). Criptografía. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Criptograf%C3%ADa

Colaboradores de Wikipedia. (2020a, julio 29). Seguridad de la información. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Colaboradores de Wikipedia. (2020, 28 agosto). Criptografía asimétrica. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica#:%7E:text=La%20criptograf%C3%ADa%20asim%C3%A9trica%20(en%20ingl%C3%A9s,para%20el%20env%C3%ADo%20de%20mensajes.

Encriptacion – NextVision. (s. f.). NextVision. Recuperado 1 de septiembre de 2020, de https://nextvision.com/tag/encriptacion/

León, D. (2019, 7 junio). ¿Qué otros usos tienen la criptografía aparte de las criptomonedas? CRIPTO TENDENCIA. https://criptotendencia.com/2019/06/06/que-otros-usos-tiene-la-criptografia-a-parte-de-las-criptomonedas/

MEDAC