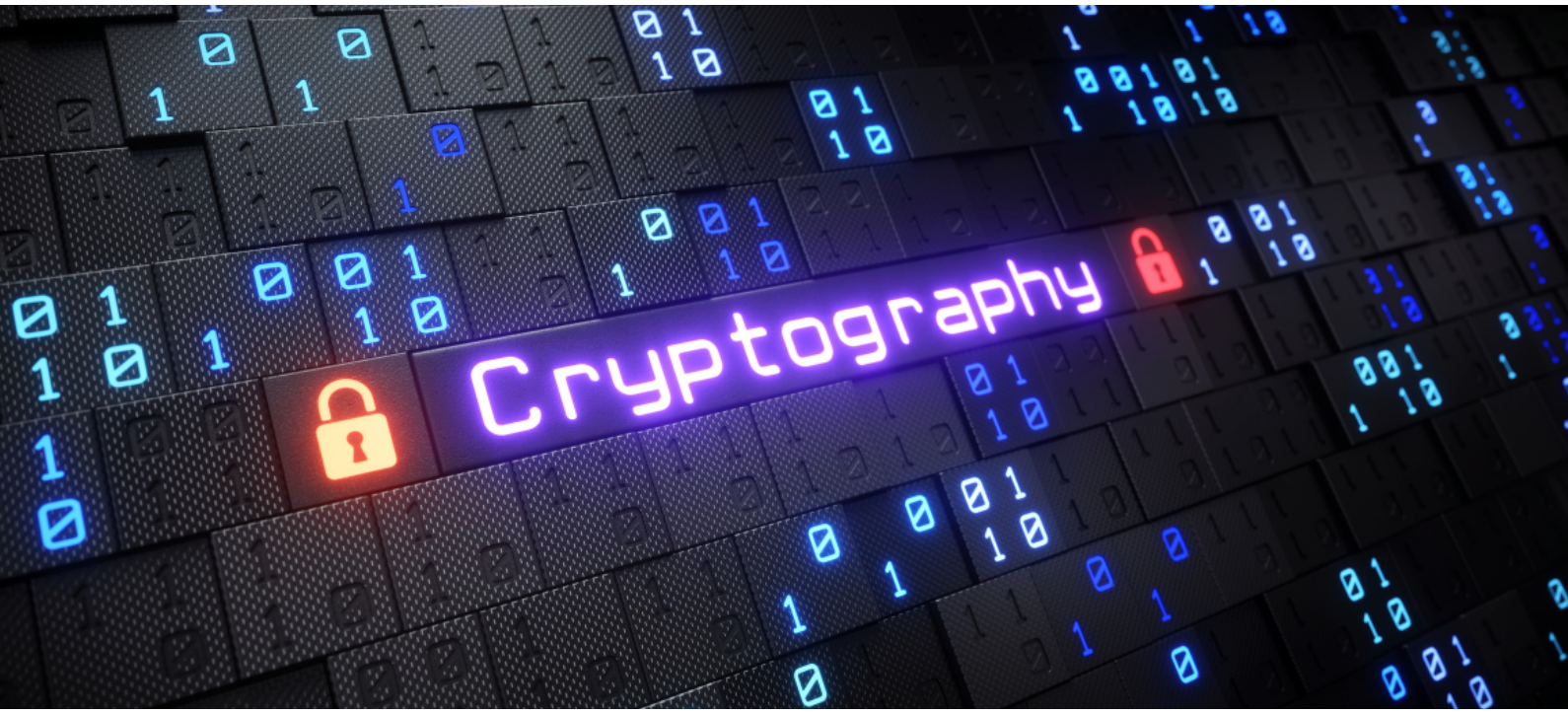
Acceso a Datos - T2
Hito grupal - Criptografía



Sergio Camino, Isla Peinado y Mario Luquero

13/12/2022

Índice:

Introducción **3**
Parte 1: investigación 3
¿Qué es la criptografía? 3
Desarrollo 4
Conceptos fundamentales asociados a la criptografía. 4
Historia y origen de la criptografía. 5
Parte 2: Práctica 8
Algoritmo Cesar 8
MDA5 8
SHA 9
Conclusiones **10**
Bibliografía **11**
Rúbrica **12**

Introducción

Parte 1: investigación

¿Qué es la criptografía?

La criptografía es un método con el cual podemos **proteger y ocultar datos mediante cifrados o codificación** en el mundo de la informática. La criptografía transforma una representación lingüística en datos ininteligibles. La criptografía no sólo se utiliza para datos sino que también se utiliza para usuarios. Por tanto, el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes, para lo cual se diseñan sistemas de cifrado y códigos.

La criptografía es una de las artes más antiguas del mundo. Los primeros mensajes cifrados tratan del siglo V, cuando los espartanos usaban la escítala, una especie de vara en la que se enrollaba una cinta de cuero o papiro con un puñado de letras sin sentido. Gracias a esta, era posible cifrar y descifrar mensajes utilizando como referencia el diámetro de la vara.

Desarrollo

Conceptos fundamentales asociados a la criptografía.

- ¿Qué es la encriptación? :

La encriptación es un mecanismo de seguridad en el cual transformamos los datos a proteger en algo que parece aleatorio y que no tiene significado.

- ¿Qué es la desencriptación? :

Es el proceso de seguridad en el que traducimos los datos encriptados a su forma original.

- Qué es un algoritmo criptográfico :

Es una función matemática que utilizamos para la encriptación y desencriptación. Para encriptar, la función matemática combina la información a proteger con una clave provista. Para desencriptar, la función matemática mediante los datos encriptados y la clave provista los desencripta y tenemos los datos de forma visible para el usuario (texto plano).

- Mecanismos de cifrado :

Es un mecanismo de seguridad que nos permite modificar un texto simple de forma que su contenido sea ilegible, salvo para su destinatario.

- Técnicas de encriptación :
    - César : Su origen se sitúa en el siglo I antes de Cristo. Consiste en cambiar las letras del texto plano por números fijos en el alfabeto.

    - Transposición : Es un tipo de cifrado en el que unidades de texto plano se cambian de posición siguiendo un esquema bien definido,, que puede ser sencillo o complejo. Fue inventada por el Comandante Baudoin en 1939

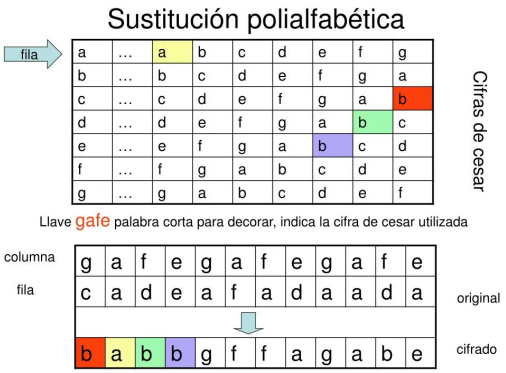
    - Gronsfeld : Se tiene un conjunto de alfabetos cifrado. El alfabeto cifrado que se utiliza depende de la clave pasada.

    - DES : Data Encryption Standard es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo.

- AES : En el cifrado AES (Advanced Encryption Standard), la información se estructura en bloques, todos de un tamaño fijo de 128 bits. Estos están compuestos de una matriz de cuatro por cuatro bytes (cada byte tiene 8 bits, de ahí los 128). Después, cada byte se va moviendo de sitio y reemplazando siguiendo una serie de instrucciones recogidas en la clave. Es un cifrado que se caracteriza por su rapidez y eficiencia.

- Cifrado exponencial : Es un sistema criptográfico que se caracteriza por utilizar dos claves, una clave pública y otra privada, para el envío de mensajes o datos informáticos. Cabe señalar que ambas claves están conectadas entre sí, siendo que la clave pública es la responsable del cifrado y la clave privada del descifrado. En cuanto al procedimiento, el destinatario genera ambas claves y comunica la clave pública al emisor del mensaje quien, por su parte, tiene ahora la opción de cifrar el mensaje. Una vez que se haya enviado el mensaje, solo se podrá descifrar con la clave privada, de manera que si el mensaje cifrado es interceptado, la información del mensaje permanecerá oculta.

Historia y origen de la criptografía.



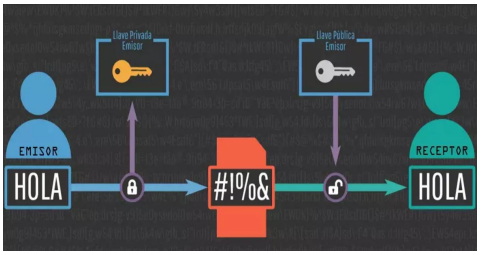
El uso de la criptografía se remonta a la antigua Grecia y Egipto, donde se utilizaban técnicas simples como la **sustitución de letras** para ocultar mensajes. Durante la Edad Media, las técnicas mejoraron, en esta época se utilizaba el **cifrado por sustitución polialfabética**. La principal razón por la que la criptografía se empezó a desarrollar fue para proteger los mensajes militares y políticos, a la vez de para escapar de la censura tanto religiosa como política. Hasta llegar a la actualidad donde se podría decir que la utilizamos todos los días.

Durante el siglo XV, el matemático italiano Leon Battista Alberti desarrolló una técnica de codificación conocida como el "**cifrado de sustitución polialfabética**", que consistía en reemplazar letras con otras letras o símbolos.

En la Revolución Francesa, el matemático francés Blaise de Vigenère desarrolló una técnica de cifrado conocida como la "**tabla de Vigenère**", que utilizaba una combinación de varios alfabetos para codificar un mensaje.

En el siglo XIX, el matemático alemán Auguste Kerckhoffs publicó un artículo donde se establecieron los principios básicos de la seguridad de la criptografía, enfatizando la importancia de la **clave secreta** y la necesidad de que el algoritmo de codificación sea conocido públicamente.

En el siglo XX, con el avance de la tecnología, Whitfield Diffie y Martin Hellman propusieron un gran avance en criptografía "**cifrado de clave pública".** Este cifrado utiliza dos claves: una clave pública que se utiliza para codificar el mensaje, y una clave privada que se utiliza para descifrarlo.



La criptografía en el siglo XXI se ha convertido en una herramienta esencial para la seguridad de la información en un mundo cada vez más digital. Los avances tecnológicos han permitido el desarrollo de nuevos algoritmos de cifrado más seguros, como el cifrado **RSA** y el cifrado **AES**. Además, la criptografía se utiliza en una variedad de aplicaciones, como la seguridad de la información en la nube, la privacidad en las redes sociales y la seguridad en las transacciones comerciales en línea, para garantizar la seguridad de las transacciones financieras. En el mundo de las criptomonedas, la tecnología blockchain utiliza criptografía. La criptografía también juega un papel importante en la ciberseguridad y la protección contra el cibercrimen.

En resumen, la **criptografía es una herramienta** esencial **para garantizar la seguridad de la información** en la era digital. Sus raíces se remontan a la antigüedad, pero ha evolucionado y se ha vuelto cada vez más compleja con el paso del tiempo, especialmente con el aumento de las comunicaciones electrónicas y la necesidad de proteger nuestra información confidencial.

Parte 2: Práctica

Explicación en el zip

Algoritmo Cesar

```
public class Cesar {
   public static final String ALPHABET = "abcdefghijklmnopqrstuvwxyz ";
   public static String Encriptar(String mensaje, int puestos){
            mensaje = mensaje.toLowerCase();
       String mensajeEncriptado = "";
       for (int i = 0; i < mensaje.length(); i++){
           int pos = ALPHABET.indexOf(mensaje.charAt(i));
           int encriptadoPos = (puestos + pos) % 26;
           char mensajeCifrado = ALPHABET.charAt(encriptadoPos);
           mensajeEncriptado+=mensajeCifrado;
       }
       return mensajeEncriptado;
   }
   public static String Desencriptar(String mensaje, int puestos){
       mensaje = mensaje.toLowerCase();
       String mensajeDesencriptado = "";
       for (int i = 0; i < mensaje.length(); i++){
           int pos = ALPHABET.indexOf(mensaje.charAt(i));
           int desencriptarPos = (pos - puestos) % 26;
           if (desencriptarPos < 0){
               desencriptarPos = ALPHABET.length() + desencriptarPos;
           }
           char mensajeDescifrado = ALPHABET.charAt(desencriptarPos);
           mensajeDesencriptado+=mensajeDescifrado;
       }
       return mensajeDesencriptado;
   }
}
```

MDA5

```
public class MD5 {
   public static String EncriptarCorreo() throws NoSuchAlgorithmException {
       Scanner sc = new Scanner(System.in);
       System.out.println("Introduce el correo que desea cifrar: ");
       String correo = sc.nextLine();
       MessageDigest md = null;
       try {
           md = MessageDigest.getInstance("MD5");
       } catch (NoSuchAlgorithmException e) {
           throw new RuntimeException(e);
       }
       md.update(correo.getBytes());
       byte[] digest = md.digest();
       StringBuffer sb = new StringBuffer();
       for (byte b : digest) {
           sb.append(String.format("%02x", b & 0xff));
       }
       String resultadoCorreo=sb.toString();
           return resultadoCorreo;
   }
   public static String EncriptarPass() throws NoSuchAlgorithmException {
       Scanner sc2 = new Scanner(System.in);
       System.out.println("Introduce la contraseña que desea cifrar: ");
```

```
        String pass = sc2.nextLine();
        MessageDigest md = null;
        try {
            md = MessageDigest.getInstance("MD5");
        } catch (NoSuchAlgorithmException e) {
            throw new RuntimeException(e);
        }
        md.update(pass.getBytes());
        byte[] digest = md.digest();
        StringBuffer sb = new StringBuffer();
        for (byte b : digest) {
            sb.append(String.format("%02x", b & 0xff));
        }
        String resultadoPass=sb.toString();
        return resultadoPass;
    }
}
```

SHA

```
public class SHA {
    public static String EncriptarCorreoSha() throws NoSuchAlgorithmException {
        Scanner sc = new Scanner(System.in);
        System.out.println("Introduce el correo que desea cifrar: ");
        String correoSha = sc.nextLine();
        MessageDigest md = MessageDigest.getInstance("SHA-1");
        md.update(correoSha.getBytes());
        byte[] digest = md.digest();
        StringBuffer sb = new StringBuffer();
        for (byte b : digest) {
            sb.append(String.format("%02x", b & 0xff));
        }
        String resultadoCorreoSha = sb.toString();
        return resultadoCorreoSha;
    }

    public static String EncriptarPassSha() throws NoSuchAlgorithmException {
        Scanner sc2 = new Scanner(System.in);
        System.out.println("Introduce la contraseña que desea cifrar: ");
        String passSha = sc2.nextLine();
        MessageDigest md = MessageDigest.getInstance("SHA-1");
        md.update(passSha.getBytes());
        byte[] digest = md.digest();
        StringBuffer sb = new StringBuffer();
        for (byte b : digest) {
            sb.append(String.format("%02x", b & 0xff));
        }
        String resultadoPassSha = sb.toString();
        return resultadoPassSha;
    }
}
```

Conclusiones

Según pasan los años, en el mundo tecnológico se utiliza cada vez más el cifrado de mensajes. El cifrado de mensajes es una herramienta muy importante para mantener la privacidad de los usuarios en internet. También es importante que estos algoritmos se mantengan actualizados para brindar mayor seguridad. Hay algoritmos que se encuentran comprometidos, por tanto a día de hoy es muy sencillo descifrarlos y por ello no deben usarse para seguridad informática, por ello se han creado nuevas versiones de algoritmos ya existentes. También existen versiones nuevas de algoritmos ya existentes debido a que ese algoritmo es inseguro debido a la posibilidad de colisiones (es decir, dos conjuntos de datos diferentes que producen el mismo hash).

En nuestro proyecto lo que más difícil nos ha resultado ha sido sacar la lógica sobre como podemos comprobar que el usuario existe. Nosotros guardamos los datos de un usuario en un archivo y más tarde si ese usuario quiere iniciar sesión tenemos que comprobar que los datos introducidos son los mismos que los datos almacenados en el fichero.

Nosotros lo hemos solucionado de la siguiente forma; hemos cifrado tanto los datos del fichero como los datos que nos pasa el usuario (con la misma estructura) y comprobamos estos datos, si son iguales inicia sesión si no lo son le pide que se registre.

Bibliografía

Nombre Web	Apartado
¿Qué es la criptografía? Wikipedia	Que es la criptografía. Técnicas de criptografía.
Sede Electrónica - Real casa de la moneda	Que es la Encriptación o Cifrado
Wikipedia	Historia y origen de la criptografía.
Criptografía - Conceptos básicos	Técnicas de encriptación
Conceptos básicos de criptografía	Conceptos básicos de Criptografía
Cifrado por transposición	Cifrado por transposición
Cifrado Gronsfeld Cifrado Gronsfeld2	Cifrado Gronsfeld
Algoritmo DES	¿Qué es el algoritmo DES?
Algoritmo AES	¿Qué es el algoritmo AES?
Criptografía asimétrica	¿Qué es la criptografía asimétrica?
Ayudaley Cifrado César Linuxitos	¿Qué es el algoritmo CESAR?
acastedecu	¿Qué es el algoritmo MD5?
ProgramadorClic	¿Qué es el algoritmo SHA?

Rúbrica

He participado activamente en la realización de esta actividad y he creado un buen clima de trabajo dentro del grupo	**1 punto**
PARTE 1: ACTIVIDAD DE INVESTIGACIÓN	
El trabajo cumple con las especificaciones marcadas en el enunciado (estructura, presentación, etc.)	**1 punto**
Está bien definido el concepto de Criptografía	**0,5 puntos**
Se ha presentado de manera clara el origen de la criptografía	**1 punto**
Se han presentado con claridad los conceptos fundamentales asociados a la criptografía	**2 puntos**
El trabajo está libre de plagio. Si se ha utilizado algún párrafo copiado de otra fuente se ha citado correctamente	**1 punto**
PARTE 2: PARTE PRÁCTICA	
Implementación de cifrado/descifrado algoritmo Cesar	**1 punto**
Implementación de cifrado/descifrado MDA5 y SHA	**1,5 punto**
Uso de ficheros y control de errores y excepciones	**1 punto**