# Informe Laboratorio 4

**Sección 1**

Rayen Millaman
e-mail: rayen.millaman@mail.udp.cl

Mayo de 2024

# Índice

# 1. Descripción de actividades

Para este laboratorio, deberá utilizar Tampermonkey y la librería CryptoJS (con SRI) para lograr obtener los mensajes que le está comunicando su informante. En esta ocasión, su informante fue más osado y se comunicó con usted a través de un sitio web abierto a todo el público https://cripto.tiiny.site/.

Sólo un ojo entrenado como el suyo logrará descifrar cuál es el algoritmo de cifrado utilizado y cuál es la contraseña utilizada para lograr obtener la información que está oculta.

1. Desarrolle un plugin para tampermonkey que permita obtener la llave para el descifrado de los mensajes ocultos en la página web. La llave debe ser impresa por la consola de su navegador al momento de cargar el sitio web. Utilizar la siguiente estructura:

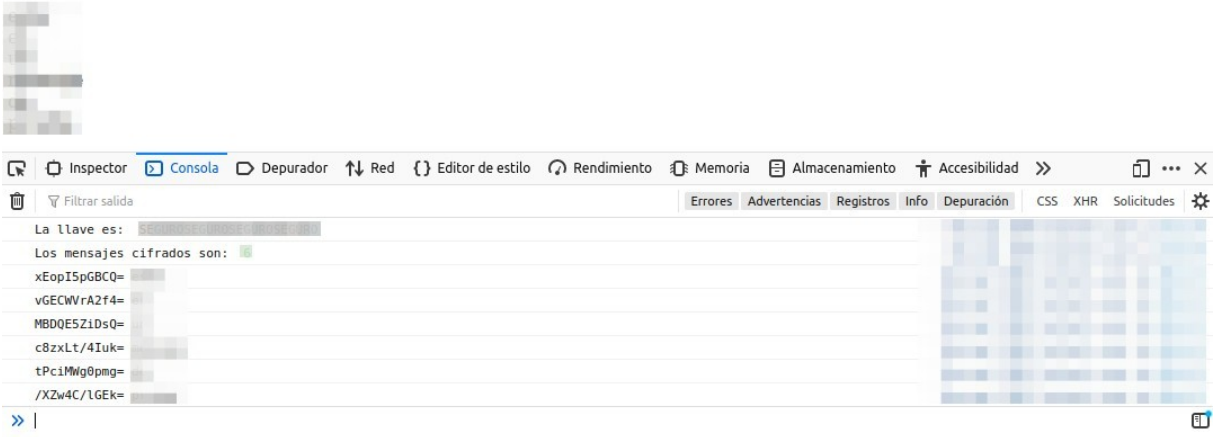
   - La llave es: KEY

2. En el mismo plugin, se debe detectar el patrón que permite identificar la cantidad de mensajes cifrados. Debe imprimir por la consola la cantidad de mensajes cifrados. Utilizar la siguiente estructura: Los mensajes cifrados son: NUMBER

3. En el mismo plugin debe obtener cada mensaje cifrado y descifrarlo. Ambos mensajes deben ser informados por la consola (cifrado espacio descifrado) y además cada mensaje en texto plano debe ser impreso en la página web.

   El script desarrollado debe ser capaz de obtener toda la información del sitio web (llave, cantidad de mensajes, mensajes cifrados) sin ningún valor forzado. Para verificar el correcto funcionamiento de su script se utilizará un sitio web con otro texto y una cantidad distinta de mensajes cifrados. Deberá indicar la url donde se podrá descargar su script.

   Un ejemplo de lo que se debe visualizar en la consola, al ejecutar automáticamente el script, es lo siguiente:



Sin el conocimiento de información secreta, el criptoanálisis se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanálisis es un componente importante del proceso de creación de criptosistemas sólidos. Gracias al criptoanálisis, podemos comprender los criptosistemas y mejorarlos identificando los puntos débiles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un código secreto más seguro y protegido. Resultado del criptoanálisis es la protección de la información crítica para que no sea interceptada, copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluyen evaluar, analizar y localizar las debilidades en los sistemas y algoritmos de seguridad criptográfica. Sin el conocimiento de información secreta, el criptoanálisis se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanálisis es un componente importante del proceso de creación de criptosistemas sólidos. Gracias al criptoanálisis, podemos comprender los criptosistemas y mejorarlos identificando los puntos débiles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un código secreto más seguro y protegido. Resultado del criptoanálisis es la protección de la información crítica para que no sea interceptada, copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluyen evaluar, analizar y localizar las debilidades en los sistemas y algoritmos de seguridad criptográfica. Sin el conocimiento de información secreta, el criptoanálisis se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanálisis es un componente importante del proceso de creación de criptosistemas sólidos. Gracias al criptoanálisis, podemos comprender los criptosistemas y mejorarlos identificando los puntos débiles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un código secreto más seguro y protegido. Resultado del criptoanálisis es la protección de la información crítica para que no sea interceptada, copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluyen evaluar, analizar y localizar las debilidades en los sistemas y algoritmos de seguridad criptográfica. Sin el conocimiento de información secreta, el criptoanálisis se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanálisis es un componente importante del proceso de creación de criptosistemas sólidos. Gracias al criptoanálisis, podemos comprender los criptosistemas y mejorarlos identificando los puntos débiles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un código secreto más seguro y protegido. Resultado del criptoanálisis es la protección de la información crítica para que no sea interceptada, copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluyen evaluar, analizar y localizar las debilidades en los sistemas y algoritmos de seguridad criptográfica.

[redacted]

```
La llave es: [redacted]
Los mensajes cifrados son: [redacted]
xEopI5pGBCQ= [redacted]
vGECWVrA2f4= [redacted]
MBDQE5ZiDsQ= [redacted]
c8zxLt/4Iuk= [redacted]
tPciMWg0pmg= [redacted]
/XZw4C/lGEk= [redacted]
```

# 2. Desarrollo (Parte 1)

## 2.1. Detecta el cifrado utilizado por el informante

Una vez ingresada a la página solicitada, se buscan elementos que puedan ser indicativos de algún mensaje a descifrar.
De manera visual, se detecta que las letras mayusculas del texto forman la palabra: **SEGUROSEGUROSEGUROSEGURO** , correspondiente a la llave.

## 2.2. Logra que el script solo se gatille en el sitio usado por el informante

Para que el script solo funcione en un sitio especifico, se debe especificar al inicio del script de la siguiente forma.

```
// @author      You
// @match       https://cripto.tiiny.site/
// @icon        
```

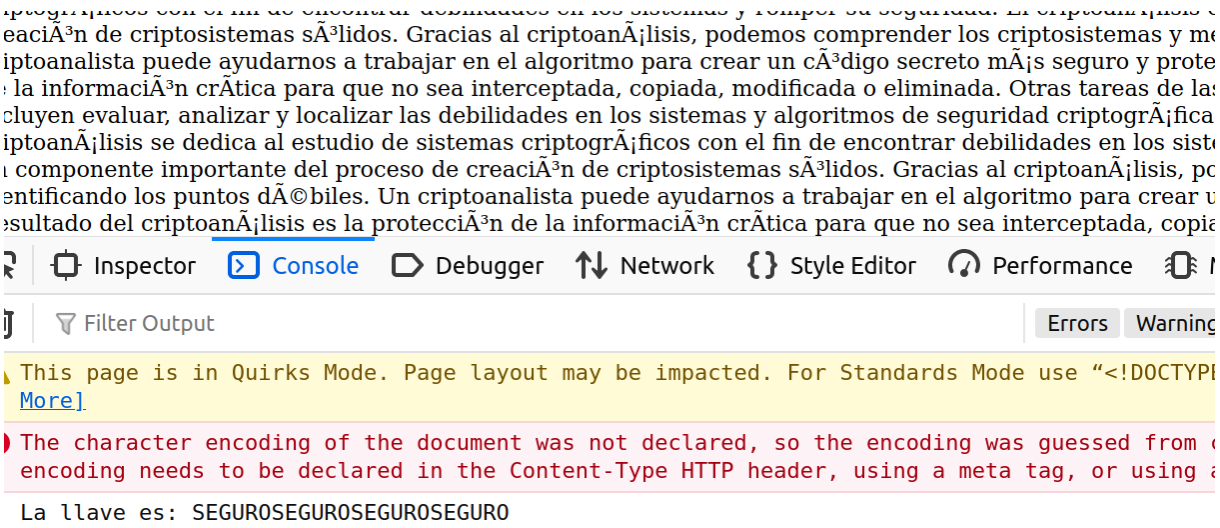
## 2.3. Define función que obtiene automáticamente el password del documento

La funcion debe identificar solo las letras mayusculas presentes en el texto, para luego juntarlas y entregar su unión por consola.

```
// ==UserScript==
// @name         este si
// @namespace    http://tampermonkey.net/
// @version      2024-06-07
// @description  try to take over the world!
// @author       You
// @match        https://cripto.tiiny.site/
// @icon         
// @grant        none
// @require      https://update.greasyfork.org/scripts/12080/71213/CryptoJS
// ==/UserScript==

(function() {
    'use strict';'use strict';

    function mayusculas(text) {
        return text.match(/[A-Z]/g) || [];
    }
        var allText = document.body.innerText;

    var upperCaseLetters = mayusculas(allText);

    var key = upperCaseLetters.join('');

    console.log('La llave es:', key);
```

## 2.4. Muestra la llave por consola

Ingresado a la pagina, se carga el tampermonkey con el scrit realizado para poder inspeccionar por consola lo obtenido.




Adicionalmente, al inspeccionar la pagina se encunetran 6 divs con mensajes cifrados en base 64, que pueden pertenecer a los mensajes encriptados por el informante.
Para analizar el mensaje, se utiliza un enlace externo para poder decodificar estos mensajes. Como el mensaje obtenido carece de sentido, este quiere decir que se encuentra encriptado, para saber la encriptación se probara entre los modelos vistos en clases (AES,DES y 3DES)

# 3. Desarrollo (Parte 2)

## 3.1. Reconoce automáticamente la cantidad de mensajes cifrados

Como se vio en la parte uno, cada div representa un mensaje; por lo que se actualiza el script para añadir un contador según los div obtenidos en el texto.

```
var divElements = document.getElementsByTagName('div');
var cont = divElements.length;

console.log('Los mensajes cifrados son:', cont);
```

## 3.2. Muestra la cantidad de mensajes por consola

Resultado obtenido por consola:

```
La llave es: SEGUROSEGUROSEGUROSEGURO
Los mensajes cifrados son: 6
```

# 4. Desarrollo (Parte 3)

## 4.1. Importa la librería cryptoJS

Para poder descifrar los mensajes se utiliza la libreria crytoJS desde el siguiente link:crypto-js

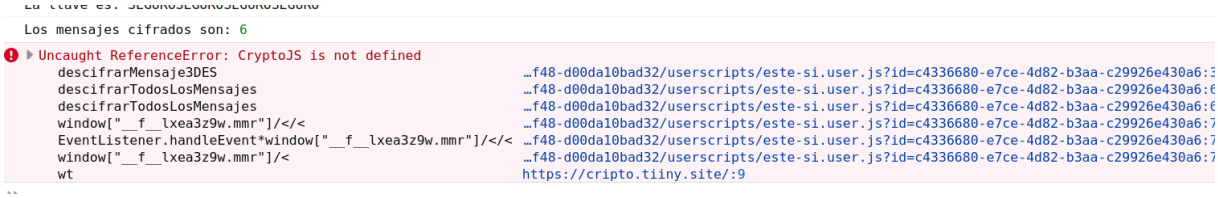
## 4.2. Utiliza SRI en la librería CryptoJS

Para insertar SRI, se concatena en conjunto con la libreria de Crytojs por medio del algorito sha512

```
https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js#sha512-E8QSvWZ0eCLGk4km3hxSsNmGWbLtSCSUcewDQPQWZF6pEU8GlT8a5fF32wOlli8ftdMhssTrF/OhyGWwonTcXA==
==
```

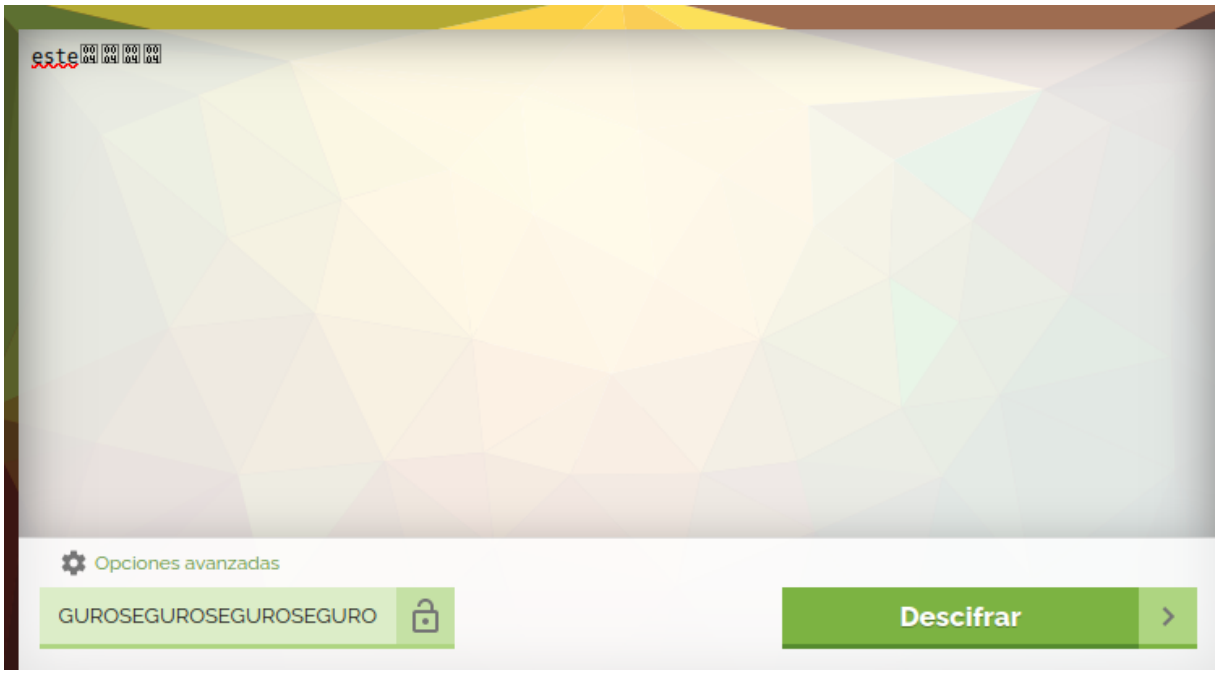
## 4.3. Repercusiones de SRI inválido

En caso de que el SRI sea invalido, se mostrara un mensaje por consola que indicando que la carga del recurso ha fallado debido a un fallo en la verificación del SRI.




## 4.4. Logra decifrar uno de los mensajes

Ahora, continuando, se conoce la llave, por lo que faltaría probar cuál es el método de descifrado (AES, DES o 3DES). Con el uso de la página Cifrado online se obtuvo que el método adecuado fue 3DES con modo ECB, donde para el primer mensaje div: **xEopI5pGBCQ=** se obtuvo la palabra .$^{es}$te". Con esto en cuenta, se implementa el código según estas especificaciones.




```
function cifrarMensaje(mensaje, llave) {
    return CryptoJS.TripleDES.encrypt(mensaje, llave, {
        mode: CryptoJS.mode.ECB,
        padding: CryptoJS.pad.Pkcs7
    }).toString();
}

function descifrarMensaje3DES(mensajeCifradoBase64, clave) {
    let claveHex = CryptoJS.enc.Utf8.parse(clave);
    let mensajeDescifrado = CryptoJS.TripleDES.decrypt({
        ciphertext: CryptoJS.enc.Base64.parse(mensajeCifradoBase64)
    }, claveHex, {
        mode: CryptoJS.mode.ECB,
        padding: CryptoJS.pad.Pkcs7
    });
    return mensajeDescifrado.toString(CryptoJS.enc.Utf8);
}
```

```
Los mensajes cifrados son: 6

xEopI5pGBCQ= : este
```

## 4.5. Imprime todos los mensajes por consola

Luego se modifica el script para que reccorra la lista de mensajes a desifrar y los pueda desifrar.

```
// Función para contar los mensajes cifrados y descifrarlos
function descifrarTodosLosMensajes() {
    let divs = document.querySelectorAll("div[id]");
    console.log('Los mensajes cifrados son:', divs.length);

    divs.forEach(div => {
        let mensajeCifradoBase64 = div.id;
        if (mensajeCifradoBase64) {
            let mensajeDescifrado = descifrarMensaje3DES(mensajeCifradoBase64, claveGlobal);
            console.log(` ${mensajeCifradoBase64} : ${mensajeDescifrado}`);
            imprimirMensajesEnPagina(mensajeDescifrado);
        }
    });
}
```

```
La llave es: SEGUROSEGUROSEGUROSEGURO
Los mensajes cifrados son: 6
 xEopI5pGBCQ= : este
 vGECWVrA2f4= : es
 MBDQE5ZiDsQ= : un
 c8zxLt/4Iuk= : mensaje
 tPciMWg0pmg= : de
 /XZw4C/lGEk= : prueba
 GET https://cripto.tiiny.site/favicon.ico
```

## 4.6. Muestra los mensajes en texto plano en el sitio web

Luego, se añade una nueva función para imprimir los mensajes descifrados en el texto plano del documento.

```
// Función para imprimir mensajes en la página
function imprimirMensajesEnPagina(mensajeCifrado, mensajeDescifrado) {
    let div = document.createElement('div');
    div.textContent = `${mensajeCifrado} : ${mensajeDescifrado}`;
    document.body.appendChild(div);
}
```

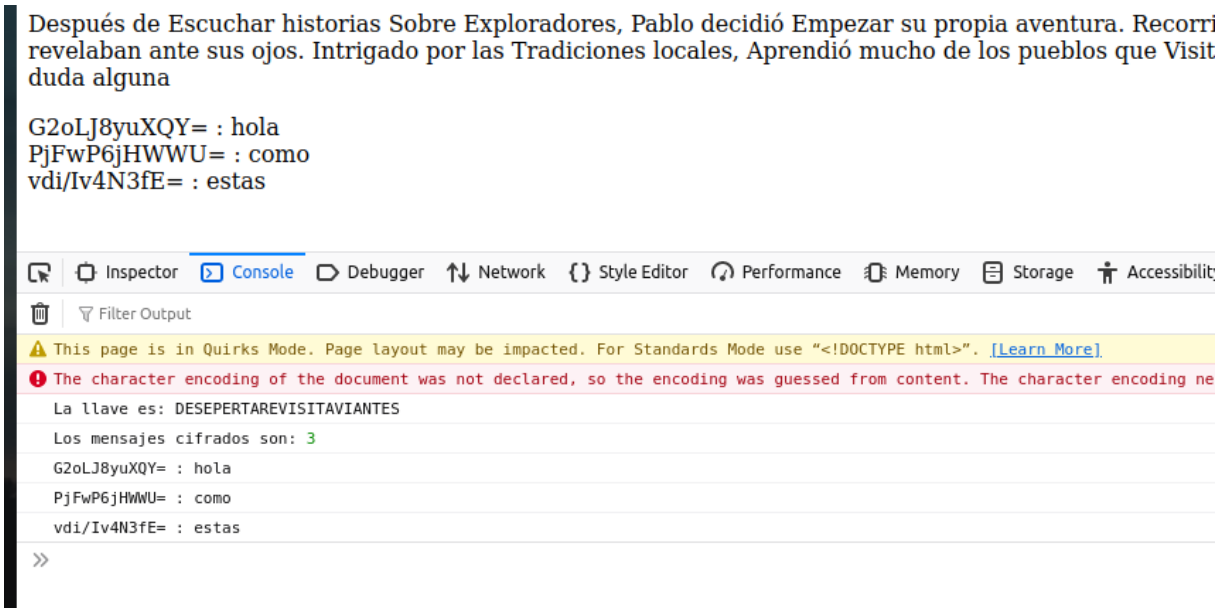
criptoanÃ¡lisis es la protecciÃ³n de la informaciÃ³n crÃtica para que no sea interceptada, copiada, mod
localizar las debilidades en los sistemas y algoritmos de seguridad criptogrÃ¡fica. Sin el conocimiento d
debilidades en los sistemas y romper su seguridad. El criptoanÃ¡lisis es un componente importante del
mejorarlos identificando los puntos dÃ©biles. Un criptoanalista puede ayudarnos a trabajar en el algor
informaciÃ³n crÃtica para que no sea interceptada, copiada, modificada o eliminada. Otras tareas de la
algoritmos de seguridad criptogrÃ¡fica.

xEopI5pGBCQ= : este
vGECWVrA2f4= : es
MBDQE5ZiDsQ= : un
c8zxLt/4Iuk= : mensaje
tPciMWg0pmg= : de
/XZw4C/lGEk= : prueba

## 4.7. El script logra funcionar con otro texto y otra cantidad de mensajes

Luego, para que el mensaje funcione con otro texto, añadimos la función de modificar el texto y agregamos los nuevos mensajes encriptados.

```
function cambiarContenido() {
    var elementosP = document.querySelectorAll('p');

    elementosP.forEach(function(p) { // Elimina los campos <p>
        p.remove();
    });

    var elementosDiv = document.querySelectorAll('div');

    elementosDiv.forEach(function(div) { // Elimina los campos <div>
        div.remove();
    });

    var nuevoT = document.createElement('p');
    nuevoT.textContent = 'Después de Escuchar historias Sobre Exploradores, Pablo decidió Empezar su propia
    document.body.appendChild(nuevoT);

    var mCifrados = ['G2oLJ8yuXQY=', 'PjFwP6jHWWU=', 'vdi/Iv4N3fE='];

    for (var i = 0; i < mCifrados.length; i++) {
        var nuevoDiv = document.createElement('div');
        nuevoDiv.id = mCifrados[i];
        nuevoDiv.className = 'm' + i.toString();
        document.body.appendChild(nuevoDiv);
    }
}
```




## 4.8. Indica url al código .js implementado para su validación

Codigo .js

# Conclusiones y comentarios

Se logró comprender los diferentes algoritmos de cifrado y cómo descifrar utilizando javascript. Asímismo se potenciaron los conocimientos de la cátedra y se pudo palpar la asignatura desde un lado mucho más común como lo es HTML y Javascript. La experiencia fué un éxito.

## Issues

Uno de los problemas que tuve fue encontrar en la parte 3 los mensajes cifrados para el nuevo texto; no lograba identificar cuáles eran sin causar error. Otro problema fue en el manejo de los cifrados; me costó determinar cuál era el cifrado correcto a utilizar, lo cual se resolvió con ayuda de otras páginas para la implementación e ir probando cada una. También se tuvieron problemas en la implementación de la librería Crypto-js y su implementación con SRI, me costó entender el funcionamiento y cómo implementarla. Por último, uno de los problemas fue en la realización del código, ya que no me funcionaba en la mayoría de las ocasiones, por lo que su solución fue recurrir a la inteligencia artificial.icial.