Informe Laboratorio 4

Sección 1

Cristopher Osorio Kappes
e-mail: cristopher.osorio_k@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.

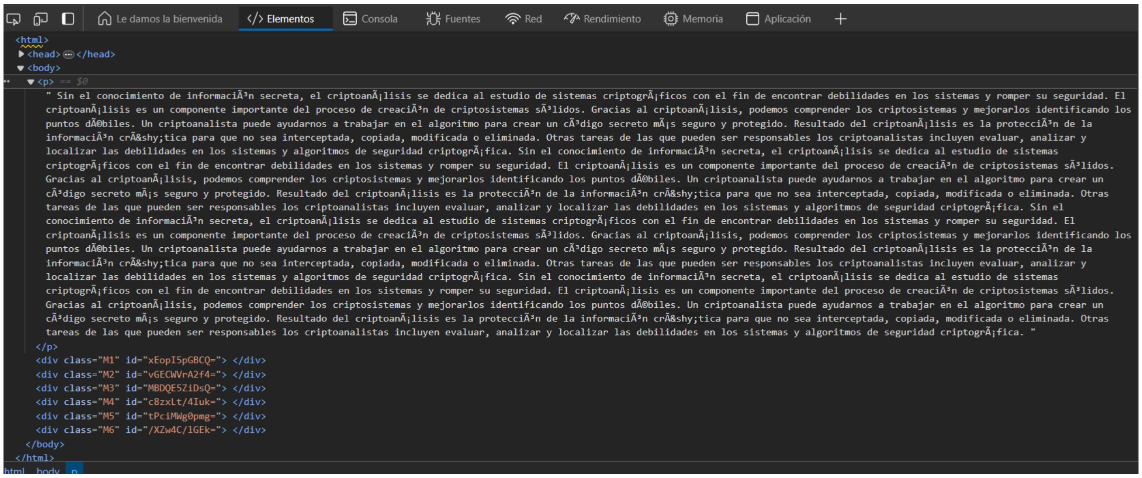
[redacted]

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

[redacted]

2. Desarrollo (Parte 1)

2.1. Detecta el cifrado utilizado por el informante



```
<html>
 ▶<head> ⋯ </head>
 ▼<body>
   ▼<p> == $0
      " Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡ficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El
      criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos comprender los criptosistemas y mejorarlos identificando los
      puntos dÃ©biles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seguro y protegido. Resultado del criptoanÃ¡lisis es la protecciÃ³n de la
      informaciÃ³n crÃ&shy;tica 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 criptogrÃ¡fica. Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas
      criptogrÃ¡ficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos.
      Gracias al criptoanÃ¡lisis, podemos comprender los criptosistemas y mejorarlos identificando los puntos dÃ©biles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un
      cÃ³digo secreto mÃ¡s seguro y protegido. Resultado del criptoanÃ¡lisis es la protecciÃ³n de la informaciÃ³n crÃ&shy;tica 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 criptogrÃ¡fica. Sin el
      conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡ficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El
      criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos comprender los criptosistemas y mejorarlos identificando los
      puntos dÃ©biles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seguro y protegido. Resultado del criptoanÃ¡lisis es la protecciÃ³n de la
      informaciÃ³n crÃ&shy;tica 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 criptogrÃ¡fica. Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas
      criptogrÃ¡ficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos.
      Gracias al criptoanÃ¡lisis, podemos comprender los criptosistemas y mejorarlos identificando los puntos dÃ©biles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un
      cÃ³digo secreto mÃ¡s seguro y protegido. Resultado del criptoanÃ¡lisis es la protecciÃ³n de la informaciÃ³n crÃ&shy;tica 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 criptogrÃ¡fica. "
     </p>
     <div class="M1" id="xEopI5pGBCQ="> </div>
     <div class="M2" id="vGECWVrA2f4="> </div>
     <div class="M3" id="MBDQE5ZiDsQ="> </div>
     <div class="M4" id="c8zxLt/4Iuk="> </div>
     <div class="M5" id="tPciMWg0pmg="> </div>
     <div class="M6" id="/XZw4C/lGEk="> </div>
   </body>
 </html>
```

Figura 1: Vista al inspeccionar la pagina.

Para detectar el cifrado utilizado por el informante, se opta por inspeccionar el sitio web como se puede observar en la imagen 2.1, viendo el texto plano entre los "tags" "p" y notando hay 6 lineas con "tags" "div" que contienen una sección "id" con textos de 11 caracteres en base 64 con 1 carácter para "padding" en cada uno.

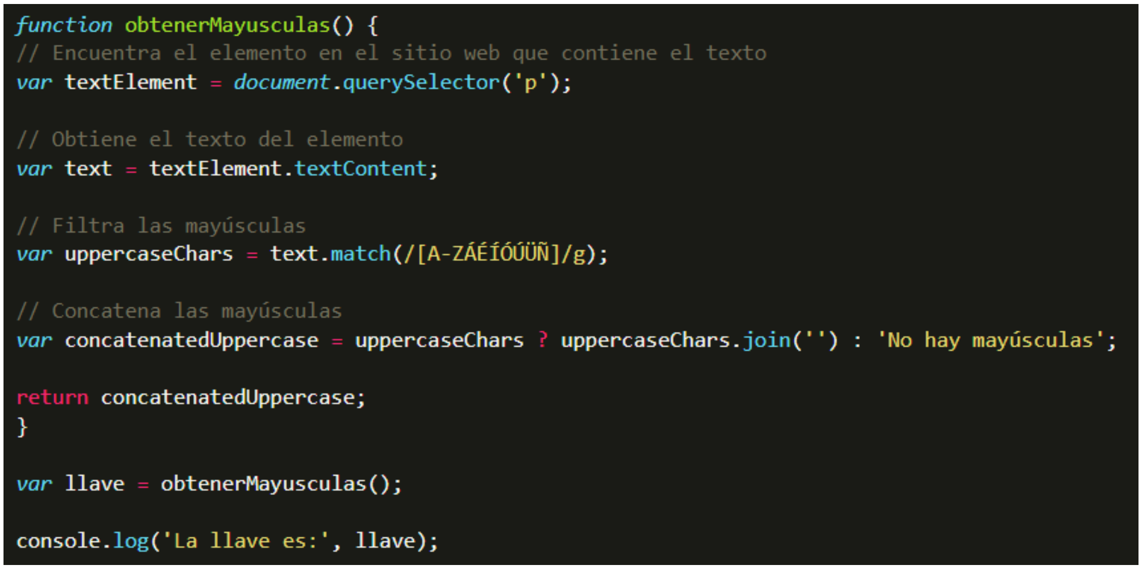
En este laboratorio al tener solo una llave para cifrar un mensaje, se puede pensar que se está trabajando con un algoritmo de cifrado simétrico.

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

Para que el "script" solo pueda usarse en el sitio del informante se agrega la siguiente linea de código:

```
// @match        https://cripto.tiiny.site/*
```

2.3. Define función que obtiene automáticamente el password del documento

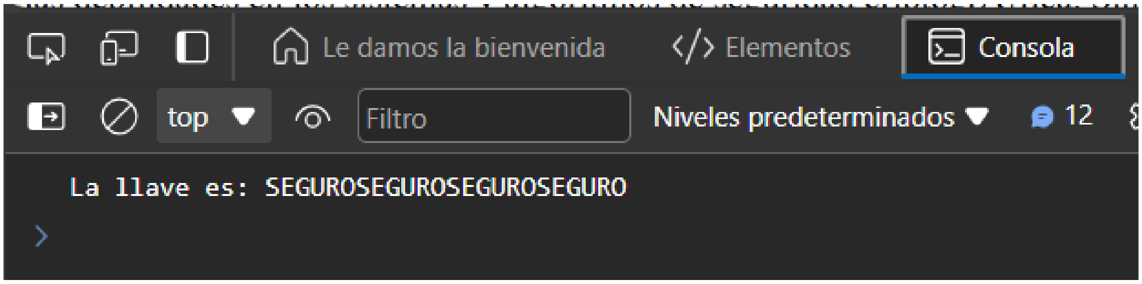


```
function obtenerMayusculas() {
// Encuentra el elemento en el sitio web que contiene el texto
var textElement = document.querySelector('p');

// Obtiene el texto del elemento
var text = textElement.textContent;

// Filtra las mayúsculas
var uppercaseChars = text.match(/[A-ZÁÉÍÓÚÜÑ]/g);

// Concatena las mayúsculas
var concatenatedUppercase = uppercaseChars ? uppercaseChars.join('') : 'No hay mayúsculas';

return concatenatedUppercase;
}

var llave = obtenerMayusculas();

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

Figura 2: Función de obtención de password.

La función del código mostrado en la imagen 2.3 obtiene la llave del sitio web. Se utiliza ”console.log” para mostrar la llave en consola en el formato pedido. Se debe mencionar que el código finalmente utilizado para este laboratorio fue extraído de otro repositorio, el cual es pertinentemente referenciado en la entrega final (`https://github.com/cesarlmt27/CIT2113/tree/main/Laboratorio%204`).

2.4. Muestra la llave por consola



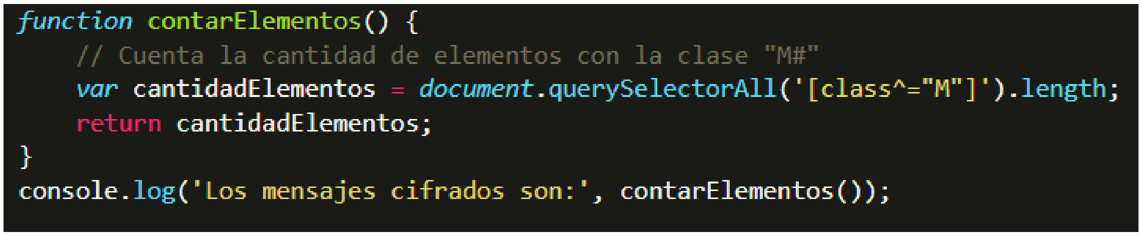
```
La llave es: SEGUROSEGUROSEGUROSEGURO
```

Figura 3: Obtención de la llave por consola.

En la imagen 2.4 se puede ver la llave por consola siendo esta: ”SEGUROSEGUROSEGUROSEGURO”.

3. Desarrollo (Parte 2)

3.1. Reconoce automáticamente la cantidad de mensajes cifrados

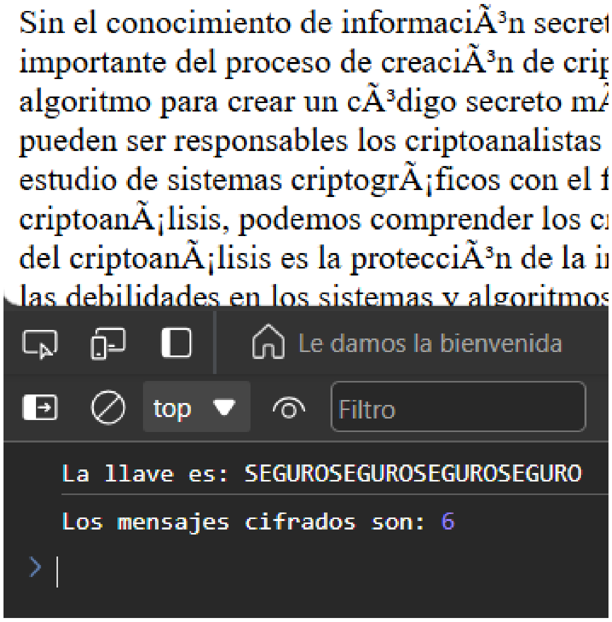


```
function contarElementos() {
    // Cuenta la cantidad de elementos con la clase "M#"
    var cantidadElementos = document.querySelectorAll('[class^="M"]').length;
    return cantidadElementos;
}
console.log('Los mensajes cifrados son:', contarElementos());
```

Figura 4: Función para retornar la cantidad de mensajes cifrados.

La función de la imagen 3.1 cuenta la cantidad de elementos en donde se tenga la clase ”M”, esto debido a que todos los mensajes cifrados cuentan con ella, tal como se ve en la imagen 2.1.

3.2. Muestra la cantidad de mensajes por consola



Sin el conocimiento de informaciÃ³n secret
importante del proceso de creaciÃ³n de cri
algoritmo para crear un cÃ³digo secreto m
pueden ser responsables los criptoanalistas
estudio de sistemas criptogrÃ¡ficos con el
criptoanÃ¡lisis, podemos comprender los c
del criptoanÃ¡lisis es la protecciÃ³n de la
las debilidades en los sistemas y algoritmos

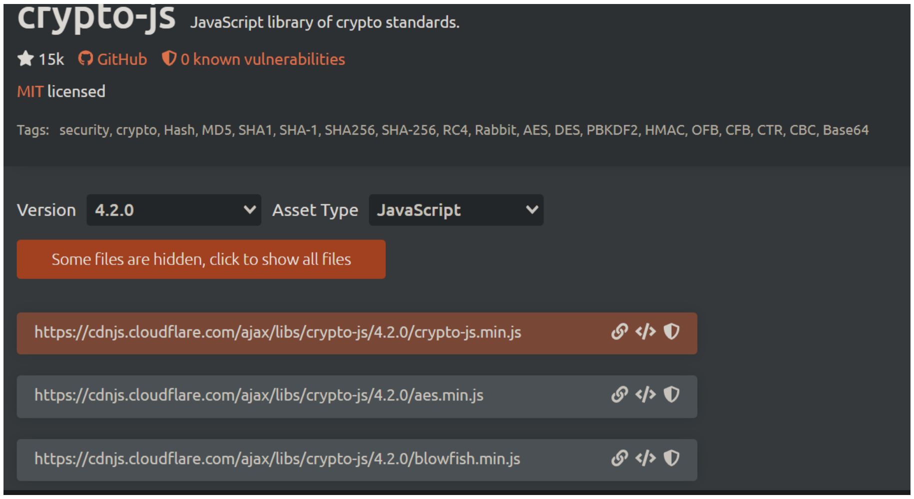
```
La llave es: SEGUROSEGUROSEGUROSEGURO
Los mensajes cifrados son: 6
```

Figura 5: Función para obtención de cantidad de mensajes.

La imagen 3.2 muestra por consola la cantidad de mensajes cifrados del sitio web.

4. Desarrollo (Parte 3)

4.1. Importa la librería cryptoJS


crypto-js JavaScript library of crypto standards.

15k GitHub 0 known vulnerabilities

MIT licensed

Tags: security, crypto, Hash, MD5, SHA1, SHA-1, SHA256, SHA-256, RC4, Rabbit, AES, DES, PBKDF2, HMAC, OFB, CFB, CTR, CBC, Base64

Version 4.2.0 Asset Type JavaScript

Some files are hidden, click to show all files

https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/crypto-js.min.js

https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/aes.min.js

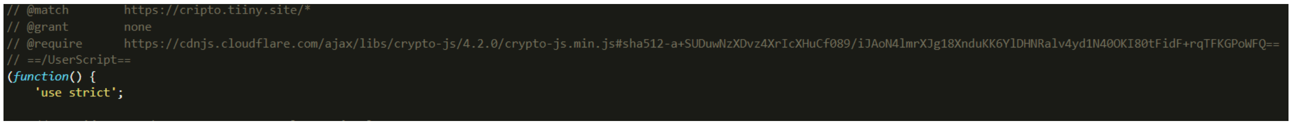
https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/blowfish.min.js

Figura 6: Pagina de donde se extrajo la librería.

La librería se obtiene de la pagina del la imagen 4.1, cuya ”url” es la siguiente, ”`https://cdnjs.com/libraries/crypto-js`”. Se importa ”crypto-js” copiando la ”url” correspondiente a ”`https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/crypto-js.min.js`” y se agrega a la linea ”@require” como se muestra a continuación:

```
// @require https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/crypto-js.
```

4.2. Utiliza SRI en la librería CryptoJS



```
// @match        https://cripto.tiiny.site/*
// @grant        none
// @require      https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/crypto-js.min.js#sha512-a+SUDuwNzXDvz4XrIcXHuCf089/iJAoN4lmrXJg18XnduKK6YlDHNRalv4yd1N40OKI80tFidF+rqTFKGPoWFQ==
// ==/UserScript==
(function() {
    'use strict';
```

Figura 7: SRI hash.

Se copia de la misma pagina mostrada en la imagen 4.1 la SRI Hash apretando en el simbolo del escudo. Para usarla se agrega al ”@require” un ”#” junto a la librería ”cryptoJs” para luego agregar el SRI copiado, tal como se ve en la imagen 4.2.

`https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/crypto-js.min.js#sha512-a+SUDuwNzXDvz4XrIcXHuCf089/iJAoN4lmrXJg18XnduKK6YlDHNRalv4yd1N40OKI80tFidF+rqTFKGPoWFQ==`

4.3. Repercusiones de SRI inválido

El ”SRI” permite verificar a los navegadores si los recursos obtenidos se entregan sin manipulaciones por medio de un ”Has” criptográfico. Un ”SRI” inválido es cuando el ”Hash” de un archivo no coincide con el ”Hash” del ”HTML” que carga el recurso. Algunas repercusiones que podría tener el uso de un SRI invalido según la pagina `https://dev.to/inchukwudi/understanding-subresource-integrity-sri-3ep7` son:

- Bloqueo de recursos al encontrar un hash que no coincide.
- Corromper la funcionalidad del sitio web.

4.4. Logra decifrar uno de los mensajes

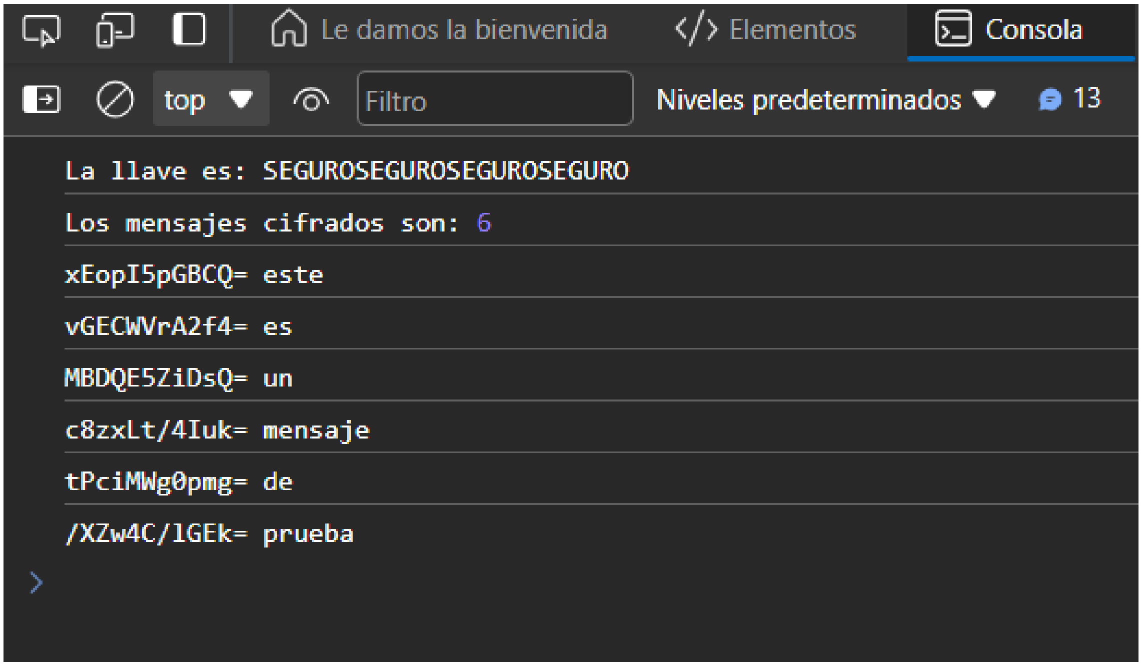
Como se trabaja en con solo una llave en un mensaje cifrado se puede asumir que se requiere de un algoritmo de cifrado simétrico, llegando a probar 3DES en modo ECB, el cual permitió obtener un mensaje descifrado legible. Por ejemplo el mensaje descifrado de ”xEopI5pGBCQ=” es : ”este”.

4.5. Imprime todos los mensajes por consola

```
function obtenerYDescifrarMensajes() {
    // Selecciona todos los elementos div con la clase "M#"
    var mensajeElements = document.querySelectorAll('[class^="M"]');

    // Itera sobre cada elemento y obtiene el id y contenido cifrado
    mensajeElements.forEach(function(mensajeElement) {
        var id = mensajeElement.id;

        // Descifra el mensaje utilizando 3DES en modo ECB
        var mensajeDescifrado = CryptoJS.TripleDES.decrypt({
            ciphertext: CryptoJS.enc.Base64.parse(id)
        }, CryptoJS.enc.Utf8.parse(llave), {
                mode: CryptoJS.mode.ECB,
                padding: CryptoJS.pad.Pkcs7
            }).toString(CryptoJS.enc.Utf8);

        console.log(id + ' ' + mensajeDescifrado);

        // Muestra el id descifrado en el div correspondiente
        mensajeElement.innerHTML = mensajeDescifrado;
    });
}
// Llama a la función para obtener y descifrar mensajes
obtenerYDescifrarMensajes();
```

Figura 8: Función para obtención de mensajes.

En la imagen 4.5 se ve la función utilizada para obtener los mensajes cifrados indicando que se utilice ”TripleDES”. La función selecciona todos los elementos ”div” con una clase que comience con ”M”, descifra los mensajes utilizando el algoritmo 3DES en modo ECB(”CryptoJS.TripleDES.decrypt”) y muestra el resultado descifrado en el mismo elemento ”div”.

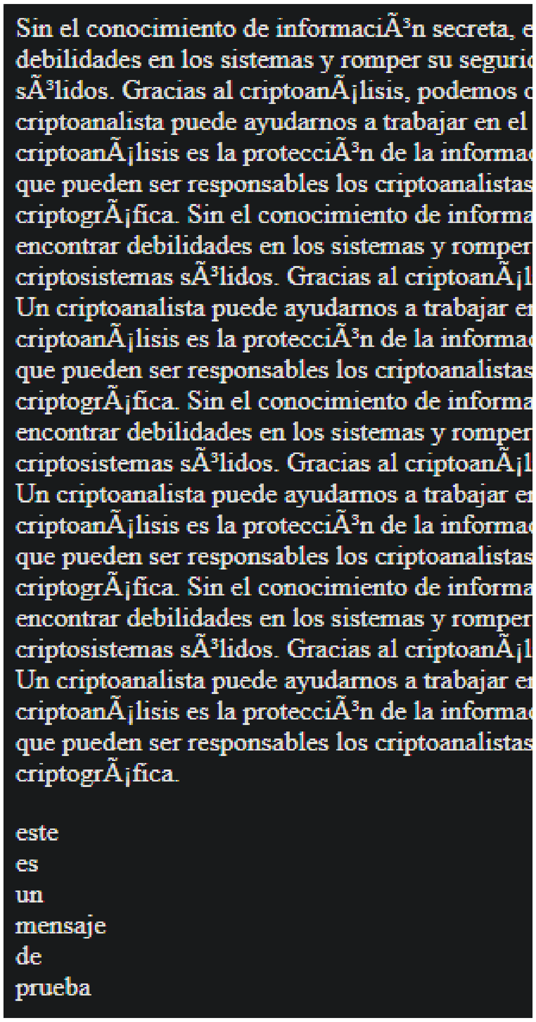


```
La llave es: SEGUROSEGUROSEGUROSEGURO
Los mensajes cifrados son: 6
xEopI5pGBCQ= este
vGECWVrA2f4= es
MBDQE5ZiDsQ= un
c8zxLt/4Iuk= mensaje
tPciMWg0pmg= de
/XZw4C/1GEk= prueba
```

Figura 9: Mensajes mostrados por consola.

En la imagen 4.5 se ven los mensajes descifrados en consola.

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



```
Sin el conocimiento de informaciÃ³n secreta, e
debilidades en los sistemas y romper su seguri
sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos
criptoanalista puede ayudarnos a trabajar en el
criptoanÃ¡lisis es la protecciÃ³n de la informa
que pueden ser responsables los criptoanalistas
criptogrÃ¡fica. Sin el conocimiento de informa
encontrar debilidades en los sistemas y romper
criptosistemas sÃ³lidos. Gracias al criptoanÃ¡l
Un criptoanalista puede ayudarnos a trabajar e
criptoanÃ¡lisis es la protecciÃ³n de la informa
que pueden ser responsables los criptoanalistas
criptogrÃ¡fica. Sin el conocimiento de informa
encontrar debilidades en los sistemas y romper
criptosistemas sÃ³lidos. Gracias al criptoanÃ¡l
Un criptoanalista puede ayudarnos a trabajar e
criptoanÃ¡lisis es la protecciÃ³n de la informa
que pueden ser responsables los criptoanalistas
criptogrÃ¡fica. Sin el conocimiento de informa
encontrar debilidades en los sistemas y romper
criptosistemas sÃ³lidos. Gracias al criptoanÃ¡l
Un criptoanalista puede ayudarnos a trabajar e
criptoanÃ¡lisis es la protecciÃ³n de la informa
que pueden ser responsables los criptoanalistas
criptogrÃ¡fica.

este
es
un
mensaje
de
prueba
```

Figura 10: Obtención de mensajes.

En la imagen 4.6 se muestran los mensajes directamente en la pagina, notando el ”este es un mensaje de prueba”.

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

El código no fuerza la entrada de valores buscados, obteniendo toda la información del sitio web (llave, cantidad de mensajes, mensajes cifrados).

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

`https://github.com/kasorio/cripto_lab4`

Conclusiones y comentarios

Para resumir, en esta experiencia se realiza un script que permita obtener la llave de los mensajes cifrados en la pagina web indicada en laboratorio y que muestre los mensajes descifrados.

En esta experiencia de laboratorio se logra cumplir con las actividades solicitadas, adquiriendo aprendizaje del desarrollo y uso de scripts usando la extinción "Tampermonkey".

Aunque se logran los objetivos, se mantuvieron presentes algunas dificultades el cumplimiento total de las actividades.

- **Errores al ejecutar los scripts**: Al principio no se tenia en cuenta el efecto de las otras exenciones que podía tener el computador utilizado, al notar que exenciones como los bloqueadores de anuncios mostraban algunos errores al inspeccionar en consola, se opta por apagar las exenciones innecesarias para evitar cualquier otro problema.
- **Nula experiencia en Javascript**: Hasta el momento se a acumulado muy poca experiencia en este lenguaje de programación, sin embargo gracias a la documentación de Javascript se pudo lograr entender a tiempo el funcionamiento `https://developer.mozilla.org/en-US/docs/Web/API/Document/querySelector`.
- **Problemas para encontrar el algoritmo de cifrado**: Este punto no se logro por medio de la prueba y error, la asesoría con estudiantes de semestres anteriores permitió saber que modo de 3DES era el correcto para utilizar.
- **Obtención del mensaje descifrado correcto**: Si bien el mensaje encontrado era legible y tenia sentido, se requería encontrar la forma de corroborar estos datos, se opta por utilizar descifradores en la web a los que se le entregan los datos necesarios para realizar las comprobaciones, corroborando la obtención de los mensajes.

Issues