Informe Laboratorio 4

Sección 2

Santiago Larraín Morales
e-mail: Santiago.Larrain@mail.udp.cl

Noviembre de 2023

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:

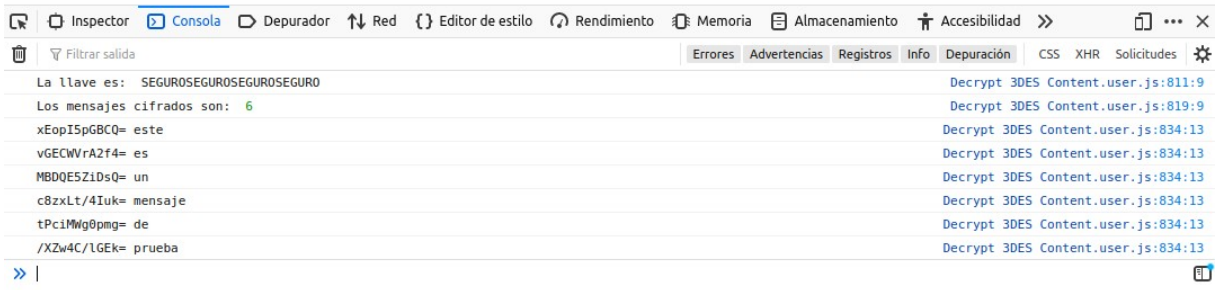
   - La llave es: KEY

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.

este
es
un
mensaje
de
prueba

```
La llave es:  SEGUROSEGUROSEGUROSEGURO          Decrypt 3DES Content.user.js:811:9
Los mensajes cifrados son:  6                  Decrypt 3DES Content.user.js:819:9
xEopI5pGBCQ= este                             Decrypt 3DES Content.user.js:834:13
vGECWVrA2f4= es                               Decrypt 3DES Content.user.js:834:13
MBDQE5ZiDsQ= un                               Decrypt 3DES Content.user.js:834:13
c8zxLt/4Iuk= mensaje                          Decrypt 3DES Content.user.js:834:13
tPciMWg0pmg= de                               Decrypt 3DES Content.user.js:834:13
/XZw4C/lGEk= prueba                           Decrypt 3DES Content.user.js:834:13
»
```

2. Desarrollo (Parte 1)

2.1. Detecta el cifrado utilizado por el informante

Para detectar el cifrado utilizado por el informante, se analizó la imagen entregada en el paso 3. Observando la imagen, se indica la llave con "La llave es: SEGUROSEGUROSEGUROSEGURO". Luego, usando esto como punto de referencia, nos enfocamos en el texto.

Después de leer el texto y buscar patrones, observamos que existe una relación entre la contraseña y las mayúsculas del texto, comenzando desde la parte del texto donde aparece la primera letra mayúscula y el primer carácter de la clave, y así sucesivamente.

2.2. Logra que el script solo se active en el sitio utilizado por el informante

Para asegurarnos de que nuestro script funcione solo en las páginas web pertinentes, hemos agregado la directiva `@match https://cripto.tiiny.site/` en la sección **==UserScript==**.

La directiva **@match** indica que el script se ejecutará en el sitio web **https://cripto.tiiny.site/** y en sus subdominios.

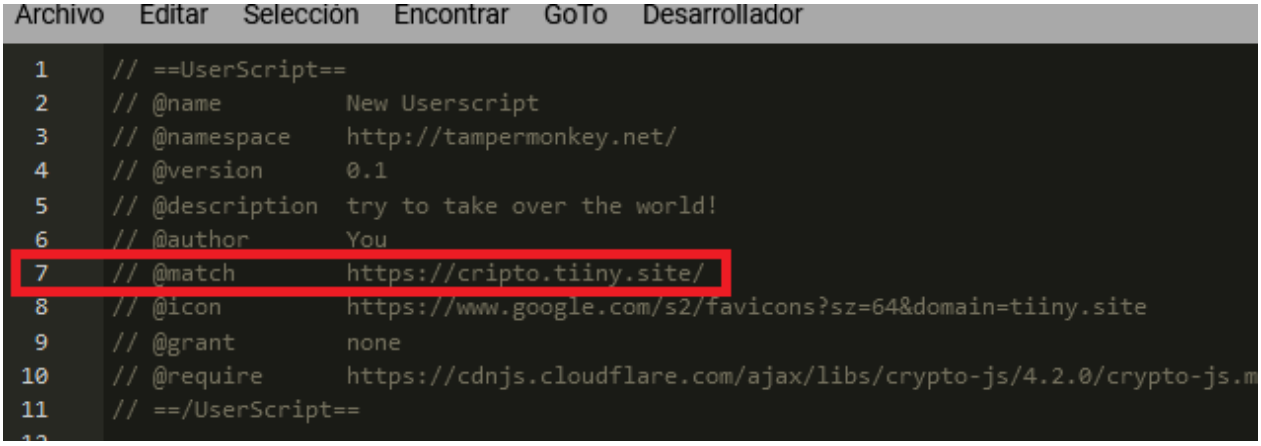


Figura 1: Implementación de la directiva @match.

2.3. Define función que obtiene automáticamente el password del documento

```
1 // Obtén el párrafo de la página
2 var parrafo = document.querySelector('p'); // Puedes ajustar el
     selector según tu HTML
3
```

```
4  // Función para obtener la clave a partir de las letras mayú
       sculas del párrafo
5  function obtenerClaveDesdeParrafo(parrafo) {
6    var clave = '';
7    var texto = parrafo.textContent;
8
9    for (var i = 0; i < texto.length; i++) {
10     var caracter = texto[i];
11     if (caracter === caracter.toUpperCase() && caracter.match(/[A
           -Z]/)) {
12       clave += caracter;
13     }
14   }
15
16   return clave;
17 }
18
19 // Obtiene la clave
20 var clave = obtenerClaveDesdeParrafo(parrafo);
21
22 // Imprime la clave en la consola
23 console.log('La llave es: ' + clave);
```

Listing 1: Codigo Parte 1 obtencion Key

2.4. Muestra la llave en la consola

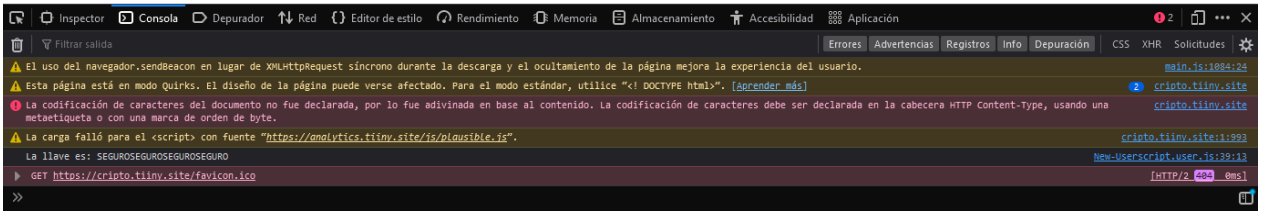


Figura 2: Mostrar la clave obtenida en la consola.

La clave obtenida es: SEGUROSEGUROSEGUROSEGURO

3. Desarrollo (Parte 2)

```
1  // Función para contar y mostrar la cantidad de mensajes cifrados
2  function contarMensajesCifrados() {
3    var mensajesCifrados = document.querySelectorAll('div[class^="M
       "]');
4    var cantidadMensajesCifrados = mensajesCifrados.length;
5
6    console.log('Los mensajes cifrados son: ' +
       cantidadMensajesCifrados);
7    mensajesCifrados.forEach(function (mensajeCifrado) {
8      var id = mensajeCifrado.id;
9      console.log('Los mensajes cifrados son: ' + id);
10   });
11 }
12
13 // Llama a la función para contar y mostrar los mensajes cifrados
14 contarMensajesCifrados();
```

Listing 2: example

3.1. Reconocimiento automático de la cantidad de mensajes cifrados

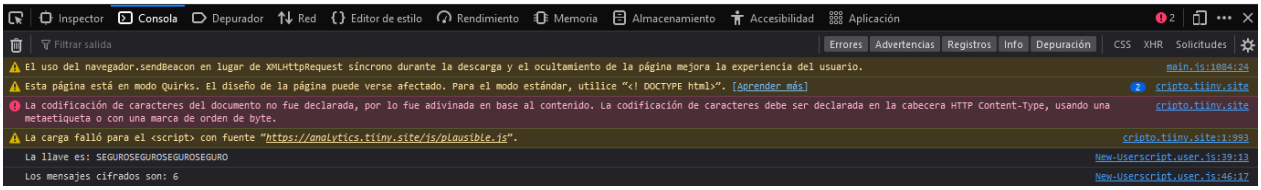


Figura 3: Mensajes cifrados detectados.

Figura 4: Cantidad de mensajes cifrados detectados.

3.2. Mostrar la cantidad de mensajes por consola

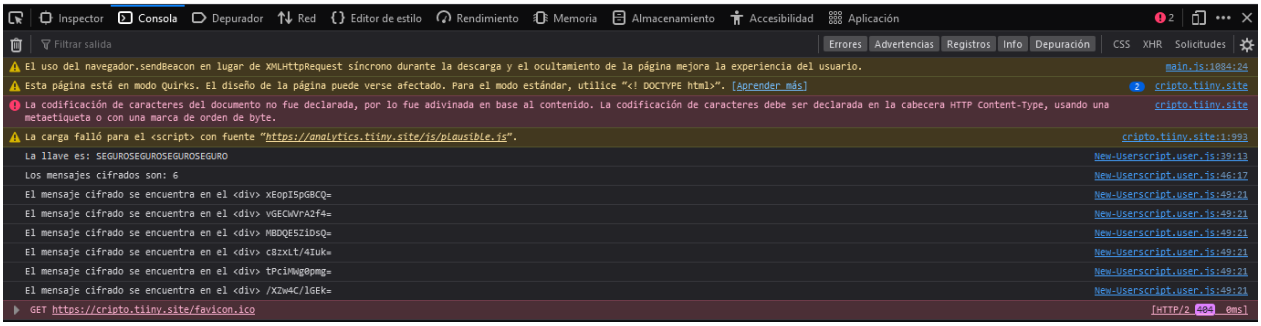


Figura 5: Mensajes cifrados detectados.

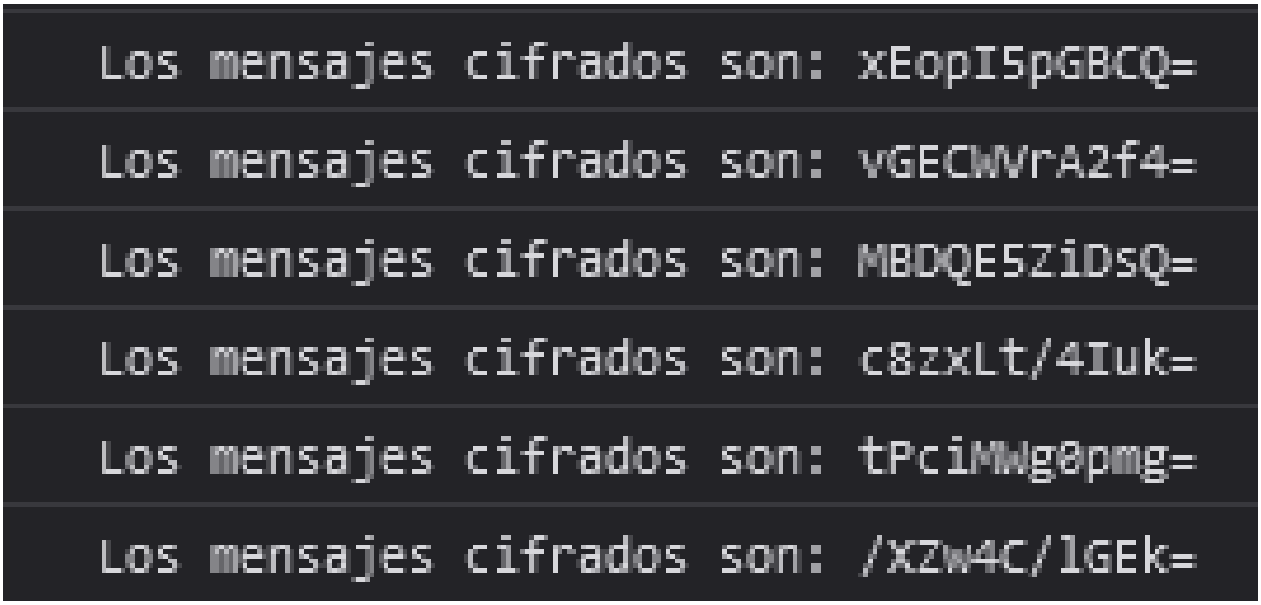


Figura 6: Mensajes cifrados detectados.

4. Desarrollo (Parte 3)

4.1. Importa la librería CryptoJS y utiliza SRI en la librería CryptoJS

Para importar la librería CryptoJS, primero se debe visitar la página `https://cdnjs.com/libraries/crypto-js`. Utiliza la primera opción. Luego, en la sección **==UserScript==**, agrega la línea `// @require` seguida del URL de la primera opción de la librería. A continuación, agrega un # seguido del valor hash SRI `sha512-a+SUDuwNzXDvz4XrIcXHuCf089/iJAoN4lm`
El fragmento de código resultante se muestra a continuación:

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

(Por motivos de formato del informe, el SRI se dividió en 2 partes, pero son una sola).

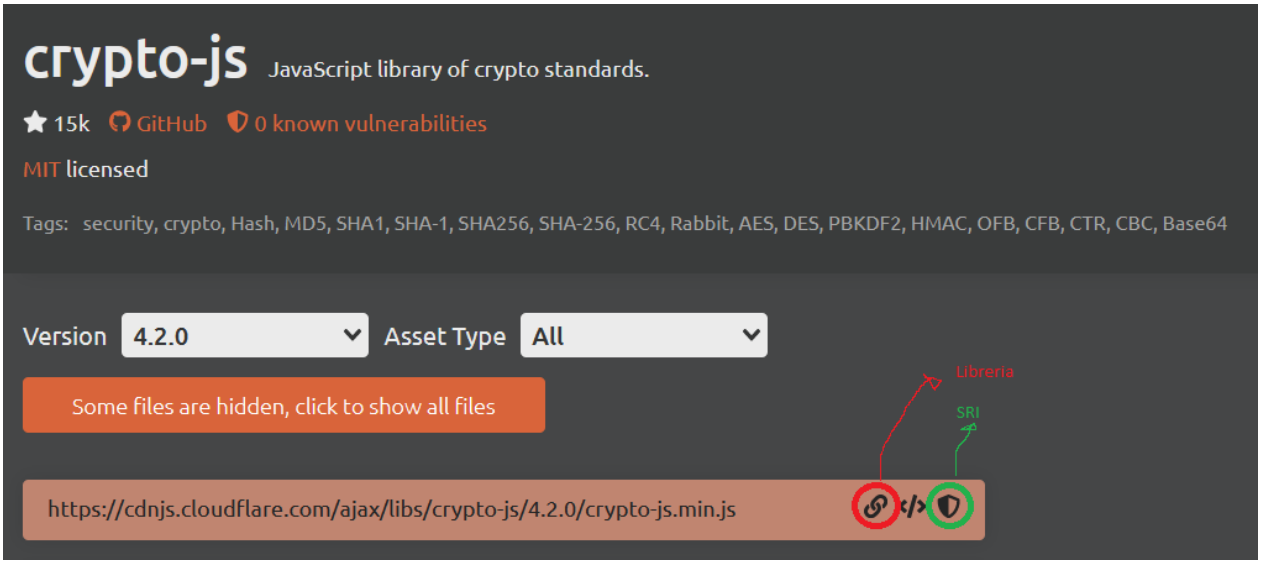


Figura 7: Cómo obtener la librería y el SRI.

4.2. Descifra uno de los mensajes

Para determinar el algoritmo de cifrado a utilizar, se debe observar la imagen de referencia para el paso 3. Se puede notar que aparece a la derecha de cada mensaje cifrado-descifrado la opción **Decrypt 3DES**. Esto sugiere que el algoritmo de cifrado utilizado por el informante es 3DES.

Figura 8: Algoritmo 3DES en la imagen de referencia.

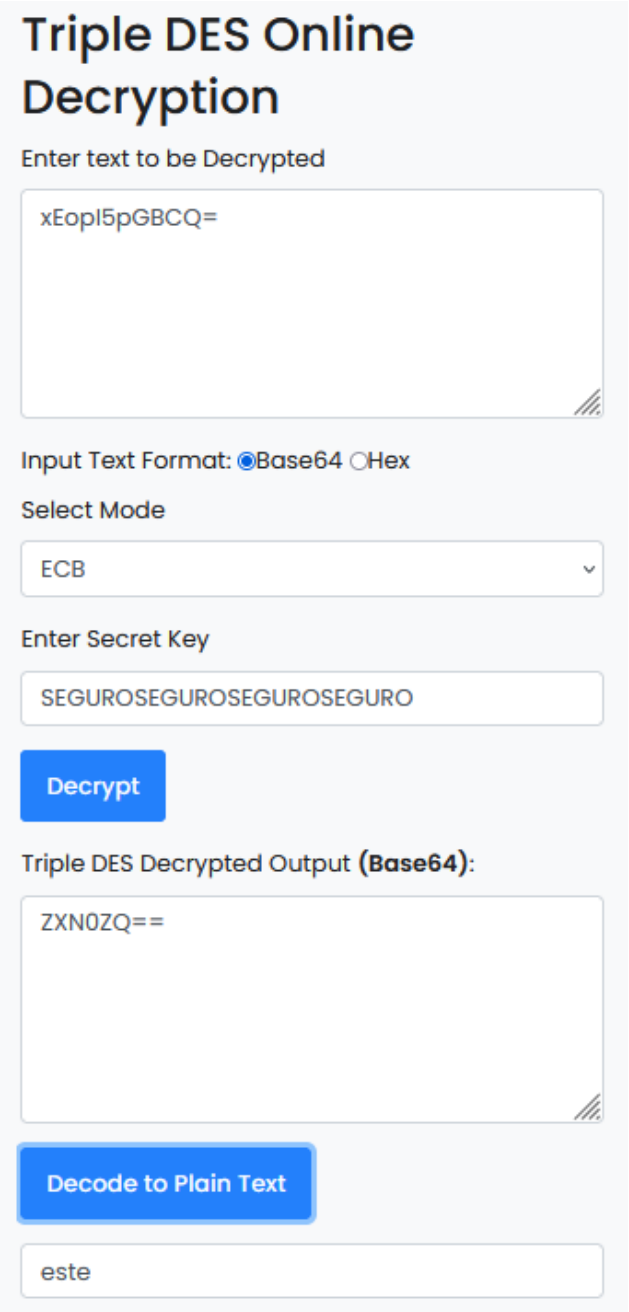


Figura 9: Prueba de descifrado de un mensaje usando 3DES, mensaje cifrado obtenido y la clave encontrada.

Como se puede observar al descifrar el primer mensaje capturado con la clave obtenida en la parte 1 utilizando un descifrador web, se obtuvo una palabra similar a la mostrada en el ejemplo. Por lo tanto, se puede suponer que tanto el algoritmo como la clave son correctos.

Una vez que se sabe qué algoritmo se está utilizando, se implementa una función para descifrar los mensajes capturados y luego mostrarlos por consola en el formato "mensaje cifrado - mensaje descifrado".

```
function contarMensajesCifrados2() {
    var mensajesCifrados = document.querySelectorAll('div[class^="M"]');
    var cantidadMensajesCifrados = mensajesCifrados.length;
    var idsMensajesCifrados = []; // Arreglo para almacenar los IDs
    mensajesCifrados.forEach(function (mensajeCifrado) {
        var id = mensajeCifrado.id;
        idsMensajesCifrados.push(id); // Agregar el ID al arreglo
    });
    return idsMensajesCifrados; // Devolver el arreglo de IDs
}

var idsMensajesCifrados = contarMensajesCifrados2();

function descifrar3DES(ids, clave) {
    var contrasenasDescifradas = [];
    var claveConvertido = CryptoJS.enc.Utf8.parse(clave);
    var claveEnBase64 = CryptoJS.enc.Base64.stringify(claveConvertido);
    for (var i = 0; i < ids.length; i++) {
        var id = ids[i];

        var clave4 = CryptoJS.enc.Base64.parse(claveEnBase64);
        var mensajeCifrado4 = CryptoJS.enc.Base64.parse(id);
        var mensajeDescifrado5 = CryptoJS.TripleDES.decrypt({
            ciphertext: mensajeCifrado4
        }, clave4, {
            mode: CryptoJS.mode.ECB,
            padding: CryptoJS.pad.Pkcs7
        });
        var mensajeDescifradoTexto = CryptoJS.enc.Utf8.stringify(mensajeDescifrado5);
        console.log(id, mensajeDescifradoTexto);
    }
}
var Descifradas = descifrar3DES(idsMensajesCifrados, clave);
```

Listing 3: example

4.3. Imprime todos los mensajes por consola

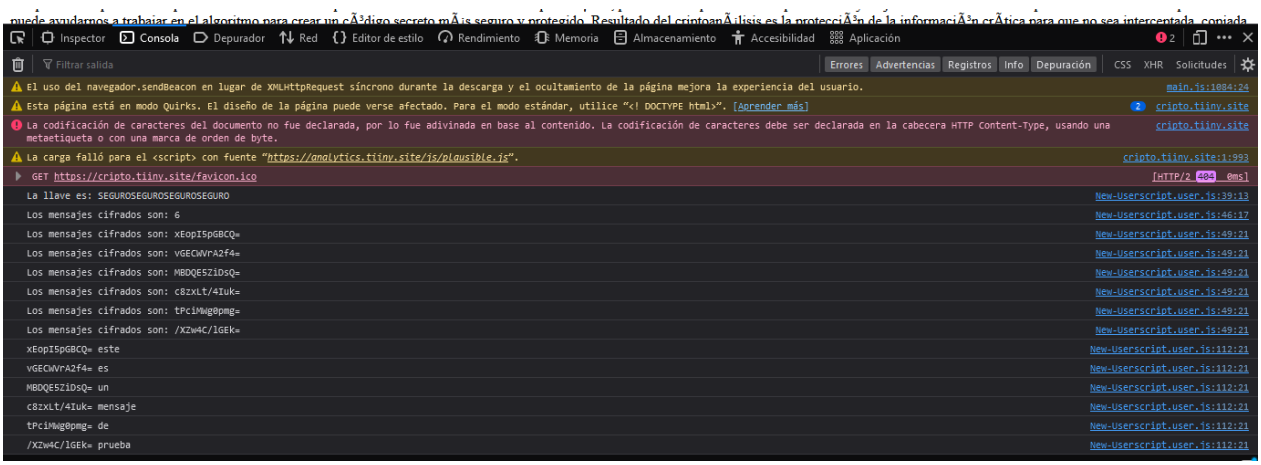


Figura 10: Mostrar los datos obtenidos por la terminal.

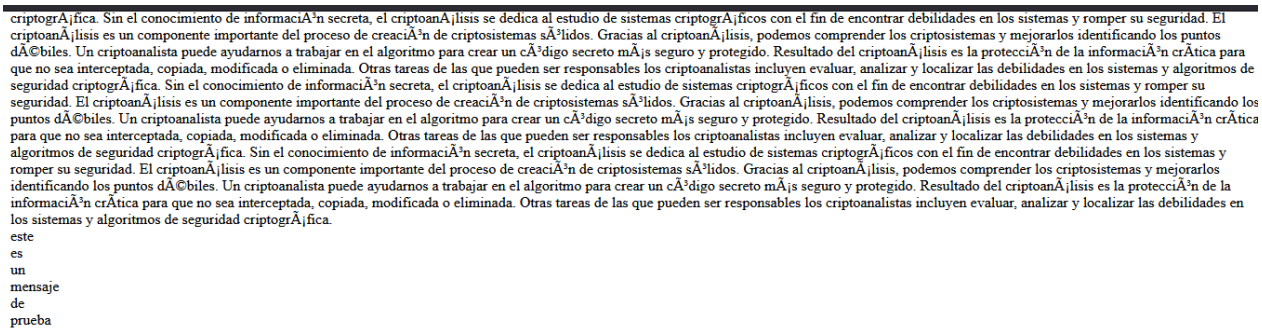
4.4. Muestra los mensajes en texto plano en el sitio web

Para mostrar las palabras cifradas al final del código, se han añadido las siguientes líneas de código que agregan las palabras cifradas al texto proporcionado por el informante.

```
1 // Actualizar el contenido del elemento <p> en el DOM
2 var parrafo = document.querySelector('p'); // Selecciona el único
      elemento <p> en el documento
3 if (parrafo) {
4     // Agregar el mensaje descifrado al párrafo con saltos de lí
        nea
5     parrafo.innerHTML += '<br>' + mensajeDescifradoTexto;
6 }
```

Listing 4: example

Listing 1: Codigo para mostrar las palabras en la pagina



criptogrA¡fica. Sin el conocimiento de informaciA³n secreta, el criptoanA¡lisis se dedica al estudio de sistemas criptogrA¡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 crÃtica 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 crÃtica 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 crÃtica 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.

este
es
un
mensaje
de
prueba

Figura 11: Mostrar los datos obtenidos en la pantalla.

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

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

5. Conclusiones y Comentarios

En este laboratorio, hemos explorado el uso de la herramienta web **Tampermonkey**, que nos permite implementar código en páginas web.

A lo largo de este informe, hemos detallado el proceso para obtener una contraseña proporcionada por un informante. Para ello, extrajimos las letras mayúsculas de un párrafo contenido en la etiqueta ¡p¿del elemento body y las utilizamos para construir una clave con la que descifraremos los mensajes.

Posteriormente, examinamos el código fuente de la página para identificar los mensajes cifrados enviados por el informante. Notamos que se presentaban en elementos ¡div¿con una clase ”M”seguida de un número y un ID en formato Base64, que correspondía al mensaje cifrado. Desarrollamos un código para procesar estos mensajes, separando la clase del ID y almacenando esta información.

Finalmente, logramos descifrar los mensajes cifrados utilizando el algoritmo Triple DES que utilizó el informante. Implementamos un código para desencriptar los mensajes y convertirlos de su formato Base64 a texto plano. Luego, mostramos estos mensajes tanto en la consola como en la página web.

Esta experiencia nos permitió aprender cómo utilizar Tampermonkey junto con JavaScript para descifrar mensajes ocultos. Además, adquirimos habilidades útiles, como la manipulación del DOM y la comprensión de algoritmos de cifrado.

En resumen, este laboratorio nos desafió a utilizar herramientas y conocimientos técnicos para resolver un misterio en una página web, y nos dejó con una mayor comprensión de cómo funcionan los sistemas de cifrado y cómo aplicar nuestras habilidades en situaciones del mundo real.

6. Referencias

- Repositorio de Github.
- Documentación Tampermonkey.
- Documentación CryptoJS.
- Librería cdnjs.
- Pagina de decif rado-cifrado.