Informe Laboratorio 4

Sección 3

Pablo Castro
e-mail: pablo.castro_d@mail.udp.cl

11 de 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:

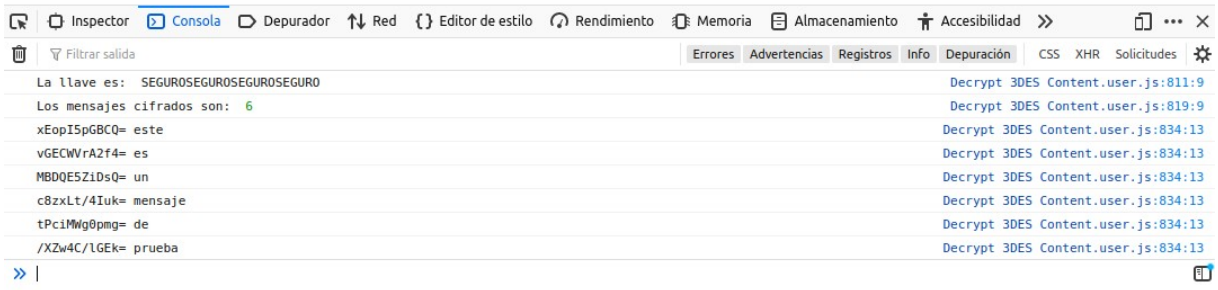
   - La llave es: KEY

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
» |
```

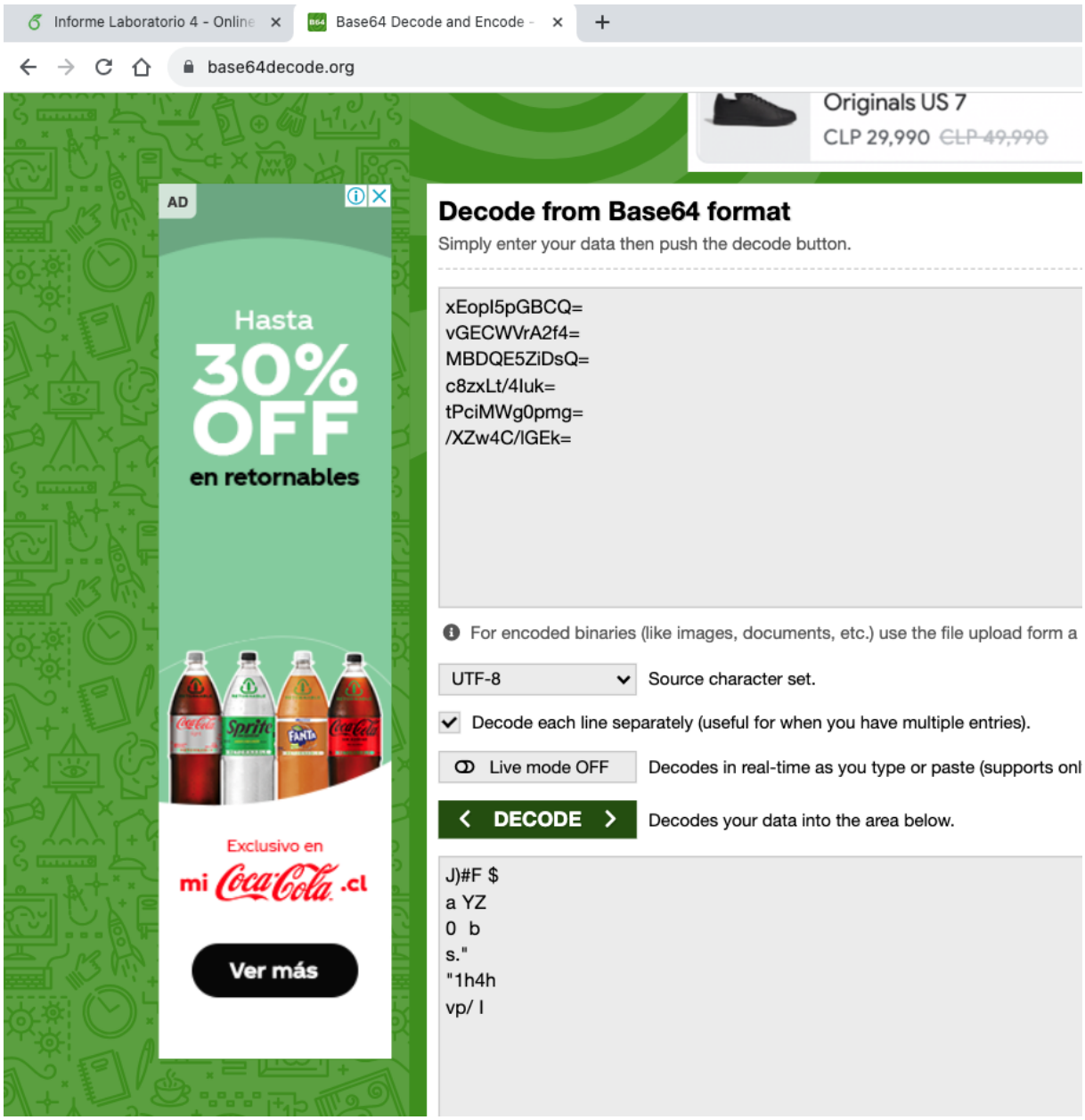
2. Desarrollo (Parte 1)

2.1. Detecta el cifrado utilizado por el informante

De manera visual, al analizar el texto de la página, se encuentra que al concatenar las mayúsculas, se genera la palabra **”SEGUROSEGUROSEGUROSEGURO”** que corresponderá a la KEY para luego descifrar más información. También, al analizar el código fuente de la página, aparecen unos div con mensajes en base 64, estos deben ser los mensajes encriptados del informante.

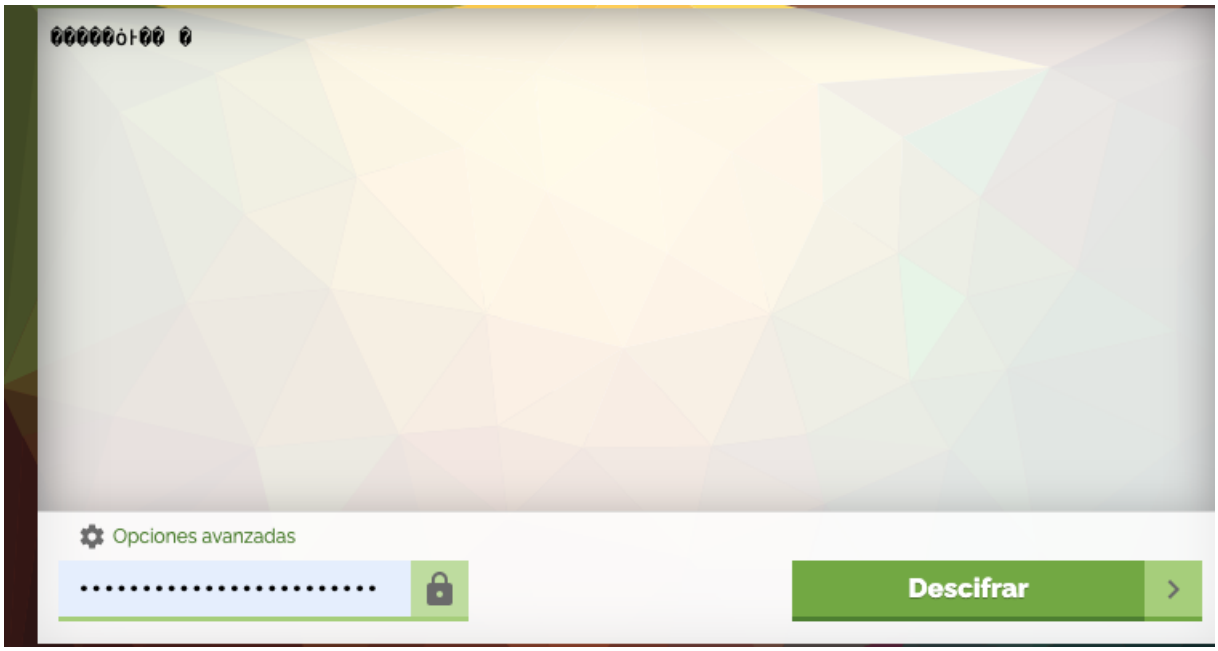
```
2
3  Sin el conocimiento de informaciÃ³n secreta, el crip
4  </p>
5  <div class="M1" id="xEopI5pGBCQ="> </div>
6  <div class="M2" id="vGECWVrA2f4="> </div>
7  <div class="M3" id="MBDQE5ZiDsQ="> </div>
8  <div class="M4" id="c8zxLt/4Iuk="> </div>
9  <div class="M5" id="tPciMWg0pmg="> </div>
10 <div class="M6" id="/XZw4C/lGEk="> </div>
11
```

Para saber que tipo de cifrado utiliza, primero se deben decodificar los mensajes en base 64, para esto se utilizará el siguiente sitio web https://www.base64decode.org/(Enlace a un sitio externo.).

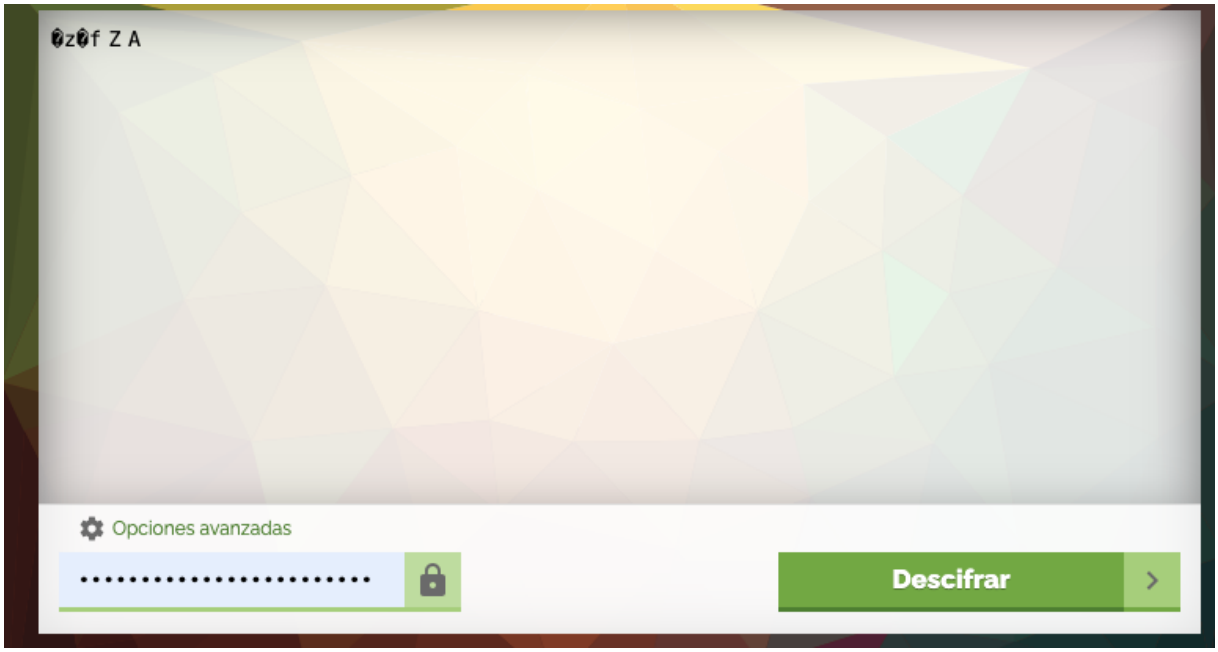


Se puede apreciar que la decodificación no entregó mensaje con algún sentido, lo que indica que está encriptado. Para saber exactamente que tipo de encriptación es, se probarán AES,DES y 3DES que son los que más hemos visto en clases. Como no se ha encontrado un vector de inicialización, y solo la key, "SEGUROSEGUROSEGUROSEGURO", se probará con el modo ECB, sin modificaciones. Para esto se utilizará el sitio web https://cifraronline.com/(Enlace a un sitio externo.). Estos fueron los resultados:

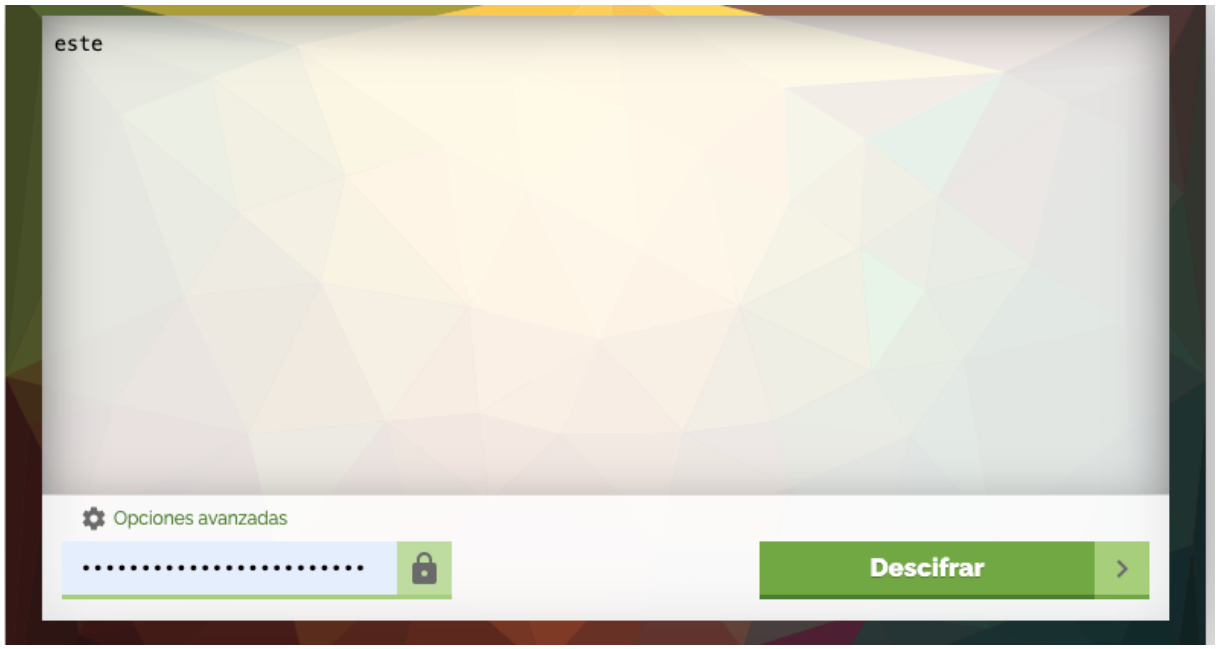
AES:


Opciones avanzadas
Descifrar

DES:


Opciones avanzadas
Descifrar

3DES:



Por ende la KEY es ***"SEGUROSEGUROSEGUROSEGURO"*** y el cifrado es **3DES con modo ECB.**

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

Para evitar que el código se ejecute en cualquier sitio, en el script se utiliza " ***"@match https://cripto.tiiny.site/"*** Esto literalmente hace que el script se ejecute solo cuando la url coincida con el sitio del informante.

2.3. Define función que obtiene automáticamente el password del documento

Script:

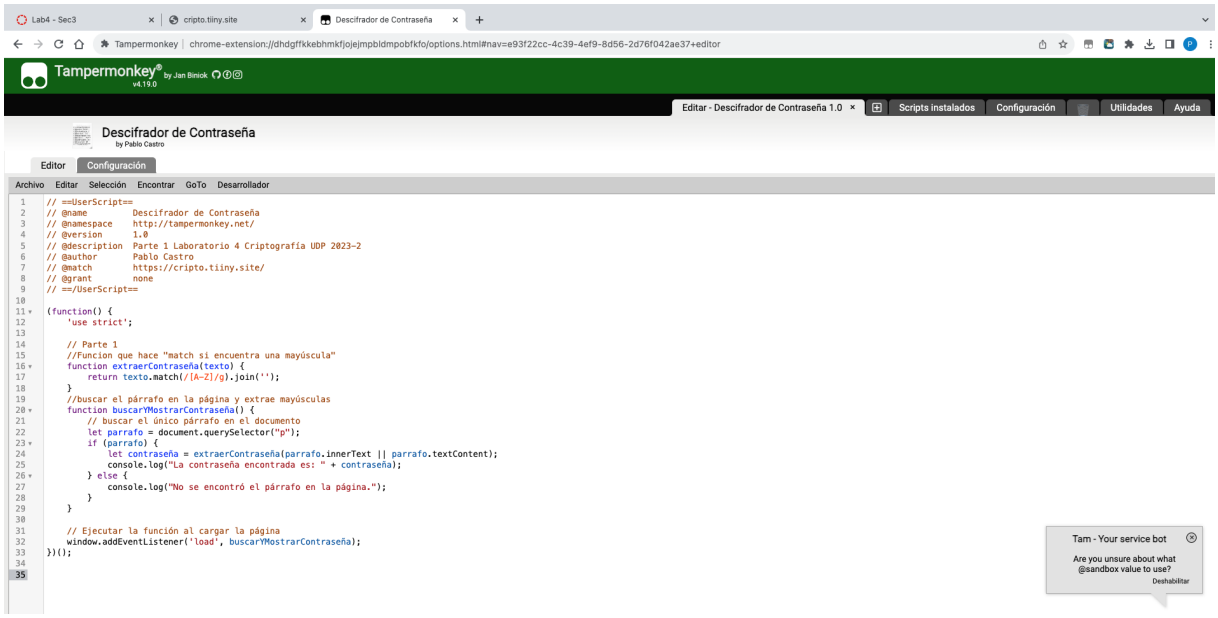
```
// ==UserScript==
// @name         Descifrador de Contraseña
// @namespace    http://tampermonkey.net/
// @version      1.0
// @description  Parte 1 Laboratorio 4 Criptografía UDP 2023.2
// @author       Pablo Castro
// @match        https://cripto.tiiny.site/
// @grant        none
// ==/UserScript==
```

```
(function() {
    'use strict';
    // Parte 1
    //Funcion que hace "match si encuentra una mayúscula"
    function extraerContraseña(texto) {
        return texto.match(/[A-Z]/g).join('');
    }
    //buscar el párrafo en la página y extrae mayúsculas
    function buscarYMostrarContraseña() {
        // buscar el único párrafo en el documento
        let parrafo = document.querySelector("p");
        if (parrafo) {
            let contraseña = extraerContraseña(parrafo.innerText || parrafo.textConten
            console.log("La contraseña encontrada es: " + contraseña);
        } else {
            console.log("No se encontró el párrafo en la página.");
        }
    }
    // Ejecutar la función al cargar la página
    window.addEventListener('load', buscarYMostrarContraseña);
})();
```

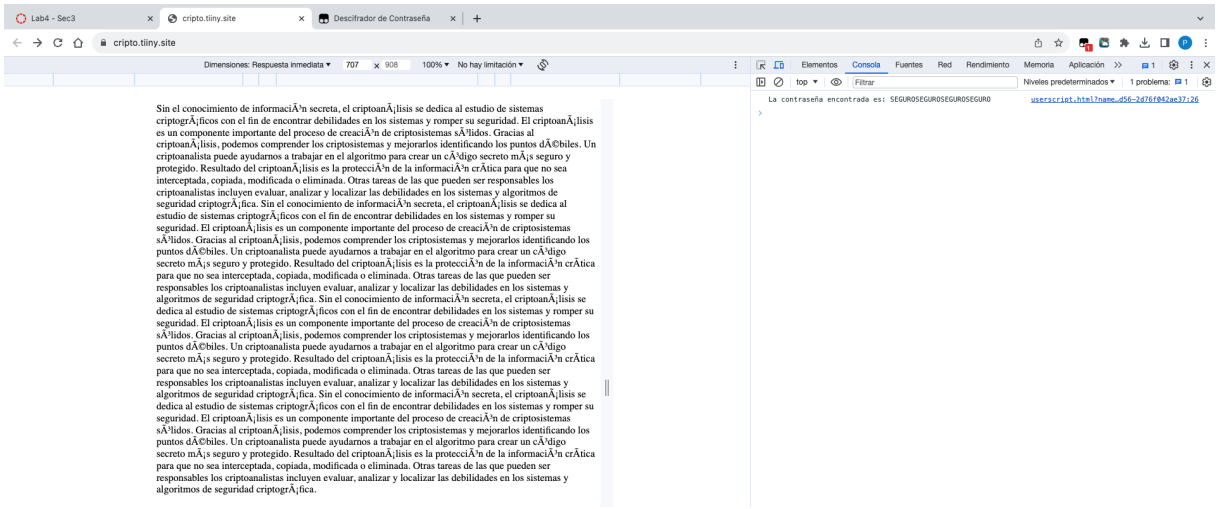
(NOTA: A medida que se pidan mas cosas en este laboratorio, será el mismo código el que se irá ejecutando, con más cosas. Para no caer en redundancia de texto y código, desde aquí en adelante, todos los scripts mostrados serán un complemento del código final adjuntado y sólo se mostrará lo nuevo.)

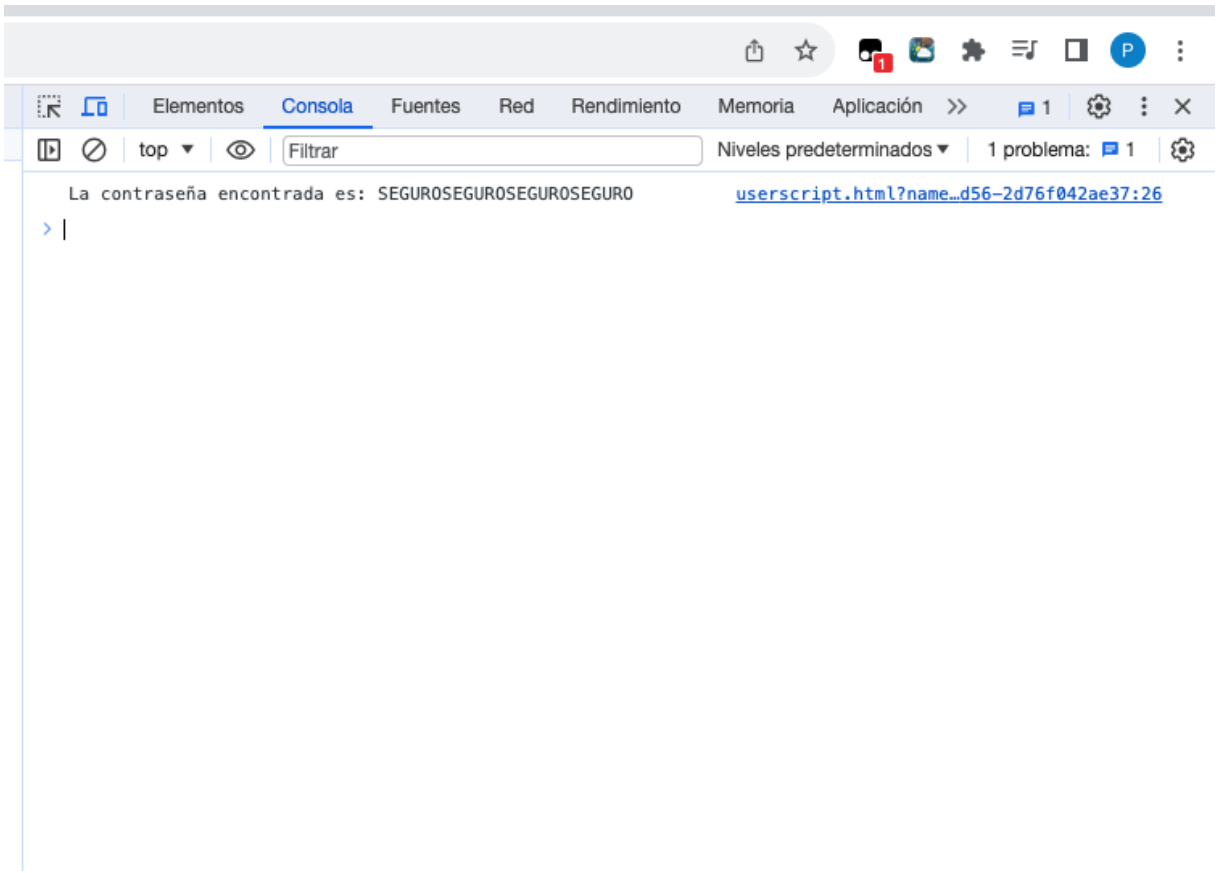
2.4. Muestra la llave por consola

En primer lugar se debe cargar el script en Tampermonkey, el proceso refleja esto:



Ahora este es el resultado en consola:

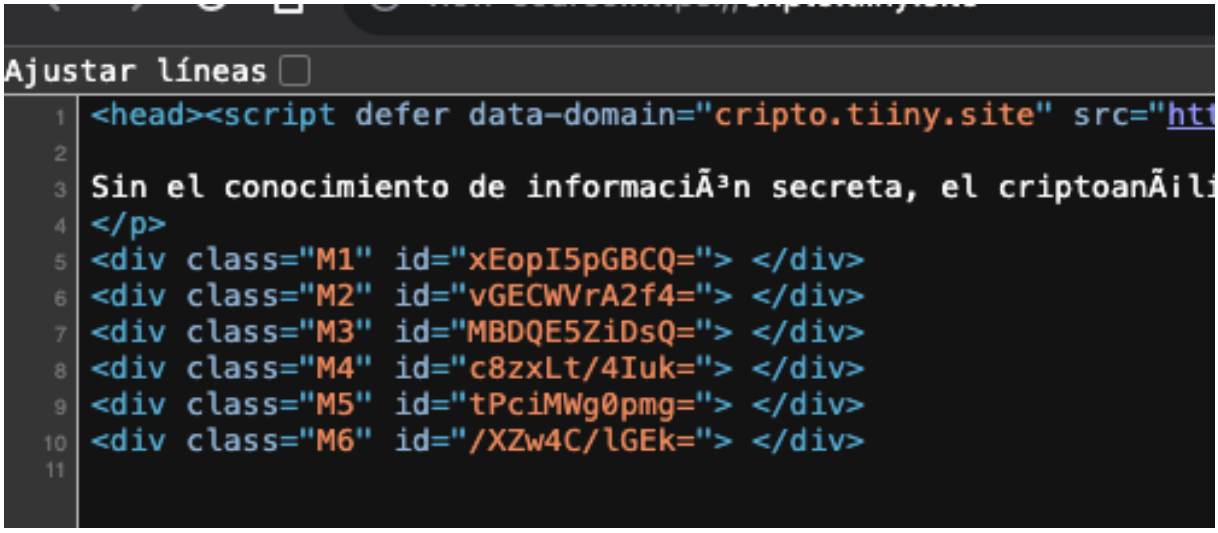



Elementos
Consola
Fuentes
Red
Rendimiento
Memoria
Aplicación
top
Filtrar
Niveles predeterminados
1 problema: 1
La contraseña encontrada es: SEGUROSEGUROSEGUROSEGURO
userscript.html?name…d56-2d76f042ae37:26

3. Desarrollo (Parte 2)

3.1. reconoce automáticamente la cantidad de mensajes cifrados

Los mensajes están ocultos en el html de la página, son estos:

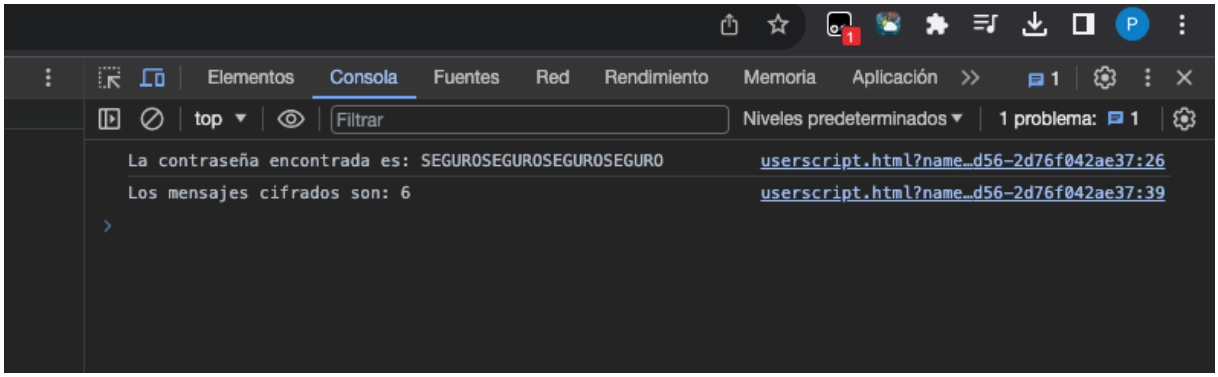


Como los mensajes están entre *«div¿¡/div”*, se añade la siguiente funcion al script para que retorne la cantidad de mensajes que hay por consola. El script agregado es el siguiente:

```
function analizarMensajesCifrados() {
        let divs = document.querySelectorAll("div[id]");
        let contador = 0;
        divs.forEach(div => {
            if (div.id) {
                contador++;
            }
        });
        console.log("Los mensajes cifrados son: " + contador);
    }

    // Ejecutar la función al cargar la página
    window.addEventListener('load', () => {
        buscarYMostrarContraseña();
        analizarMensajesCifrados();
    });
```

3.2. muestra la cantidad de mensajes por consola

El resultado en la consola es el siguiente:



4. Desarrollo (Parte 3)

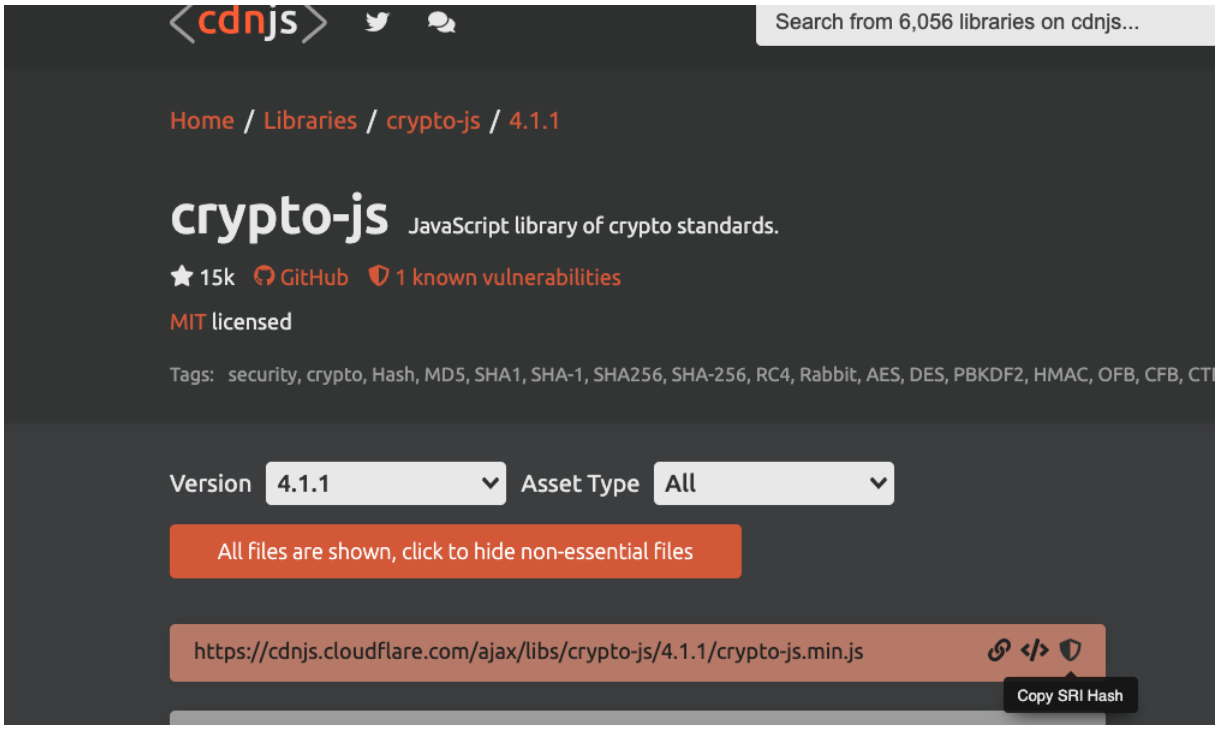
4.1. Importa la librería cryptoJS

Para poder descifrar los mensajes, es necesario importar la librería CryptoJS, desde el siguiente sitio: https://cdnjs.com/libraries/crypto-js(Enlace a un sitio externo.) En el script se agrega la siguiente linea al principio:

```
// @require https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js
```

4.2. Utiliza SRI en la librería CryptoJS

Ahora para utilizar SRI, es necesario copiar un hash que está en la misma página:



Este hash corresponde a:

```
//sha512-E8QSvWZ0eCLGk4km3hxSsNmGWbLtSCSUcewDQPQWZF6pEU8GlT8a5fF32wOl1i8ftdMhssTrF/Ohy
```

Para utilizarlo, hay que importarlo, es decir, concatenarlo con la linea de código anterior, a traves de un "#". Quedando así:

```
// @require https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js#sh
```

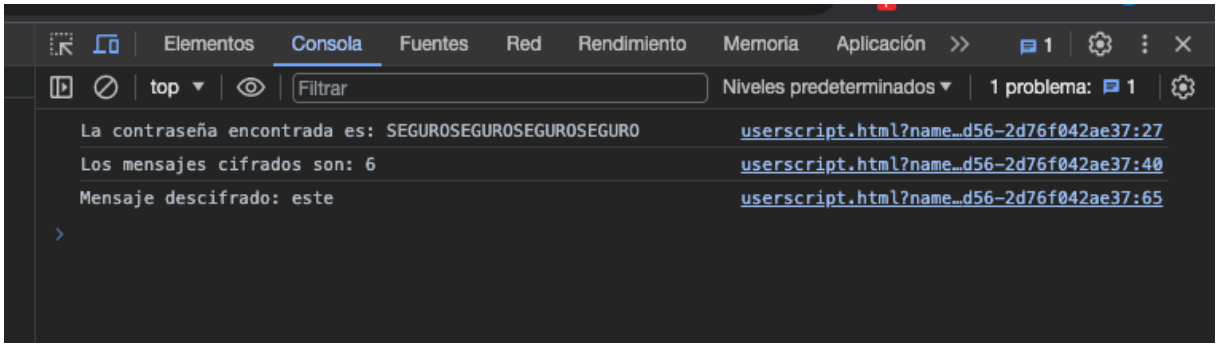
4.3. Logra descifrar uno de los mensajes

Como se descubrió en la primera parte, los mensajes están cifrados con el algoritmo 3DES en modo ECB. Y también la key es "SEGUROSEGUROSEGUROSEGURO", que corresponde a la concatenación de las mayúsculas del texto mostrado en la página del informante. Para empezar, se descifrará solo el primer mensaje "**xEopI5pGBCQ=**", con la key mencionada anteriormente, utilizando la librería CryptoJS con SRI. El script es el siguiente:

```
// Parte 3
//Descifrar 1 mensaje
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);
}


window.addEventListener('load', () => {
    buscarYMostrarContraseña();
    analizarMensajesCifrados();
     let mensajeCifradoBase64 = "xEopI5pGBCQ=";
     let clave = "SEGUROSEGUROSEGUROSEGURO";
    let mensajeDescifrado = descifrarMensaje3DES(mensajeCifradoBase64, clave);
    console.log("Mensaje descifrado " + mensajeDescifrado);
});

// Ejecutar la función al cargar la página
window.addEventListener('load', () => {
    buscarYMostrarContraseña();
    analizarMensajesCifrados();
});
```

El resultado es el siguiente:



Funciona, el descifrado es un éxito. Ahora se procede a descifrar todos los mensajes de la página.

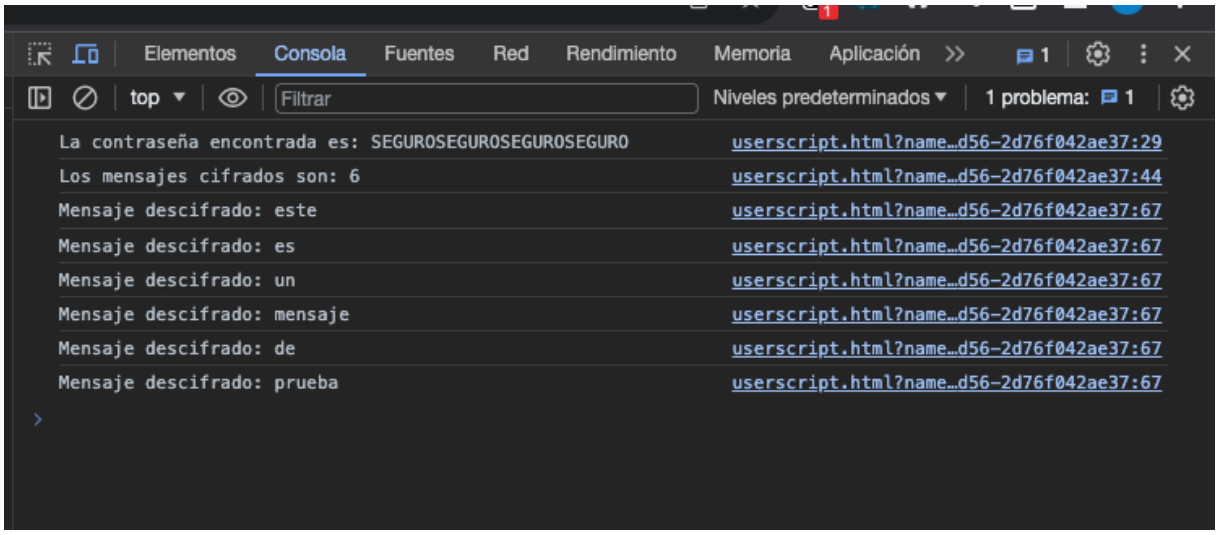
4.4. Imprime todos los mensajes por consola

Para descifrar todos los mensajes, es necesario crear una variable global donde se almacene la contraseña, luego crear una funcion para analizar todos los mensajes y descifrarlos. El código final con todas las partes anteriores queda así ***Script:***

```
// ==UserScript==
// @name         Descifrador de Contraseña y Mensajes Cifrados
// @namespace    http://tampermonkey.net/
// @version      1.0
// @description  Extrae y muestra la contraseña del texto de una página web y descifra
// @author       TuNombre
// @match        https://cripto.tiiny.site/
// @require      https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.
// @grant        none
// ==/UserScript==

(function() {
    'use strict';

    // Variable global para almacenar la clave de descifrado
    let claveGlobal = "";

    //Parte 1
    // Función que hace "match" si encuentra una mayúscula y la concatena
    function extraerContraseña(texto) {
        return texto.match(/[A-Z]/g).join('');
    }

    // Buscar el párrafo en la página y extraer las mayúsculas para formar la clave
    function buscarYMostrarContraseña() {
        let parrafo = document.querySelector("p");
        if (parrafo) {
            claveGlobal = extraerContraseña(parrafo.innerText || parrafo.textContent);
            console.log("La contraseña encontrada es: " + claveGlobal);
        } else {
            console.log("No se encontró el párrafo en la página.");
        }
    }
    //Parte 2
    // Función para contar la cantidad de mensajes cifrados
    function analizarMensajesCifrados() {
        let divs = document.querySelectorAll("div[id]");
```

```
        let contador = 0;
        divs.forEach(div => {
            if (div.id) {
                contador++;
            }
        });
        console.log("Los mensajes cifrados son: " + contador);
    }
    //Parte 3.1
    // Función para descifrar un mensaje con 3DES
    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);
    }
    //Parte 3.2
    // Función para descifrar todos los mensajes cifrados en la página
    function descifrarTodosLosMensajes() {
        let divs = document.querySelectorAll("div[id]");
        divs.forEach(div => {
            let mensajeCifradoBase64 = div.id;
            if (mensajeCifradoBase64) {
                let mensajeDescifrado = descifrarMensaje3DES(mensajeCifradoBase64, cla
                console.log("Mensaje descifrado: " + mensajeDescifrado);
            }
        });
    }
    window.addEventListener('load', () => {
        buscarYMostrarContraseña();
        analizarMensajesCifrados();
        descifrarTodosLosMensajes();
    });
})();
```

El resultado es el siguiente:



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

Para mostrar los mensajes en la página, se debe añadir la siguiente función:

```
function imprimirMensajesEnPagina(mensajeDescifrado) {
    let div = document.createElement('div');
    div.textContent = `${mensajeDescifrado}`;
    document.body.appendChild(div);
}
```

El resultado es el siguiente:

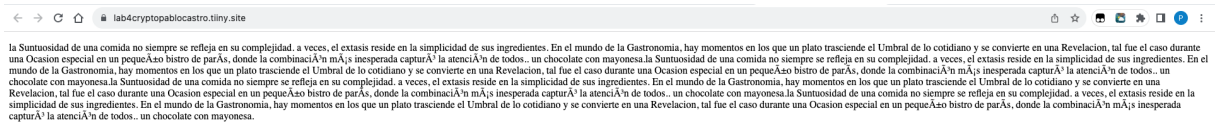
Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡ficos con el fin de encontrar debilidades en los sistemas y su seguridad. El criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos comprender criptosistemas y mejorarlos identificando los puntos dÃ©biles. Un criptoanalista puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seg protegido. Resultado del criptoanÃ¡lisis es la protecciÃ³n de la informaciÃ³n crÃtica para que no sea interceptada, copiada, modificada o eliminada. Otras tareas de pueden ser responsables los criptoanalistas incluyen evaluar, analizar y localizar las debilidades en los sistemas y algoritmos de seguridad criptogrÃ¡fica. Sin el con 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 criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos comprender los criptosistema 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. 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 d 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. E criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos comprender los criptosistema 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. 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 d 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. E criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, podemos comprender los criptosistema 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. 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

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

Para comprobar que el script funciona correctamente con otro texto y otra cantidad de mensajes cifrados, se crea un sitio html en https://tiiny.host/(Enlace a un sitio externo.). El enlace de la página es: https://lab4cryptopablocastro.tiiny.site/(Enlace a un sitio externo.).

Ahora el código debe tener una modificación en la linea ” ***”@match https://cripto.tiiny.site/”*** donde se debe remplazar esa url con la url de la página creada, quedando así: ” ***”@match https://lab4cryptopablocastro.tiiny.site/”*** El resultado es el siguiente: **Pagina HTML**

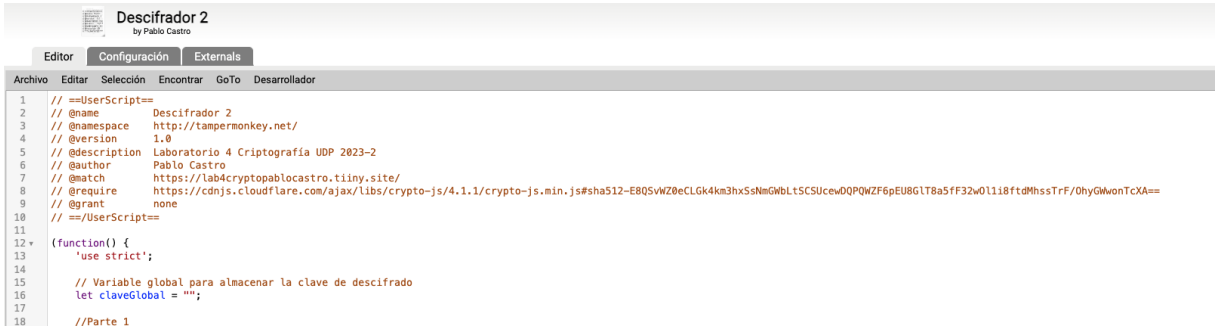


la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro de parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro de parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro de parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro de parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.

Código Fuente

```html

<!DOCTYPE html>
<html>
<head>
    <title>CHOCOLATE CON MAYO!</title>
<script type="text/javascript" src="https://tiiny.host/ad-script.js"></script><script defer data-domain="lab4cryptopablocastro.tiiny.site" src="https://analytics.tiiny.site/js/plausible.js"></script></head>
<body>
    <p>la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral d
    <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>
    <div class="M7" id="xEopI5pGBCQ="> </div>
    <div class="M8" id="vGECWVrA2f4="> </div>
    <div class="M9" id="MBDQE5ZiDsQ="> </div>
    <div class="M10" id="c8zxLt/4Iuk="> </div>
    <div class="M11" id="tPciMWg0pmg="> </div>
    <div class="M12" id="/XZw4C/lGEk="> </div>
    <div class="M13" id="xEopI5pGBCQ="> </div>
    <div class="M14" id="vGECWVrA2f4="> </div>
    <div class="M15" id="MBDQE5ZiDsQ="> </div>
    <div class="M16" id="c8zxLt/4Iuk="> </div>
    <div class="M17" id="tPciMWg0pmg="> </div>
    <div class="M18" id="/XZw4C/lGEk="> </div>
</body>
</html>

```

Código Actualizado



```javascript
// ==UserScript==
// @name         Descifrador 2
// @namespace    http://tampermonkey.net/
// @version      1.0
// @description  Laboratorio 4 Criptografía UDP 2023-2
// @author       Pablo Castro
// @match        https://lab4cryptopablocastro.tiiny.site/
// @require      https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js#sha512-E8QSvWZ0eCLGk4km3hxSsNmGWbLtSCSUcewDQPQWZF6pEU8GlT8a5fF32wOl1i8ftdMhssTrF/OhyGWwonTcXA==
// @grant        none
// ==/UserScript==

(function() {
    'use strict';

    // Variable global para almacenar la clave de descifrado
    let claveGlobal = "";

    //Parte 1
```

Resultado Consola

```
La contraseña encontrada es: SEGUROSEGUROSEGUROSEGURO    userscript.html?name…544-4356faf14d77:30
Los mensajes cifrados son: 18                            userscript.html?name…544-4356faf14d77:45
Mensaje descifrado: este                                 userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: es                                   userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: un                                   userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: mensaje                              userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: de                                   userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: prueba                               userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: este                                 userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: es                                   userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: un                                   userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: mensaje                              userscript.html?name…544-4356faf14d77:75
Mensaje descifrado: de                                   userscript.html?name…544-4356faf14d77:75
```

Resultado Página

la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, ha
momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro
parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.la Suntuosidad de una comida no siempre se refleja en su
complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral de l
cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro de parÃs, donde la combinaciÃ³n mÃ¡s inesperada captur
la atenciÃ³n de todos.. un chocolate con mayonesa.la Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de su
ingredientes. En el mundo de la Gastronomia, hay momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso
durante una Ocasion especial en un pequeÃ±o bistro de parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.la
Suntuosidad de una comida no siempre se refleja en su complejidad. a veces, el extasis reside en la simplicidad de sus ingredientes. En el mundo de la Gastronomia, hay
momentos en los que un plato trasciende el Umbral de lo cotidiano y se convierte en una Revelacion, tal fue el caso durante una Ocasion especial en un pequeÃ±o bistro
parÃs, donde la combinaciÃ³n mÃ¡s inesperada capturÃ³ la atenciÃ³n de todos.. un chocolate con mayonesa.

este
es
un
mensaje
de
prueba
este
es
un
mensaje
de
prueba
este
es
un
mensaje
de
prueba

Como se puede ver, el script funciona de manera correcta.

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

Asumiendo que el código en cuestión es el que está preparado para analizar la página que creé, se adjunta el siguiente enlace con el código. Código Página Nueva HTML(Enlace a un sitio externo.). De ser necesario un enlace para el código original, creado para la página "https://cripto.tiiny.site/", se adjunta el siguiente enlace: Código Tiiny.site(Enlace a un sitio externo.).

Conclusiones y comentarios

Se logró comprender los diferentes algoritmos de cifrado y cómo descifrar utilizando javascript. Así mismo 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.