Informe Laboratorio 4

Sección 4

Alumno Diego Serrano
e-mail: diego.serrano1@mail.udp.cl

9 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:

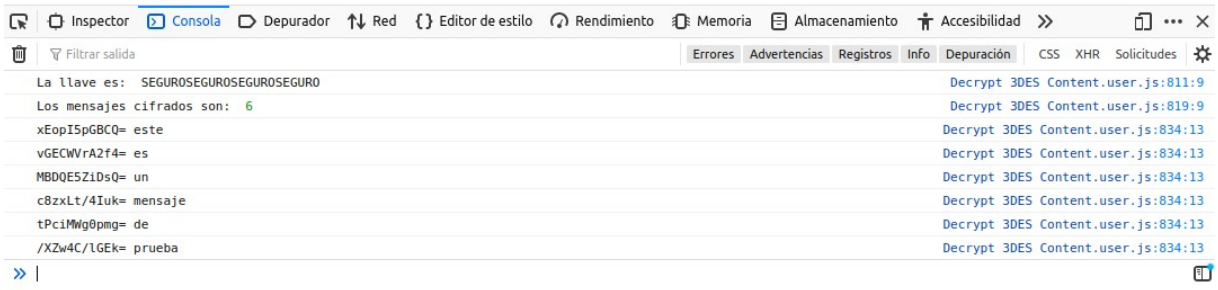
   - La llave es: KEY

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.

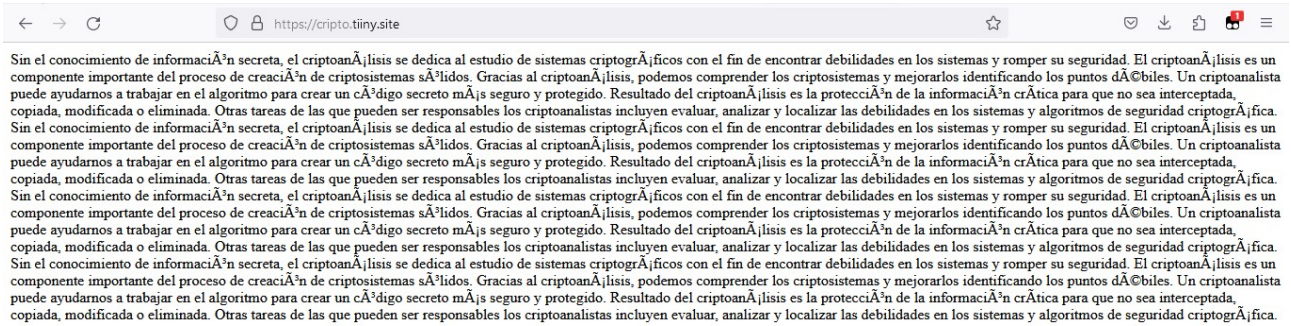
este
es
un
mensaje
de
prueba

```
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

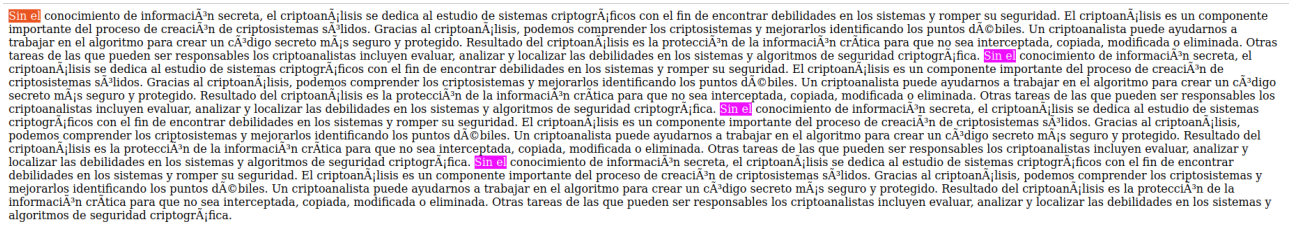
Para esta primera actividad, un informante trata de nuevamente compartir un mensaje con el usuario, solo que esta vez se ha compartido la información mediante un sitio web que se puede acceder públicamente, dicho link corresponde a ”https://cripto.tiiny.site/”. Al presionar el link de acceso, el usuario es redirigido a una página que contiene el siguiente texto:



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. 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.

Figura 1: Diseño de la página compartida por el informante

Se puede observar en el texto de la página que se habla sobre la importancia y utilidad del criptoanálisis, lo cual no sugiere a simple vista que este pueda ser el mensaje que el informante trata de compartir. Sin embargo, es posible notar que el texto sigue un patrón, de tal forma que cada una de las frases que aparece en este se repite 4 veces. Dicha información se puede respaldar utilizando las teclas Ctrl + F, herramienta de navegador que sirve para encontrar palabras específicas dentro de un texto. A continuación se muestra cómo cada una de las seis frases encontradas se repite en el texto:



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. 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.

Figura 2: Evidencia de la primera frase repitiéndose 4 veces

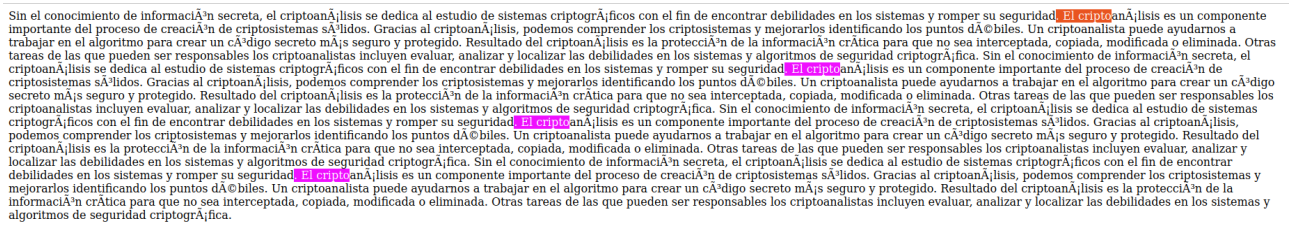


Figura 3: Evidencia de la segunda frase repitiéndose 4 veces

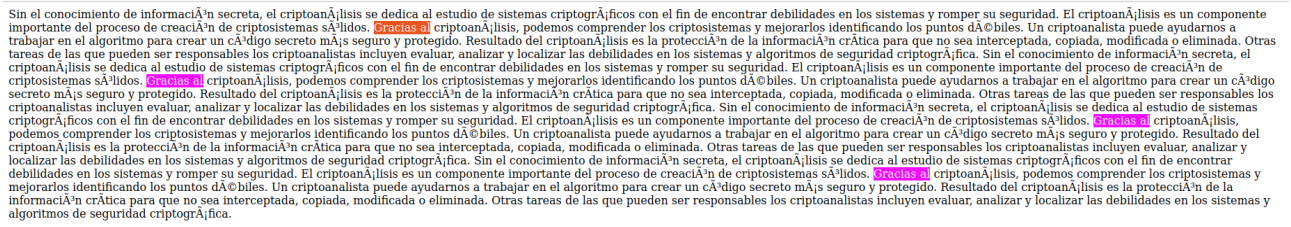


Figura 4: Evidencia de la tercera frase repitiéndose 4 veces

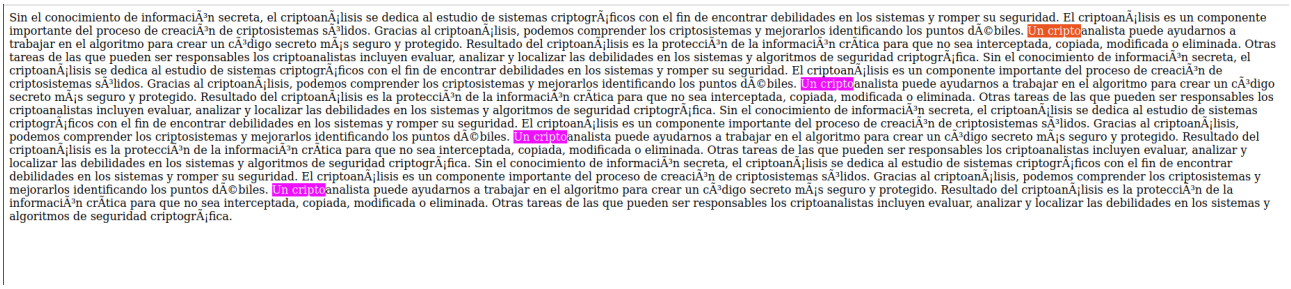


Figura 5: Evidencia de la cuarta frase repitiéndose 4 veces

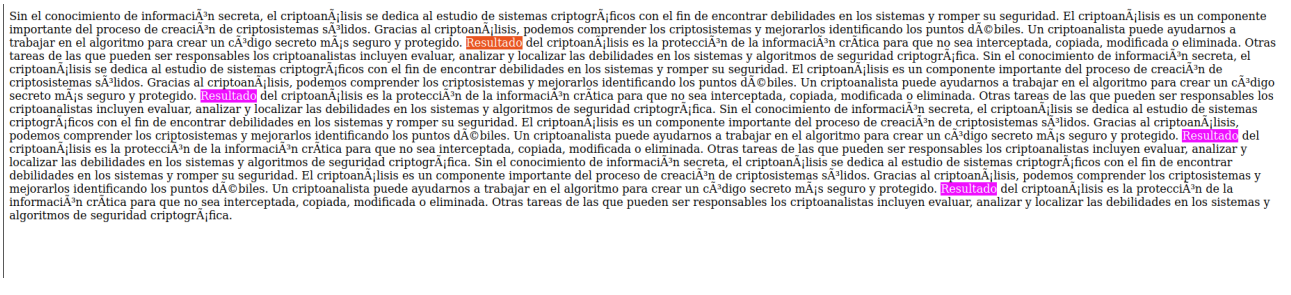


Figura 6: Evidencia de la quinta frase repitiéndose 4 veces

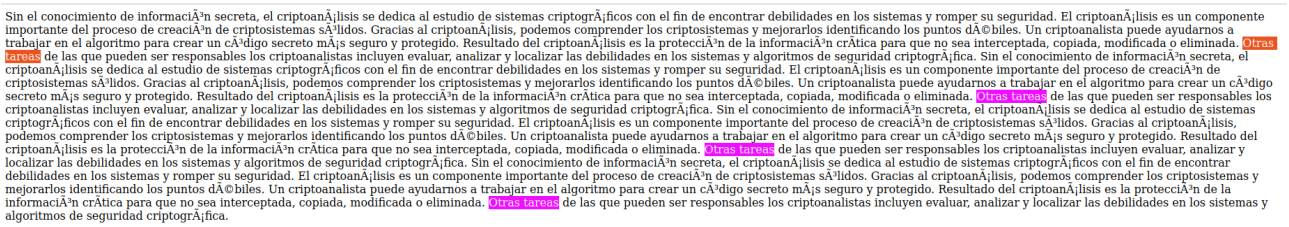

Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡ficos con el fin de encontrar debilidades en los sistemas y romper su seguridad. El criptoanÃ¡lisis es un componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, 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. 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.

Figura 7: Evidencia de la sexta frase repitiéndose 4 veces

Sabiendo que el texto se repite 4 veces, es posible notar también que si se juntan las letras mayúsculas de todas las frases en el orden que se encuentran, se puede formar la palabra "SEGUROSEGUROSEGUROSEGURO". Esto puede significar que el informante para lograr compartir la llave de cifrado con el usuario, tuvo que aplicar un formato de cifrado similar a Navy Signal Codes en la llave, de tal forma que esta puede ser encontrada si se reunen todas las letras mayúsculas del texto en una sola palabra. Sabiendo esta información, se puede confirmar que la palabra "SEGUROSEGUROSEGUROSEGURO" corresponde a la llave de cifrado.

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

Luego de deducir la llave compartida por el informante, lo que se debe hacer ahora es generar un código que permita conseguir dicha llave. Para ello, se debe acceder a las extensiones del navegador Mozilla Firefox para descargar Tampermonkey, una herramienta que funciona con el lenguaje Javascript, y que se puede utilizar para agregar o modificar componentes en una página web existente. Una vez descargado el software, lo que se debe hacer es presionar el ícono de Tampermonkey al lado derecho de la barra de páginas web y se presiona la opción de agregar un nuevo script, como se puede ver a continuación:

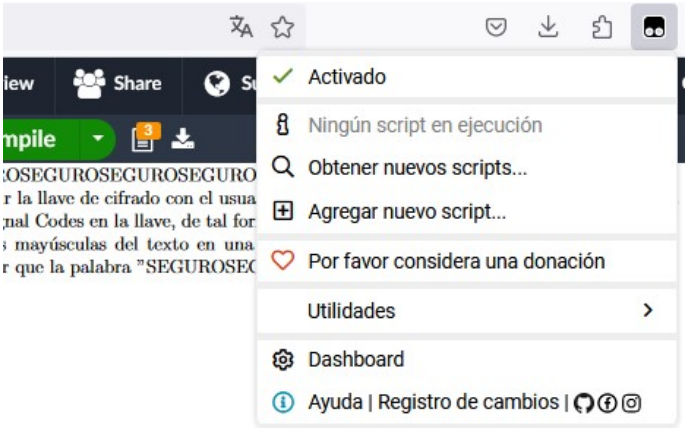


Figura 8: Opción para agregar un nuevo script

Al pulsar la opción de agregar un nuevo script, el navegador crea una nueva pestaña con una interfaz de código que tiene lo mínimo para funcionar. En esta interfaz, lo que se debe hacer es modificar la sección "@match" y se coloca la dirección de la página web que compartió el informante. Dicho cambio permite que el script creado pueda realizar modificaciones exclusivamente en la página web específica.

```
// ==UserScript==
// @name         LAB4CRIPTO
// @namespace    http://tampermonkey.net/
// @version      0.1
// @description  try to take over the world!
// @author       You
// @require      https://cdnjs.cloudflare.com/ajax/l
// @match        https://cripto.tiiny.site/
// @icon         https://www.google.com/s2/favicons?
// @grant        none
// ==/UserScript==
```

Figura 9: Modificación de la sección @match para que el script realice cambios en la página compartida por el informante

2.3. Define función que obtiene automáticamente el password del documento

Una vez definido el entorno en el que se va a aplicar este nuevo script en Tampermonkey, se procede a crear una función que permita obtener la llave encontrada en el primer paso de esta actividad. Dichos requisitos se cumplieron mediante la siguiente función:

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

    // Función para identificar letras mayúsculas en una cadena de texto
    var key = "";
    function encontrarLetrasMayusculas() {
        const textoWeb = document.body.innerText;
        key = textoWeb.match(/[A-Z]/g).join('');
        console.log('La llave de descifrado es: ' + key);
    }
```

Figura 10: Función para encontrar la llave inscrita en el texto de la página web

En la imagen anterior, se puede observar que la función creada guarda el texto de la página web del informante dentro de una variable const, y mediante el comando match, es posible guardar todos los caracteres del texto que estén en el rango de caracteres [A-Z] dentro de un string llamado key. Finalmente, luego de que se hayan guardado todas las letras mayúsculas de texto en la variable key, se procede a imprimir en la consola del navegador el resultado obtenido. Adicionalmente, la variable key fue creada fuera de la función "encontrarLetrasMayusculas" con el fin de que se pueda utilizar su resultado en las actividades siguientes.

2.4. Muestra la llave por consola

Para confirmar que la función se haya ejecutado sin problemas, se procede a abrir la página web del informante y se presiona la opción Inspeccionar luego de realizar click derecho en la página. Si el código se ejecutó sin problemas, se podrá encontrar la siguiente frase en la sección Consola de los elementos de la página.

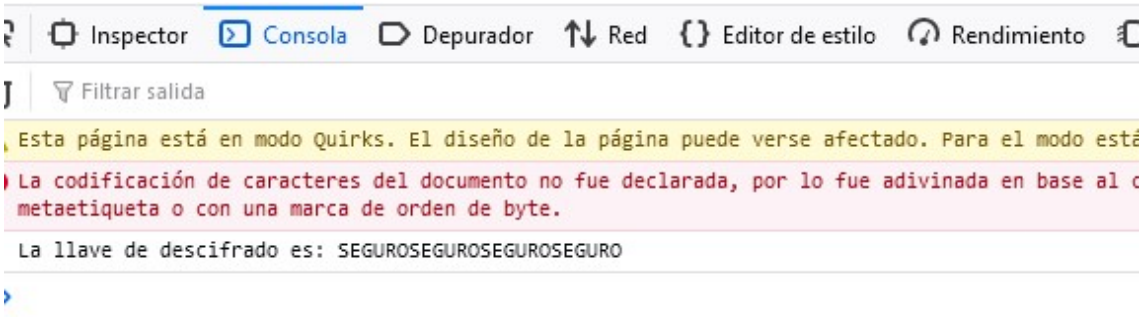


Figura 11: Resultado obtenido al ejecutar la primera función del script

3. Desarrollo (Parte 2)

3.1. reconoce automáticamente la cantidad de mensajes cifrados

Sin embargo eso no es todo, ya que en la siguiente actividad se debe generar una función dentro del mismo código creado en la actividad anterior, que permita identificar el número de mensajes que se encuentran cifrados dentro de la página. Si bien el texto de la página en sí no presenta indicios de que hayan palabras cifradas, es posible encontrar estas palabras utilizando la opción Inspeccionar luego de realizar click derecho en la página del informante. Si se observa la sección Inspector, es posible encontrar en el código de la página web lo siguiente:

Figura 12: Resultado obtenido al ejecutar la primera función del script

En la imagen anterior, es posible encontrar en el código de la página varias etiquetas div que poseen un ID de caracteres aleatorios. Una de las principales características que destacan de dichos IDs, es el hecho de que estos seis datos terminan con el caracter -", lo que puede sugerir que dichas palabras están en formato Base64. Adicionalmente a esto, todas las palabras encontradas tienen un largo de 12 caracteres, lo que puede significar que sumado al codificado en Base64, a estas palabras se les aplicó un algoritmo hash.

Sabiendo entonces que estas palabras están cifradas, se procede a crear otra función en el script de Tampermonkey que permita identificar y contar las palabras encontradas en el código de la página web. Dichos requerimientos se llevaron a cabo con la siguiente función:

```
// Función para contar palabras encriptadas
const palabras = [];
function cipheredWordsCount() {
    const codigoPagina = document.body.innerHTML;
    const palabrasEnComillasConIgual = codigoPagina.split('"');
    palabrasEnComillasConIgual.forEach(word => {
        if (word.endsWith("=") && word.length == 12) {
            palabras.push(word);
        }
    });

    if (palabrasEnComillasConIgual) {
        console.log(`Los mensajes cifrados son: ${palabras.length}`);
    } else {
        console.log('No se encontraron mensajes cifrados.');
    }
}
```

Figura 13: Función para contar cuántas palabras están cifradas

En la imagen anterior, se puede observar que en la función se almacena el código de la página web del informante mediante document.body.innerHTML, y se utiliza el caracter de doble comillas para segmentar todo el código de la página dentro de un arreglo de strings. Luego con un ciclo forEach es posible identificar cuáles son las palabras cifradas si cumplen con la condición de que la palabra termine en el caracter "=" y que su largo sea esquivalente a 12 caracteres. Si se cumplen en estas condiciones, la palabra es guardada en un nuevo arreglo de strings llamado "palabras", que tiene el objetivo de almacenar todas las palabras cifradas que se encontraron en la página web del informante. Finalmente, en la función se imprime el largo de este arreglo en la consola del navegador, el cual corresponde al número de palabras que se encuentran cifradas en el código de la página. Al igual que con la variable "key", el arreglo "palabras" fue creado fuera de la función "cipheredWordsCount", ya que se necesitan estas palabras para proceder con la actividad siguiente.

3.2. muestra la cantidad de mensajes por consola

Para confirmar que la función se haya ejecutado sin problemas, se procede a abrir la página web del informante y se presiona la opción Inspeccionar luego de realizar click derecho en la página. Si el código se ejecutó sin problemas, se podrá encontrar una frase que muestra el número de mensajes cifrados en la sección Consola de los elementos de la página.

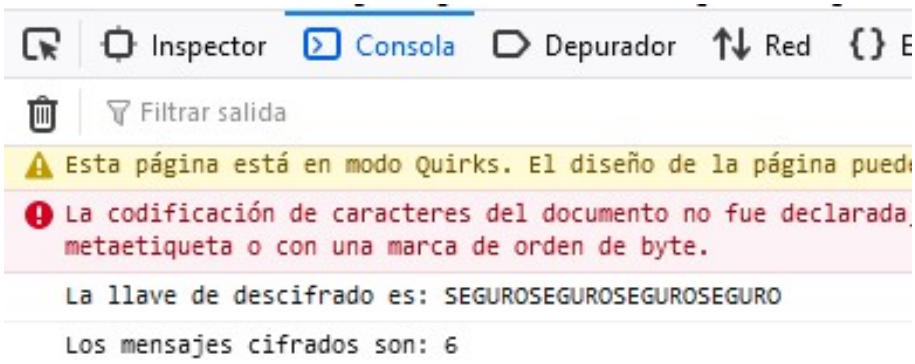


Figura 14: Resultado obtenido al ejecutar la segunda función del script

4. Desarrollo (Parte 3)

4.1. Importa la librería cryptoJS

En la siguiente actividad debe ser posible almacenar cada uno de los mensajes cifrados y descifrarlos por medio de una tercera función en el script de Tampermonkey. Los siguientes requerimientos se deben lograr importando CryptoJS, una librería de Javascript que se utiliza para cifrar y descifrar texto con una gran gama de algoritmos de cifrado disponibles. Para importar esta librería, se debe utilizar el header @require de Tampermonkey, sumado a un link de cloudflare que contenga la librería CryptoJS. La versión de CryptoJS utilizada para esta actividad fue la versión 3.1.9-1, ya que existe familiarización con esa versión específica.

```
// ==UserScript==
// @name         LAB4CRIPTO
// @namespace    http://tampermonkey.net/
// @version      0.1
// @description  try to take over the world!
// @author       You
// @require      https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/crypto-js.js
// @match        https://cripto.tiiny.site/
// @icon         https://www.google.com/s2/favicons?sz=64&domain=udp.cl
// @grant        none
// ==/UserScript==
```

Figura 15: Modificación de la sección @require para agregar la librería CryptoJS

4.2. Utiliza SRI en la librería CryptoJS

A continuación se debe aplicar el SRI en la librería CryptoJS, con el fin de asegurar que el recurso agregado al script de Tampermonkey no haya sido modificado con propósitos maliciosos. Para aplicar SRI, se debe copiar el enlace de la librería de CryptoJS para luego acceder a una página web llamada SRI Hash Generator.

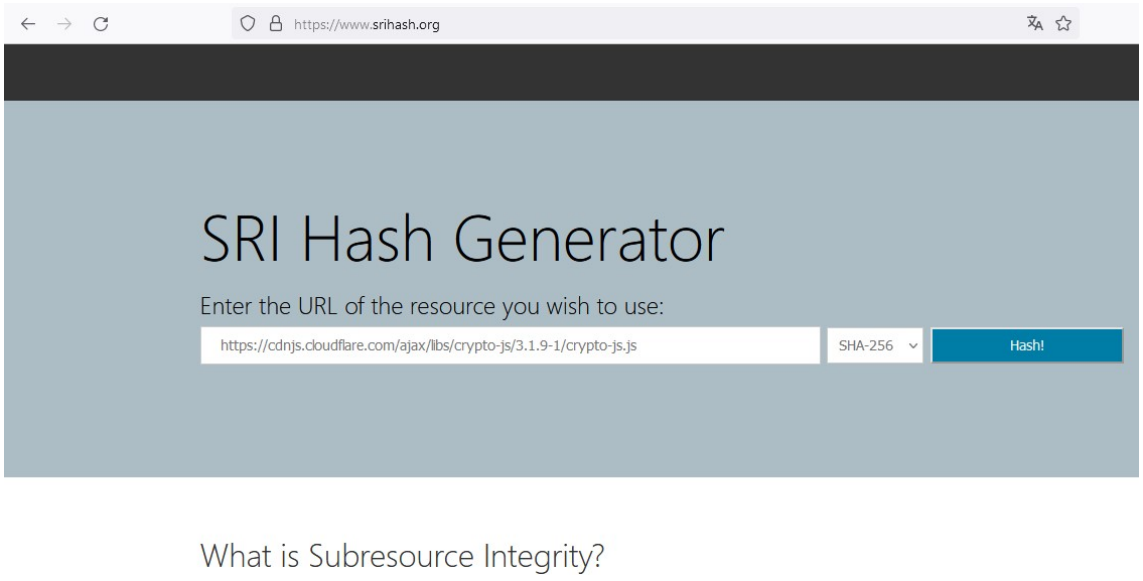


Figura 16: Página web del generador de hash SRI

Como el nombre sugiere, SRI Hash Generator utiliza un algoritmo para generar un hash de integridad de la página web que recibe en la barra transformadora. Para este caso, se utilizó el algoritmo SHA-256 para generar el hash de la librería CryptoJS, y se aplicó en el script de Tampermonkey de la siguiente manera:

Figura 17: Se agrega el hash SRI en la parte final del enlace de la librería

4.3. Logra decifrar uno de los mensajes

Una vez implementada la librería CryptoJS junto al SRI, se procede a investigar qué tipo de cifrado se utilizó para cifrar los seis mensajes obtenidos en la actividad anterior. Para ello, se intentó experimentar con las palabras disponibles y se buscó alguna página web que permitiera descifrar alguno de estos hash. Con eso en mente, se accedió a una página de cifrado y descifrado llamada "Triple DES Encryption and Decryption Online Tool", que se puede encontrar a continuación:

Figura 18: Página de cifrado/descifrado de TripleDES

Como forma de experimentación se utilizó el primer mensaje cifrado en la página del informante, y se descifró utilizando el modo ECB y la llave "SEGUROSEGUROSEGURO-SEGURO", junto a una transformación de Base64 a texto plano. Los resultados obtenidos de este descifrado se pueden ver a continuación:

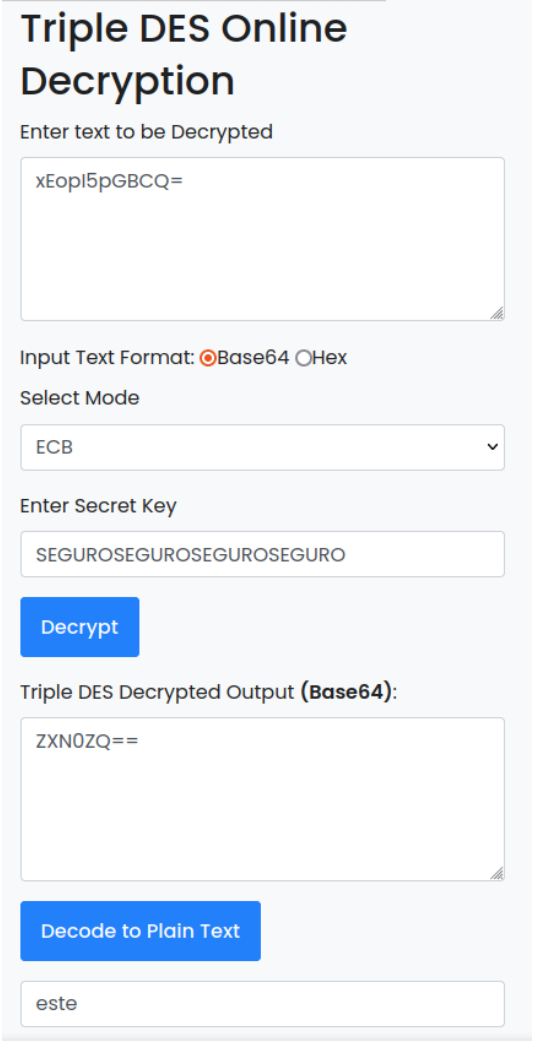


Figura 19: Resultado al descifrar el primer mensaje con Triple DES en modo ECB

De la imagen anterior, se puede observar que el descifrado en modo ECB entregó como respuesta una palabra en texto plano que corresponde a "este". Asumiendo que todas las palabras fueron cifradas mediante el mismo procedimiento, se puede concluir que las palabras fueron cifradas mediante Base64 y el algoritmo de hash Triple DES en modo ECB.

4.4. Imprime todos los mensajes por consola

Luego de descubrir el método de cifrado que utilizó el informante para entregar el mensaje al usuario, se procede a crear una tercera función en el script de Tampermonkey, que permita obtener los mensajes cifrados de la página web y descifrarlos por medio del algoritmo Triple DES en modo ECB. Para ello, se aplicó la función que se puede encontrar a continuación:

```
// Función para descifrar las palabras encontradas
const descifrados = [];
function descipherWords() {
    var cryptkey = CryptoJS.enc.Utf8.parse(key);
    palabras.forEach(word => {
        var decrypt = CryptoJS.TripleDES.decrypt(word, cryptkey, {
            mode: CryptoJS.mode.ECB,
            padding: CryptoJS.pad.Pkcs7,
        });
        var temp = decrypt.toString(CryptoJS.enc.Utf8);
        descifrados.push(temp);
    });
    var num = 0;
    descifrados.forEach(result => {
        console.log(palabras[num] + " " + result + "\n");
        num += 1;
    });
}
```

Figura 20: Función descifrar las palabras encontradas en la página

En la imagen anterior, se puede ver en la función que se transforma la llave de descifrado con el comando "CryptoJS.enc.Utf8.parse", esto se debe a que en esta librería, las llaves de descifrado solo pueden funcionar si se encuentran en formato WordArray en vez del formato string. Luego en un ciclo forEach, se procede a transformar todas las palabras encontradas en la página web del informante, y por medio de una variable "descrypt", se procede a descifrar cada una de las palabras utilizando el algoritmo Triple DES en modo ECB y la llave de descifrado "SEGUROSEGUROSEGUROSEGUROSEGURO", además de utilizar un padding Pkcs7. Las palabras obtenidas se proceden a transformar nuevamente a formato string, y se agregan dentro de un arreglo llamado "descifrados", que contiene todas las palabras descifradas. Finalmente, se vuelve a aplicar otro ciclo forEach para imprimir los resultados obtenidos en la consola del navegador.

Para confirmar que la función se haya ejecutado sin problemas, se procede a abrir la página web del informante y se presiona la opción Inspeccionar luego de realizar click derecho en la página. Si el código se ejecutó sin problemas, se podrá encontrar una lista de seis mensajes cifrados junto a sus contrapartes descifradas.

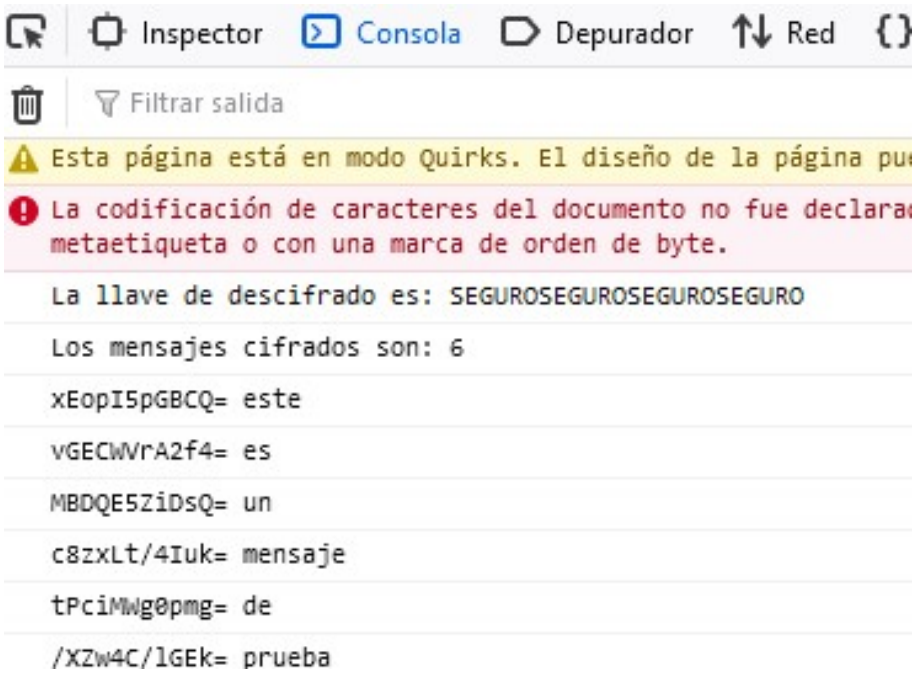


Figura 21: Resultado obtenido al ejecutar la tercera función del script

Se puede observar en la imagen anterior que, luego de descifrar cada una de las palabras, el mensaje que compartió el informante mediante esta página web corresponde a "este es un mensaje de prueba".

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

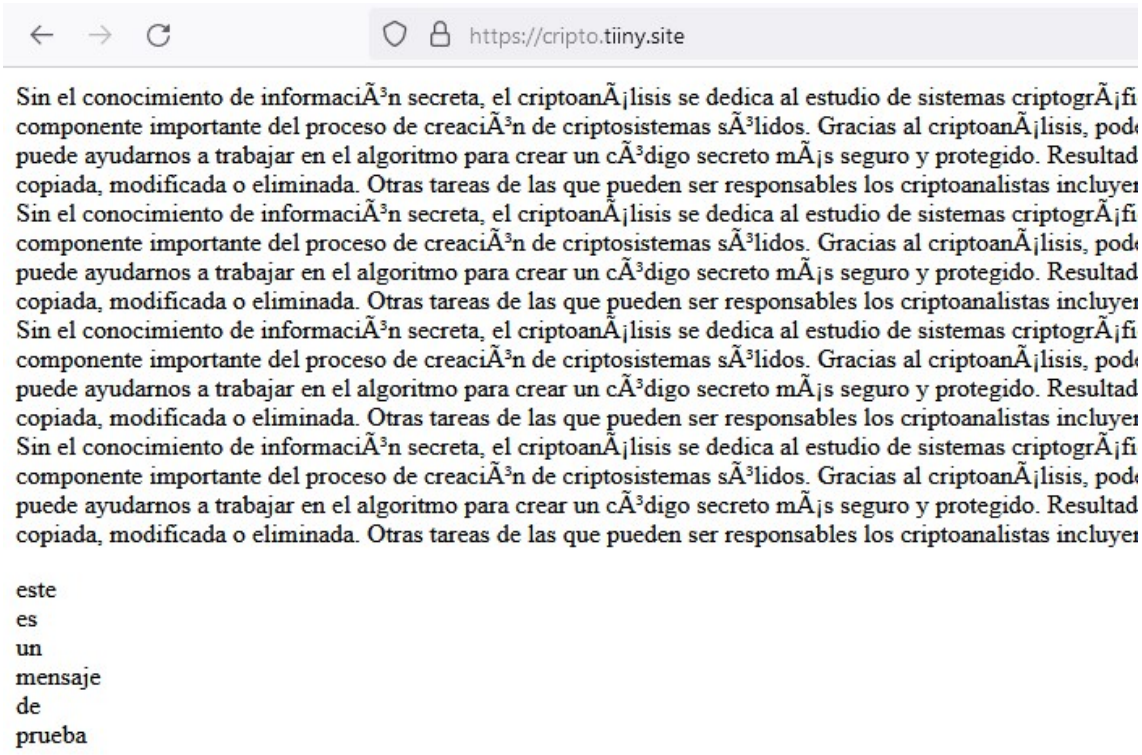
En adición a la impresión de los mensajes descifrados en la consola del navegador, se debe crear una cuarta función en el script de Tampermonkey que permita mostrar estos mensajes en texto plano dentro del texto de la página web del informante. Para ello, se implementó una función que sigue la siguiente estructura:

```
// Función para agregar palabras en una página web
function agregarPalabras() {
    var impresion = document.createElement('div');
    var temp2 = "";
    for (var i=0; i<descifrados.length; i++){
        temp2 += descifrados[i] + " <br> ";
    }
    impresion.innerHTML = temp2;
    document.body.appendChild(impresion);
}
```

Figura 22: Función para imprimir las palabras descifradas en la página web

Se puede observar en la figura anterior que se crea una nueva etiqueta "div", que se utilizará principalmente para mostrar en la página web las palabras descifradas en la actividad anterior. Luego se procede a utilizar un ciclo for con el fin almacenar cada una de las palabras en texto plano dentro de un string único, mientras se encuentran separadas por una etiqueta "br". El texto almacenado en la variable "temp2" se agrega como contenido en la etiqueta "div" creada anteriormente, y por medio del comando "document.body.appendChild", se agrega esta nueva etiqueta en la parte final del elemento body de la página web.

Para confirmar que esta función se ha ejecutado sin problemas, se procede a abrir la página web del informante y se realiza un refresh para observar si la página ha sufrido cambios. Si el código se ejecutó sin problemas, se podrá encontrar una lista de seis palabras nuevas justo debajo del texto compartido por el informante.



```
Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡fi
componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, pod
puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seguro y protegido. Resultad
copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluye
Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡fi
componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, pod
puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seguro y protegido. Resultad
copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluye
Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡fi
componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, pod
puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seguro y protegido. Resultad
copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluye
Sin el conocimiento de informaciÃ³n secreta, el criptoanÃ¡lisis se dedica al estudio de sistemas criptogrÃ¡fi
componente importante del proceso de creaciÃ³n de criptosistemas sÃ³lidos. Gracias al criptoanÃ¡lisis, pod
puede ayudarnos a trabajar en el algoritmo para crear un cÃ³digo secreto mÃ¡s seguro y protegido. Resultad
copiada, modificada o eliminada. Otras tareas de las que pueden ser responsables los criptoanalistas incluye

este
es
un
mensaje
de
prueba
```

Figura 23: Resultado obtenido al ejecutar la cuarta función del script

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

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

El código .js utilizado para realizar las actividades anteriores se puede encontrar en el siguiente link de Github, donde se incluyen también todas las imágenes utilizadas como evidencia del procedimiento que se siguió para completar los requerimientos del laboratorio.

- `https://github.com/Waluigi15243/Lab4Cripto`

Conclusiones y comentarios

En este laboratorio, se tuvo que trabajar en obtener un mensaje que estaba siendo comunicado por un informante mediante una página web pública. Utilizando herramientas como Tampermonkey y su librería CryptoJS con SRI, se tuvo que acceder a la página web de este informante, descubrir la llave de descifrado de los mensajes ocultos en la página, detectar el patrón que tienen los mensajes cifrados, y comprender cuáles algoritmos se utilizaron para cifrar estos mensajes con el fin de obtener en texto plano el mensaje que el informante trata de comunicar con su receptor.

Las actividades de laboratorio evidencian lo relativamente sencillo que es para una persona aleatoria descubrir cuál es el mensaje que se trata de compartir entre el informante y su receptor. Debido a que este mensaje está siendo compartido por medio de una interfaz pública, uno solo necesita saber cuál es el link de acceso a este sitio web para poder acceder a toda la información necesaria para descifrar el mensaje oculto en la página. Debido al problema mencionado anteriormente, este método para compartir información es altamente vulnerable a ataques como Shoulder Surfing o ataques de Capa 8 (Social Engineering).