Informe Laboratorio 4

Sección x

Javier Ahumada Bustos
e-mail: javierigna.ahumada@mail.udp.cl

Mayo de 2023

Índice

1. Descripción de actividades **2**

2. Desarrollo (Parte 1) **4**
- 2.1. Detecta el cifrado utilizado por el informante 4
- 2.2. Logra que el script solo se gatille en el sitio usado por el informante 4
- 2.3. Define función que obtiene automáticamente el password del documento . . . 5
- 2.4. Muestra la llave por consola 6

3. Desarrollo (Parte 2) **7**
- 3.1. reconoce automáticamente la cantidad de mensajes cifrados 7
- 3.2. muestra la cantidad de mensajes por consola 8

4. Desarrollo (Parte 3) **8**
- 4.1. Importa la librería cryptoJS 8
- 4.2. Utiliza SRI en la librería CryptoJS 8
- 4.3. Logra decifrar uno de los mensajes 9
- 4.4. Imprime todos los mensajes por consola 9
- 4.5. Muestra los mensajes en texto plano en el sitio web 10
- 4.6. El script logra funcionar con otro texto y otra cantidad de mensajes 10
- 4.7. Indica url al código .js implementado para su validación 10

1. Descripción de actividades

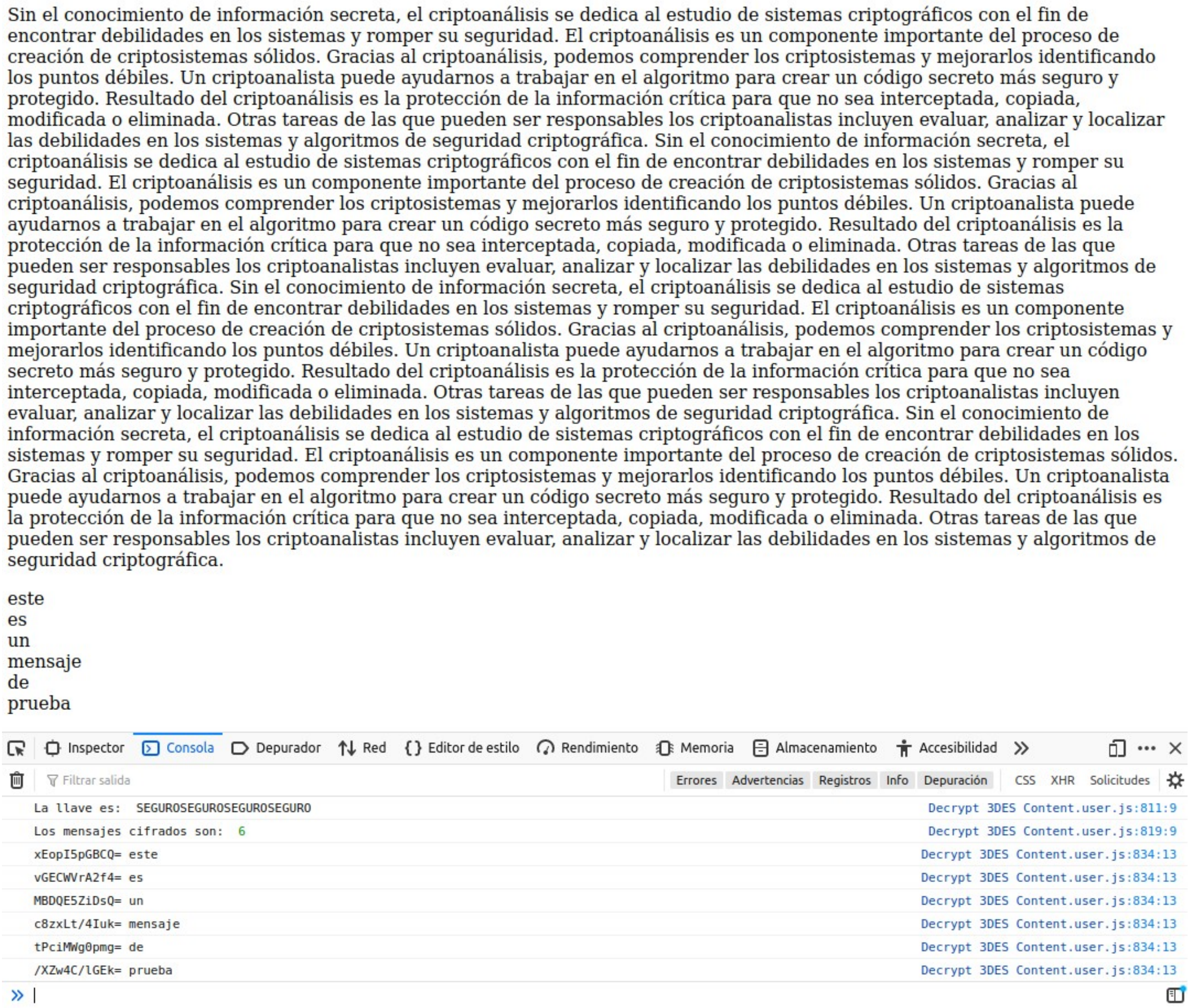
Para este laboratorio, deberá utilizar Tampermonkey y la librería CryptoJS (con SRI) para lograr obtener los mensajes que le está comunicando su informante. En esta ocasión, su informante fue más osado y se comunicó con usted a través de un sitio web abierto a todo el público https://cripto.tiiny.site/.

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
```

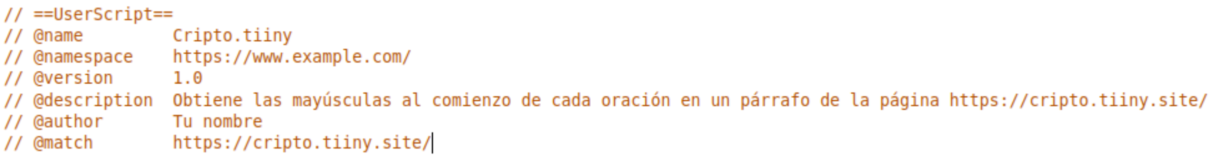
2. Desarrollo (Parte 1)

2.1. Detecta el cifrado utilizado por el informante

```
<html>
 ▶<head>⋯</head>
⋯▼<body> == $0
   ▶<div class="Parrafo">⋯</div>
    <div class="M1" id="RQCKATIdEzg="> </div>
    <div class="M2" id="2szV3wHBiw5LfRIYX/q3tw=="> </div>
    <div class="M3" id="cEiLQFAioa5cKapKZGoxuA=="> </div>
    <div class="M4" id="BNrUoP7Pb04="> </div>
    <div class="M5" id="rlkhDp/oaH4="> </div>
    <div class="M6" id="p8me9YrfrHs="> </div>
    <div class="M7" id="87L0P48K+KaE126XPkVh+Q=="> </div>
  </body>
</html>
```

Figura 1: Se encuentra un cifrado en cada contenedor div. Ademas la clave de cifrado esta en el enunciado concatenando la primera palabra de cada oracion: CRIPTOCRIPTOCRIPTOCRIPTO

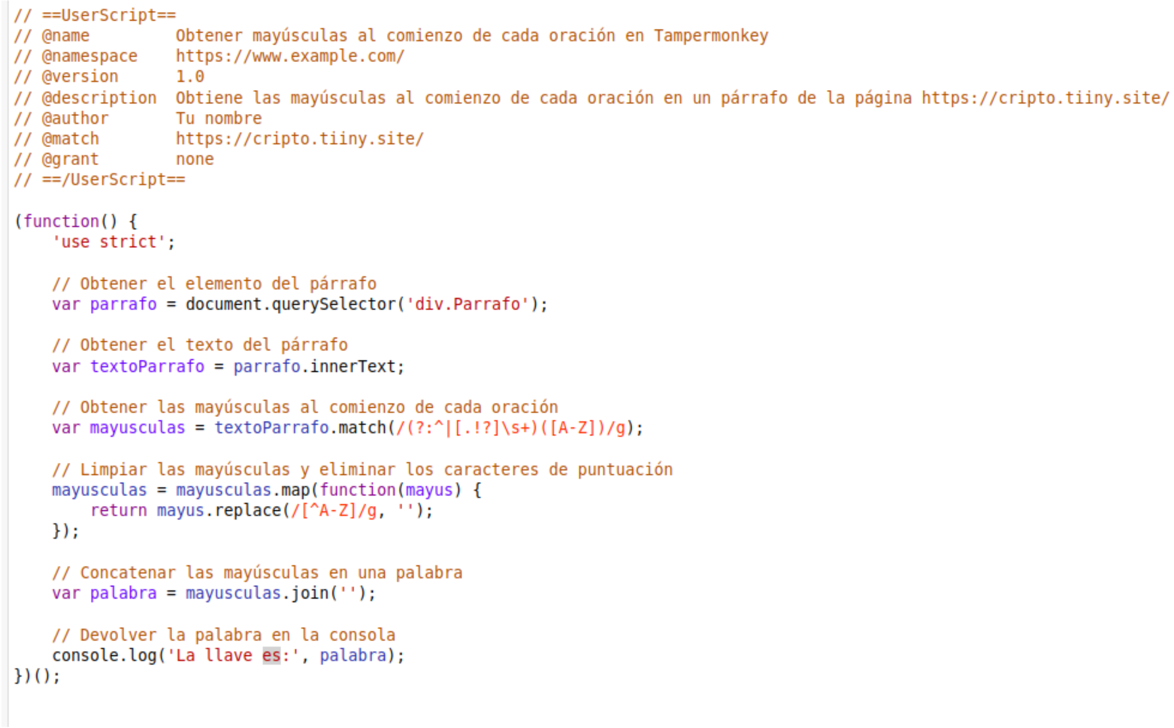
2.2. Logra que el script solo se gatille en el sitio usado por el informante



```
// ==UserScript==
// @name         Cripto.tiiny
// @namespace    https://www.example.com/
// @version      1.0
// @description  Obtiene las mayúsculas al comienzo de cada oración en un párrafo de la página https://cripto.tiiny.site/
// @author       Tu nombre
// @match        https://cripto.tiiny.site/
```

Figura 2: Este script solo se ejecuta si hace match con el dominio https://cripto.tiiny.site/

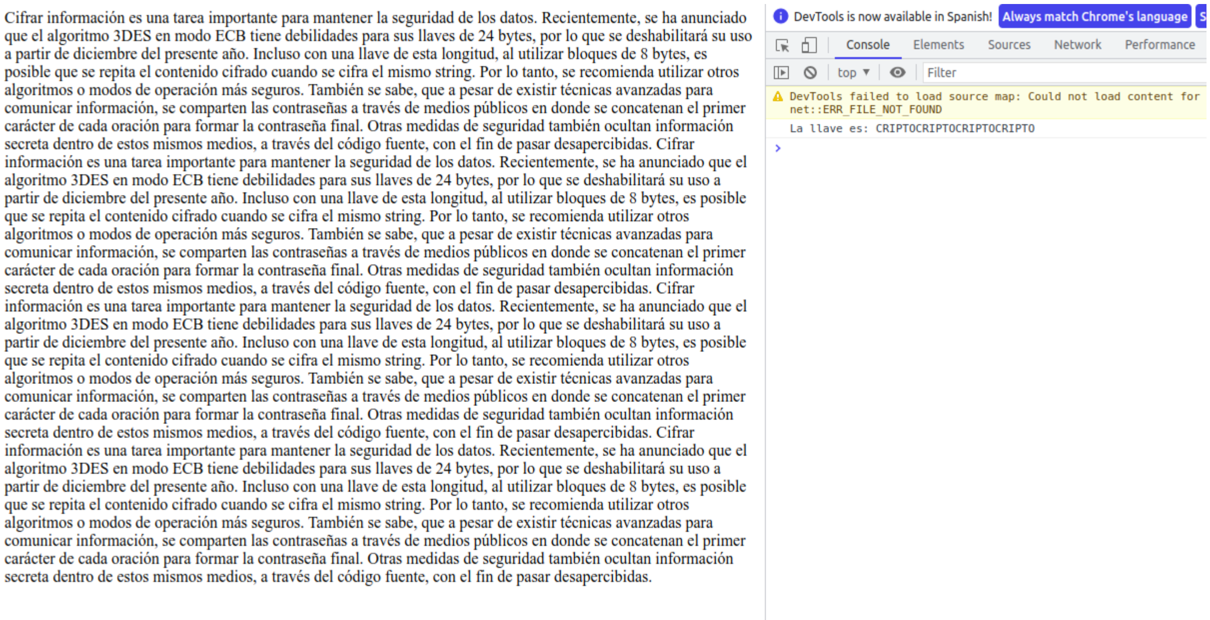
2.3. Define función que obtiene automáticamente el password del documento



```
// ==UserScript==
// @name         Obtener mayúsculas al comienzo de cada oración en Tampermonkey
// @namespace    https://www.example.com/
// @version      1.0
// @description  Obtiene las mayúsculas al comienzo de cada oración en un párrafo de la página https://cripto.tiiny.site/
// @author       Tu nombre
// @match        https://cripto.tiiny.site/
// @grant        none
// ==/UserScript==

(function() {
    'use strict';

    // Obtener el elemento del párrafo
    var parrafo = document.querySelector('div.Parrafo');

    // Obtener el texto del párrafo
    var textoParrafo = parrafo.innerText;

    // Obtener las mayúsculas al comienzo de cada oración
    var mayusculas = textoParrafo.match(/(?:^|[.!?]\s+)([A-Z])/g);

    // Limpiar las mayúsculas y eliminar los caracteres de puntuación
    mayusculas = mayusculas.map(function(mayus) {
        return mayus.replace(/[^A-Z]/g, '');
    });

    // Concatenar las mayúsculas en una palabra
    var palabra = mayusculas.join('');

    // Devolver la palabra en la consola
    console.log('La llave es:', palabra);
})();
```

Figura 3: Script Parte 1

2.4. Muestra la llave por consola



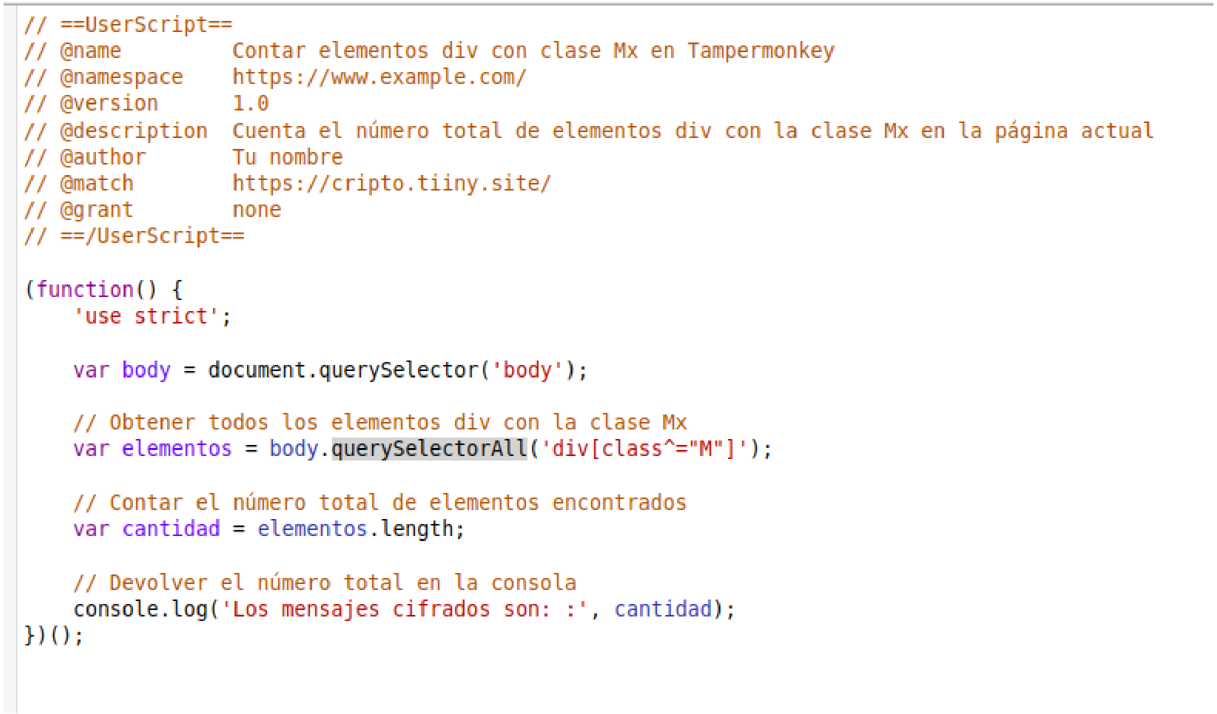
Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas.

```
⚠ DevTools failed to load source map: Could not load content for
net::ERR_FILE_NOT_FOUND
La llave es: CRIPTOCRIPTOCRIPTOCRIPTO
>
```

Figura 4: llave de cifrado CRIPTOCRIPTOCRIPTOCRIPTO de 24 bytes

3. Desarrollo (Parte 2)

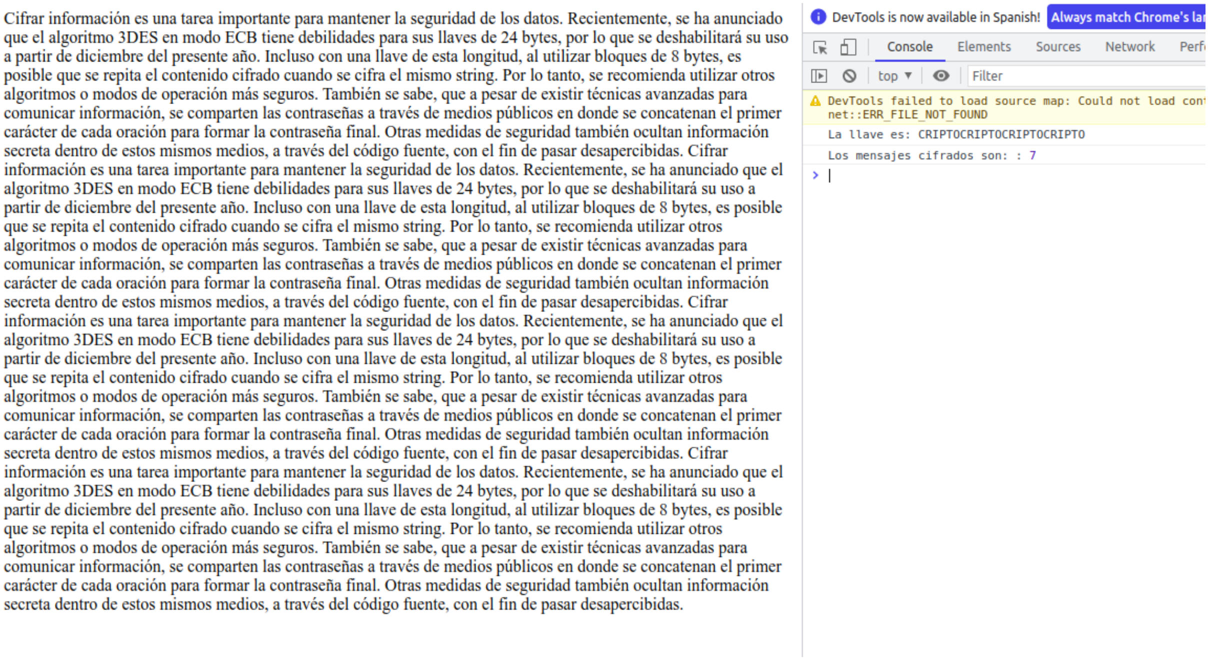
3.1. reconoce automáticamente la cantidad de mensajes cifrados



```
// ==UserScript==
// @name         Contar elementos div con clase Mx en Tampermonkey
// @namespace    https://www.example.com/
// @version      1.0
// @description  Cuenta el número total de elementos div con la clase Mx en la página actual
// @author       Tu nombre
// @match        https://cripto.tiiny.site/
// @grant        none
// ==/UserScript==

(function() {
    'use strict';

    var body = document.querySelector('body');

    // Obtener todos los elementos div con la clase Mx
    var elementos = body.querySelectorAll('div[class^="M"]');

    // Contar el número total de elementos encontrados
    var cantidad = elementos.length;

    // Devolver el número total en la consola
    console.log('Los mensajes cifrados son: :', cantidad);
})();
```

Figura 5: Cada mensaje cifrado esta en un contenedor div de clase M, luego se buscan todos los contenedores con esas caracteristicas y se retorna el total

3.2. muestra la cantidad de mensajes por consola



Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas.

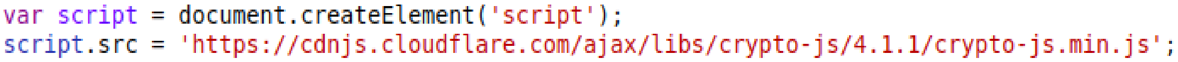
DevTools is now available in Spanish!

```
DevTools failed to load source map: Could not load con
net::ERR_FILE_NOT_FOUND
La llave es: CRIPTOCRIPTOCRIPTOCRIPTO
Los mensajes cifrados son: : 7
>
```

Figura 6: Mensajes por consola

4. Desarrollo (Parte 3)

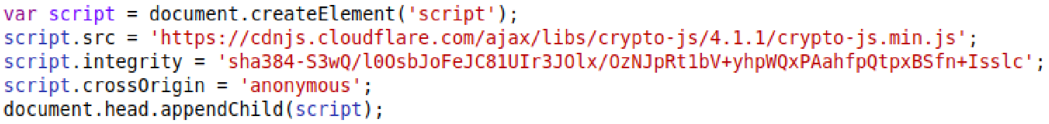
4.1. Importa la librería cryptoJS



```
var script = document.createElement('script');
script.src = 'https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js';
```

Figura 7: Como se importa CryptoJs a traves de un CDN no se necesita la sintaxis @require para importarla si no generando un elemento script

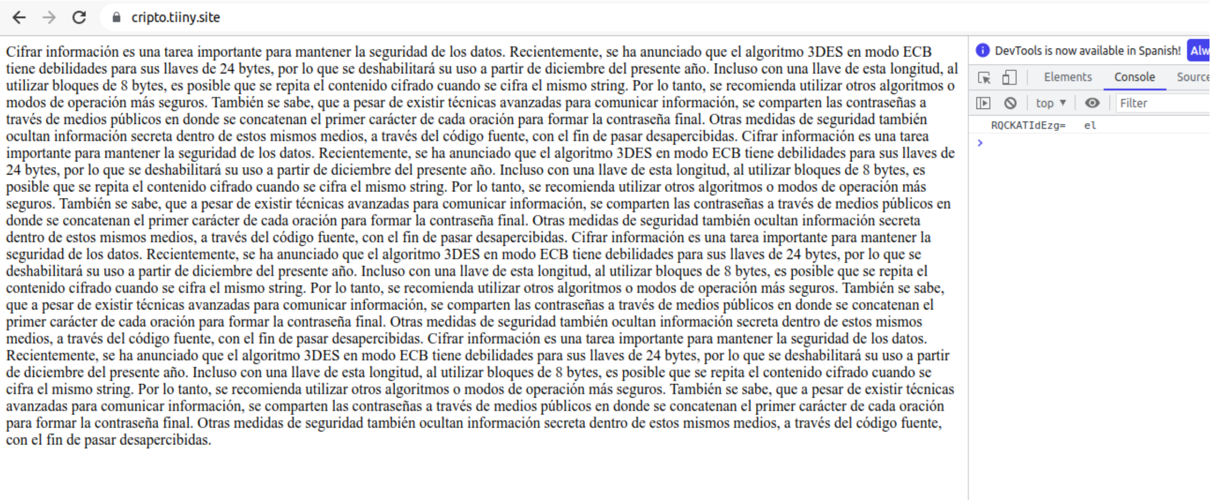
4.2. Utiliza SRI en la librería CryptoJS



```
var script = document.createElement('script');
script.src = 'https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js';
script.integrity = 'sha384-S3wQ/l0OsbJoFeJC81UIr3JOlx/OzNJpRt1bV+yhpWQxPAahfpQtpxBSfn+Isslc';
script.crossOrigin = 'anonymous';
document.head.appendChild(script);
```

Figura 8: Con SRI se establecen propiedades adicionales para garantizar la integridad del archivo

4.3. Logra decifrar uno de los mensajes

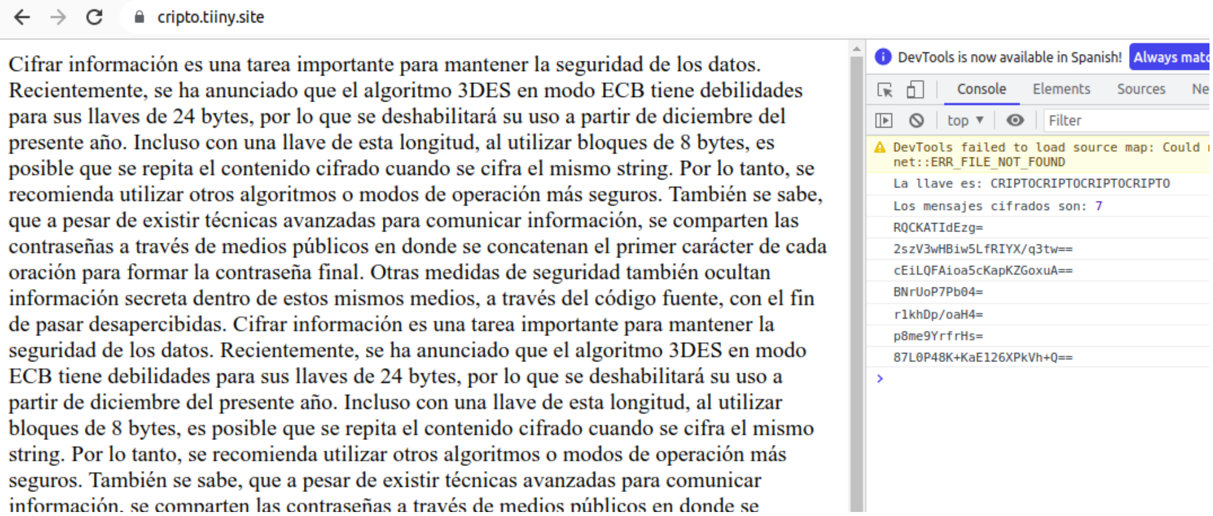


Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas.

```
RQCKATIdEzg=   el
>
```

Figura 9: Primer mensaje descifrado.

4.4. Imprime todos los mensajes por consola

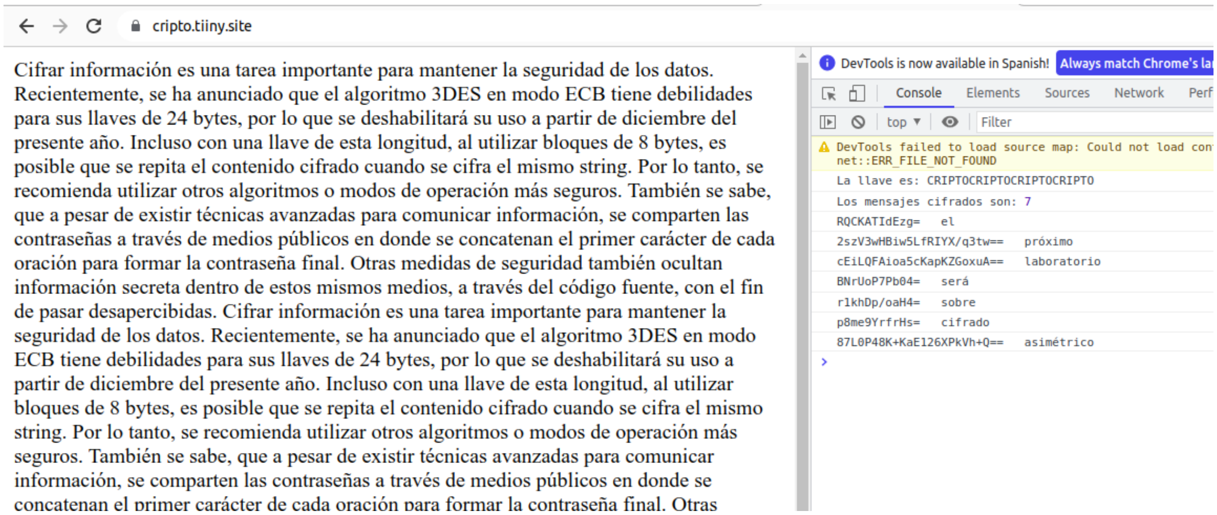


Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se

```
DevTools failed to load source map: Could
net::ERR_FILE_NOT_FOUND
La llave es: CRIPTOCRIPTOCRIPTOCRIPTO
Los mensajes cifrados son: 7
RQCKATIdEzg=
2szV3wHBiw5LfRIYX/q3tw==
cEiLQFAioa5cKapKZGoxuA==
BNrUoP7Pb04=
r1khDp/oaH4=
p8me9YrfrHs=
87L0P48K+KaE126XPkVh+Q==
>
```

Figura 10: Mensajes cifrados.

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



Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras medidas de seguridad también ocultan información secreta dentro de estos mismos medios, a través del código fuente, con el fin de pasar desapercibidas. Cifrar información es una tarea importante para mantener la seguridad de los datos. Recientemente, se ha anunciado que el algoritmo 3DES en modo ECB tiene debilidades para sus llaves de 24 bytes, por lo que se deshabilitará su uso a partir de diciembre del presente año. Incluso con una llave de esta longitud, al utilizar bloques de 8 bytes, es posible que se repita el contenido cifrado cuando se cifra el mismo string. Por lo tanto, se recomienda utilizar otros algoritmos o modos de operación más seguros. También se sabe, que a pesar de existir técnicas avanzadas para comunicar información, se comparten las contraseñas a través de medios públicos en donde se concatenan el primer carácter de cada oración para formar la contraseña final. Otras

```
DevTools failed to load source map: Could not load con
net::ERR_FILE_NOT_FOUND
La llave es: CRIPTOCRIPTOCRIPTOCRIPTO
Los mensajes cifrados son: 7
RQCKATIdEzg=   el
2szV3wHBiw5LfRIYX/q3tw==   próximo
cEiLQFAioa5cKapKZGoxuA==   laboratorio
BNrUoP7Pb04=   será
rlkhDp/oaH4=   sobre
p8me9YrfrHs=   cifrado
87L0P48K+KaE126XPkVh+Q==   asimétrico
>
```

Figura 11: Resultado Parte 3

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

En teoria debe funcionar porque se busca en la seccion body del HTML los div de clase Parrafo y Mn, donde n es la cantidad de mensajes.

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

https://github.com/jxvierpo/Tampermonkey-cryptojs.git

Conclusiones y comentarios

El SRI permite verificar la integridad del recurso descargado comparando su hash criptográfico con un valor de integridad conocido. Esto ayuda a prevenir ataques en los que un tercero malintencionado puede interceptar o modificar el recurso en tránsito, lo que podría conducir a problemas de seguridad o funcionalidad en tu sitio o aplicación. El navegador verifica automáticamente que el recurso descargado coincida con ese hash antes de ejecutar o aplicar el recurso.

Finalmente la dificultad fue trabajar en tampermonkey, en cuanto al manejo de variables. Por ejemplo, la clave de cifrado calculada habia que pasarla al mismo formato que el ID extraido para que la libreria de CryptoJs funcionara. Ese detalle ChatGPT no lo pudo resolver si no la experiencia obtenida en los ramos informaticos.