UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

CENTRO DE CIENCIAS BASICAS

ING. EN SISTEMAS COMPUTACIONALES

Nombre de la tarea:
Documentación de Criptobros

Materia:

Seguridad en Sistemas

David Menchaca Lora 281191

Profesor:
Luis Eduardo Bautista Villalpando.

Aguascalientes, Ags. **Fecha de entrega:** 20 de febrero del 2026

INDICE

INTRODUCCIÓN.....3

OBJETIVO.....4

DESARROLLO.....5

FUNCIONAMIENTO.....5

CODIGO.....10

CONCLUSIÓN.....15

BIBLIOGRAFIA.....16

INTRODUCCIÓN

El matemático árabe Al-Kindi (أبو يوسف يعقوب بن إسحاق الكندي) revolucionó la seguridad de la información en el siglo IX al desarrollar la técnica del análisis de frecuencias. Su aporte permitió "hackear" sistemas de encriptación simples, como los de sustitución monoalfabética, al demostrar que es posible descifrar un mensaje observando la frecuencia con la que aparecen ciertas letras en un idioma determinado.

Por esta razón, métodos como el cifrado Cesar y Atbash ya no son viables para la protección de datos en la actualidad. Al ser sistemas de sustitución simple con un espacio de claves extremadamente pequeño (o nulo, en el caso de Atbash), un atacante puede romperlos en milisegundos mediante análisis estadístico o ataques de fuerza bruta, careciendo de la complejidad necesaria para resistir el poder de cómputo moderno.

OBJETIVO

Desarrollar una aplicación web funcional como parte de una práctica académica para implementar los algoritmos de cifrado y descifrado César y Atbash. El sistema debe permitir la manipulación dinámica de conjuntos de caracteres personalizados basados en el código ASCII, proporcionando una interfaz intuitiva para la gestión pedagógica de información básica.

.

DESARROLLO

Para la realización de esta aplicación web se utilizaron las tecnologías de HTML, JavaScript y CSS; además se usó GitHub Pages para alojar el sitio web.

A continuación, se presenta el funcionamiento de la aplicación web:

Al entrar a la pagina lo primero que aparece es la siguiente interfaz.

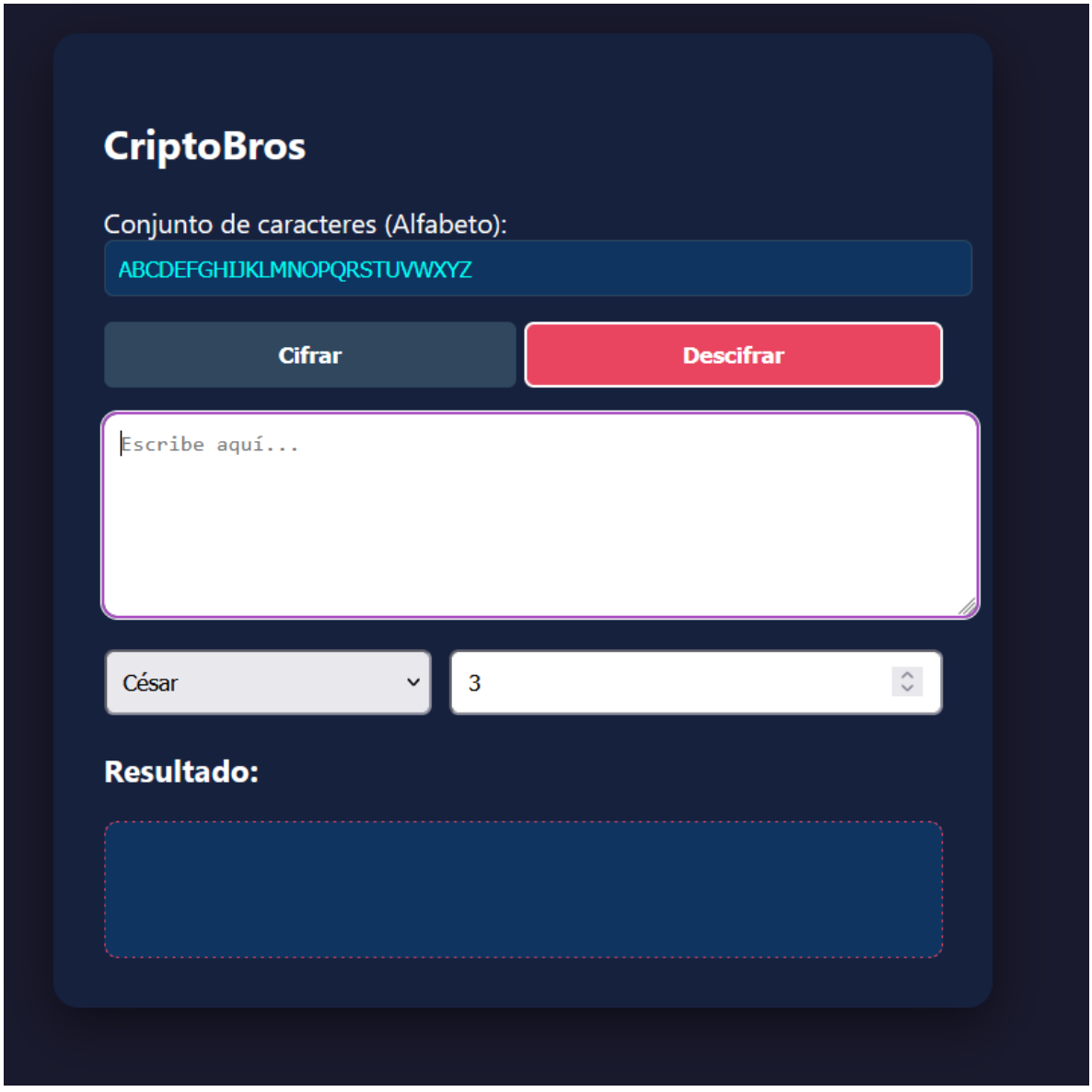

Ilustración 1 Imagen de la interfaz donde se desarrolla todo el proceso de cifrado y descifrado

En la primera sección se ingresa la cadena de caracteres que se usara para el alfabeto de cifrado y descifrado. No se permiten caracteres repetidos.

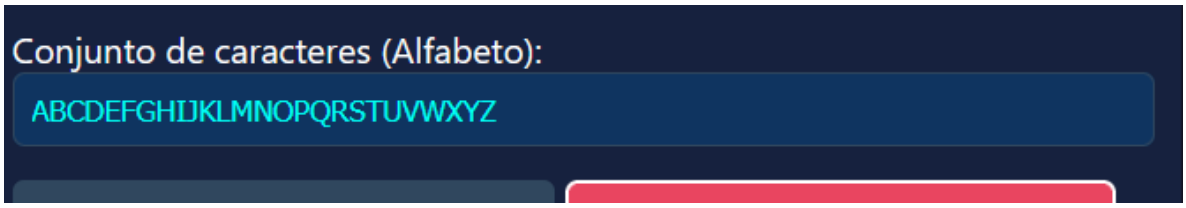

Ilustración 2 Un text input para el alfabeto

La siguiente sección se usa para seleccionar la opción de cifrar o descifrar (solo funciona en César).

Ilustración 3 botones para seleccionar el modo.

La siguiente sección es donde se escribe el mensaje que se quiere cifrar, el programa convertirá automáticamente las letras a mayúsculas para evitar errores con el alfabeto.

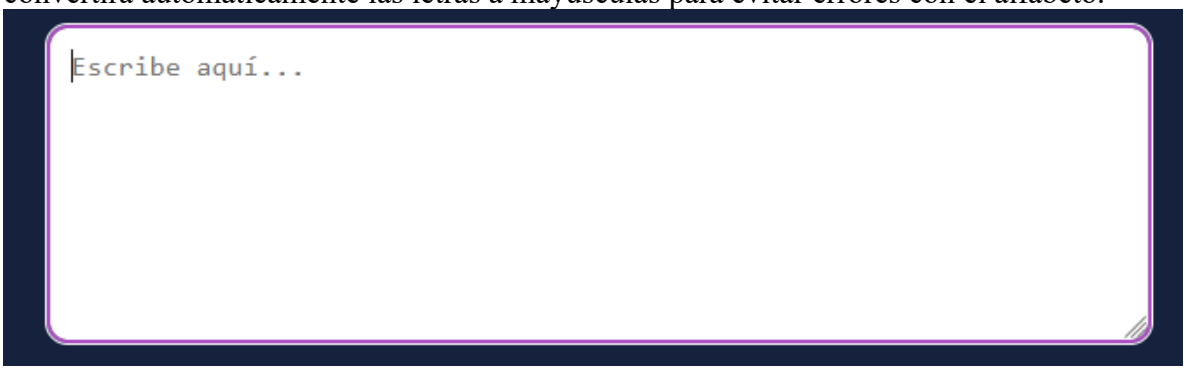

Ilustración 4 cuadro de texto donde se escribirá el mensaje a cifrar/descifrar

La siguiente sección se usa para seleccionar el tipo de cifrado, y en el caso del cifrado cesar, el offset.

Ilustración 5 selector de cifrado y offset (Cesar)

Por último esta la salida, el resultado ira apareciendo conforme se escribe el texto a cifrar o descifrar.

Ilustración 6 Salida del sistema

Ilustración 7 cifrado Atbash seleccionado

Ejemplo de uso:

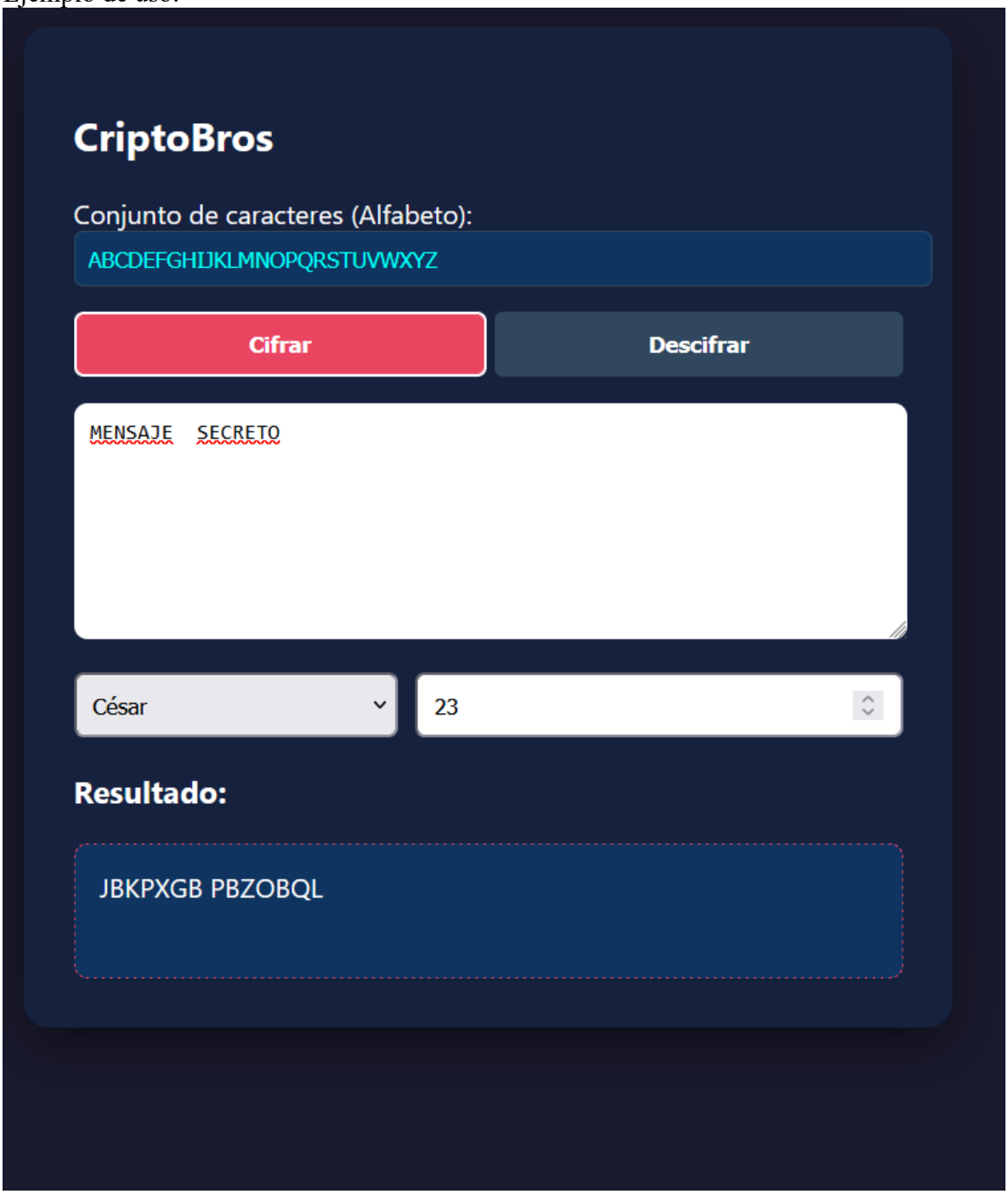

Ilustración 8 cifrando mensaje

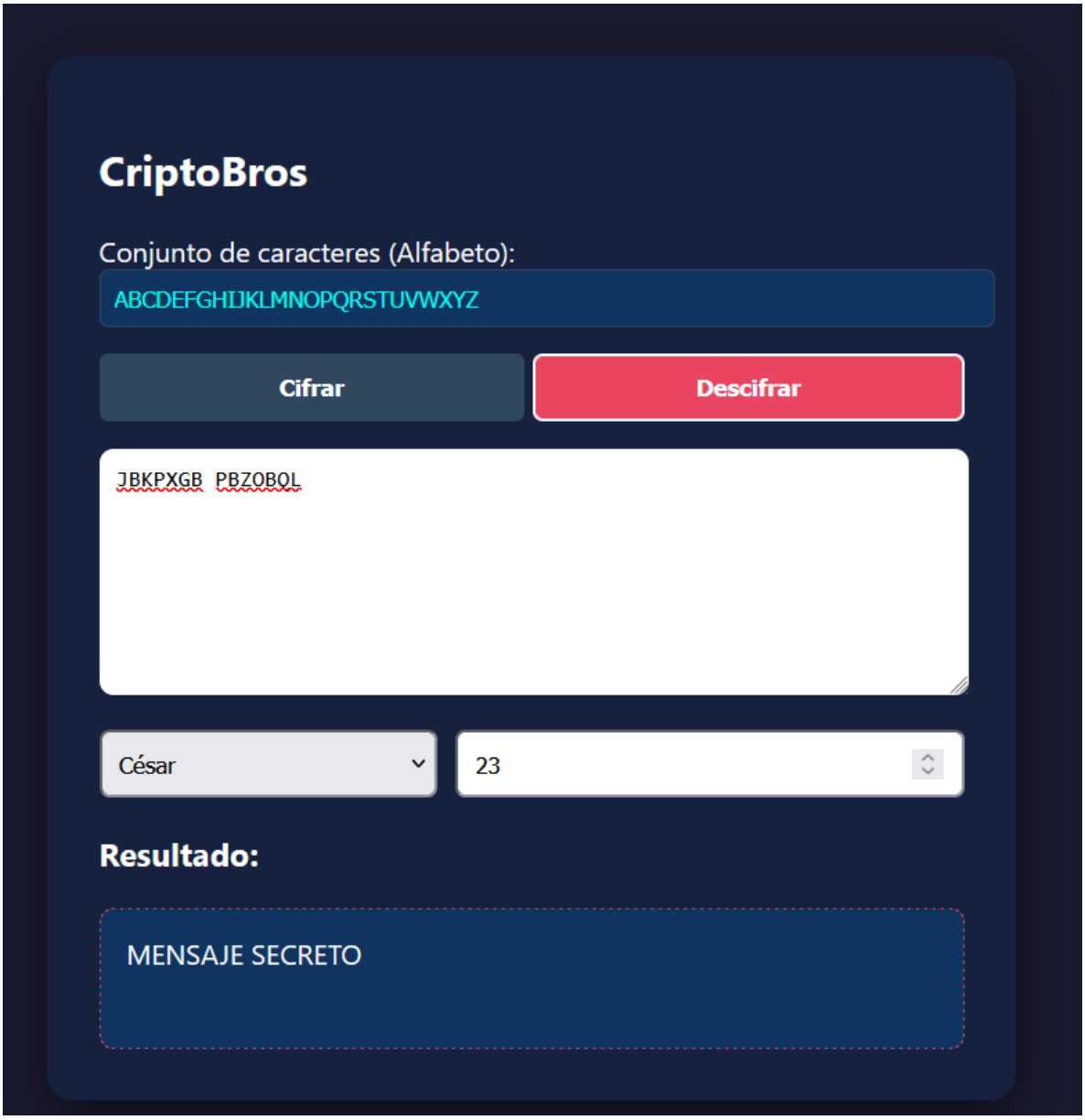

Ilustración 9 descifrando mensaje

A continuación, se presenta el código del sistema, la explicación del código se encuentra en el documento “EXPLICACIÓN_DEL_CODIGO.pdf” cada bloque de código tiene en el comentario un índice que hacer referencia a un registro de tabla en el otro documento.

Index.html:

index.html > html > body

```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <title>CriptoApp - Cesar & Atbash</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>
    <div class="container">
        <h2>CriptoBros</h2>

        <label>Conjunto de caracteres (Alfabeto):</label>
        <input type="text" id="charset" value="ABCDEFGHIJKLMNOPQRSTUVWXYZ">

        <div class="mode-selector">
            <button id="btnEncrypt" class="active" onclick="setMode('encrypt')">Cifrar</button>
            <button id="btnDecrypt" onclick="setMode('decrypt')">Descifrar</button>
        </div>

        <textarea id="inputText" placeholder="Escribe aquí..." oninput="process()"></textarea>

        <div class="controls">
            <select id="method" onchange="updateUI()">
                <option value="cesar">César</option>
                <option value="atbash">Atbash</option>
            </select>
            <input type="number" id="shift" placeholder="Offset" value="3" oninput="process()">
        </div>

        <h3>Resultado:</h3>
        <div id="result" class="result-box"></div>
    </div>
    <script src="script.js"></script>
</body>
</html>
```

Ilustración 10 index.html

Style.css:

```css
/* [SEC-STY-001]: Definición del entorno visual y tipografía */
body {
    font-family: 'Segoe UI', sans-serif;
    background: #1a1a2e;
    color: white;
    display: flex;
    justify-content: center;
    padding: 50px;
}

/* [SEC-STY-002]: Encapsulamiento del módulo criptográfico */
.container {
    background: #16213e;
    padding: 30px;
    border-radius: 15px;
    box-shadow: 0 10px 30px rgba(0,0,0,0.5);
    width: 100%;
    max-width: 500px;
}

/* [SEC-STY-003]: Interfaz de captura de texto plano/cifrado */
textarea {
    width: 100%;
    height: 100px;
    margin-bottom: 20px;
    border-radius: 8px;
    padding: 10px;
    border: none;
}

.controls {
    display: flex;
    gap: 10px;
    margin-bottom: 20px;
}

select, input {
    padding: 10px;
    border-radius: 5px;
    flex-grow: 1;
}
```

```css
/* [SEC-STY-004]: Estilización de disparadores de acción */
button {
    padding: 10px 20px;
    cursor: pointer;
    border: none;
    border-radius: 5px;
    background: #e94560;
    color: white;
    font-weight: bold;
}

button:hover {
    background: #ff2e63;
}

/* [SEC-STY-005]: Área de visualización de resultados (Criptograma) */
.result-box {
    background: #0f3460;
    padding: 15px;
    border-radius: 8px;
    min-height: 50px;
    word-break: break-all;
    border: 1px dashed #e94560;
}

.mode-selector {
    display: flex;
    gap: 5px;
    margin-bottom: 15px;
}

.mode-selector button {
    flex: 1;
    background: #30475e;
    transition: 0.3s;
}

/* [SEC-STY-006]: Feedback visual de estado de seguridad */
.mode-selector button.active {
    background: #e94560;
    border: 2px solid #fff;
}
```

```css
/* [SEC-STY-007]: Configuración del espacio de búsqueda (Alfabeto) */
#charset {
    width: 100%;
    margin-bottom: 15px;
    background: #0f3460;
    color: #00fff5;
    border: 1px solid #30475e;
    padding: 8px;
}
```

Ilustración 11 style.css

Script.js:

```javascript
let currentMode = 'encrypt';

function setMode(mode) {
    currentMode = mode;
    document.getElementById('btnEncrypt').classList.toggle('active', mode === 'encrypt');
    document.getElementById('btnDecrypt').classList.toggle('active', mode === 'decrypt');
    process();
}

function updateUI() {
    // [SEC-REF-001]
    const method = document.getElementById('method').value;
    const isAtbash = (method === 'atbash');

    document.getElementById('shift').style.visibility = isAtbash ? 'hidden' : 'visible';

    const btnD = document.getElementById('btnDecrypt');
    const btnE = document.getElementById('btnEncrypt');

    if (isAtbash) {
        btnE.innerText = "PROCESO SIMÉTRICO";
        btnE.classList.add('active');
        btnD.style.display = 'none';
    } else {
        btnE.innerText = "Cifrar";
        btnD.style.display = 'inline-block';
        setMode(currentMode);
    }
    process();
}
```

```
function process() {
    const inputField = document.getElementById('inputText');
    const charsetField = document.getElementById('charset');
    // [SEC-REF-002]
    let  let uniqueCharset: string alue.toUpperCase();
    let uniqueCharset = [...new Set(rawCharset)].join('');
    if (charsetField.value !== uniqueCharset) {
        charsetField.value = uniqueCharset;
    }
    const text = inputField.value.toUpperCase();
    inputField.value = text;
    const method = document.getElementById('method').value;
    const shift = parseInt(document.getElementById('shift').value) || 0;
    const n = uniqueCharset.length;
    let output = "";
    if (n === 0) {
        document.getElementById('result').innerText = text;
        return;
    }
    for (let char of text) {
        const index = uniqueCharset.indexOf(char);

        if (index === -1) {
            // [SEC-REF-003]
            output += char;
            continue;
        }
        if (method === 'cesar') {
            // [SEC-REF-004]
            let move = (currentMode === 'encrypt') ? shift : -shift;
            let newIndex = (index + move) % n;
            if (newIndex < 0) newIndex += n;
            output += uniqueCharset[newIndex];
        }
        else if (method === 'atbash') {
            // [SEC-REF-005]
            output += uniqueCharset[(n - 1) - index];
        }
    }
    document.getElementById('result').innerText = output;
}
```

```
// [SEC-REF-006]
try { updateUI(); } catch(e) {}
```

Ilustración 12 Script.js

CONSLUSIÓN

Este trabajo escolar permitió comprender la evolución de la criptografía desde sus bases más simples. Se demostró que, aunque el cifrado Atbash y César son lógicamente consistentes, su seguridad depende enteramente del secreto del alfabeto y no de la complejidad algorítmica. La implementación web facilita la comprensión visual de cómo la manipulación de caracteres ASCII transforma la información.

BIBLIOGRAFIA

Al-Kindi, *Manuscrito sobre el Desciframiento de Mensajes Criptográficos*.