ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

DESARROLLO DE UNA APLICACIÓN WEB PARA EL CIFRADO Y DESCIFRADO DE CADENAS DE TEXTO A PARTIR DE LA SELECCIÓN DE UN ATRACTOR CAÓTICO

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar el grado académico de:

INGENIERA DE SOFTWARE

AUTORA:

JEMMY ANAHÍ PUZMA GRANDA

Riobamba – Ecuador

2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

DESARROLLO DE UNA APLICACIÓN WEB PARA EL CIFRADO Y DESCIFRADO DE CADENAS DE TEXTO A PARTIR DE LA SELECCIÓN DE UN ATRACTOR CAÓTICO

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar el grado académico de:

INGENIERA DE SOFTWARE

AUTORA: JEMMY ANAHÍ PUZMA GRANDA

DIRECTOR: ING. OMAR SALVADOR GÓMEZ GÓMEZ

Riobamba – Ecuador

2023

Yo, Jemmy Anahí Puzma Granda, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autora asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 04 de diciembre 2023.

Jemmy Anahí Puzma Granda
1105164121

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular; Tipo: Proyecto Técnico **DESARROLLO DE UNA APLICACIÓN WEB PARA EL CIFRADO Y DESCIFRADO DE CADENAS DE TEXTO A PARTIR DE LA SELECCIÓN DE UN ATRACTOR CAÓTICO**, realizado por la señorita: **JEMMY ANAHÍ PUZMA GRANDA**, ha sido minuciosamente revisado por los Miembros del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	FECHA
Ing. Raúl Hernán Rosero Miranda **PRESIDENTE DEL TRIBUNAL**		2023-12-04
Ing. Omar Salvador Gómez Gómez **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2023-12-04
Ing. Danilo Mauricio Pástor Ramírez **ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2023-12-04

DEDICATORIA

Con el corazón lleno de amor y gratitud, dedico este logro a las personas que han sido mi mayor apoyo y alegría en este viaje.

A mi amado padre, Carlos María Puzma Gómez, por ser la guía con su sabiduría y fortaleza inquebrantable. Eres el faro que ilumina mi camino en los momentos más oscuros.

A mi querida madre, Inés Graciela Granda Capa, cuyo amor incondicional y sacrificio han sido la luz que ha guiado cada uno de mis pasos. Tu presencia es el abrazo que me reconforta en cada desafío.

A mi hermana mayor, Jessica Ortiz, por ser un pilar de fuerza y un ejemplo de perseverancia. Tu apoyo inquebrantable ha sido esencial en mi vida.

A mis hermanos menores, Jhelen Deney, Eliane Karps y Rizier Justin, por llenar nuestra casa con risas y sueños. Vuestra alegría es el regalo más precioso que tengo.

A mi hijo, Bradley Daniel Aldaz Puzma, mi luz y mi razón de ser. Cada día lejos de ti fue un desafío, lleno de anhelos y esperanzas. Tu sonrisa y tu amor han sido mi refugio en la distancia, recordándome por qué cada esfuerzo vale la pena. Eres mi inspiración diaria y mi mayor orgullo. En ti veo un futuro lleno de esperanza y maravillas, y prometo estar siempre a tu lado, guiándote y apoyándote.

A mi mejor amiga, Samantha Guerrero, y a su familia, por abrirme sus corazones y su hogar en los momentos en que estuve lejos de los míos. Samantha, tu amistad ha sido un tesoro invaluable, y los momentos que hemos compartido son joyas que guardaré por siempre en mi corazón.

Gracias a cada uno de ustedes por ser parte de mi vida, por sus enseñanzas, su amor y su incondicional apoyo. Esta tesis es más que un logro académico; es un testimonio de lo que podemos alcanzar cuando estamos rodeados de personas extraordinarias como ustedes.

Con todo mi amor,

Jemmy Anahi Puzma Granda.

AGRADECIMIENTO

En este significativo momento de culminación y reflexión, deseo expresar mi más sincero agradecimiento a aquellos que han sido parte fundamental de este viaje académico y personal.

Mi gratitud inicial es para la Escuela Superior Politécnica del Chimborazo, una institución que no solo me brindó la oportunidad de obtener una profesión, sino que también me enseñó el valor de ser una contribución positiva a la sociedad. Esta experiencia ha sido mucho más que una educación; ha sido una transformación, preparándome para enfrentar los desafíos del mundo con conocimiento, ética y compromiso.

A mis docentes, les extiendo un agradecimiento especial. Gracias por compartir su sabiduría, por su paciencia y dedicación. Cada lección, cada consejo y cada palabra de aliento han sido pilares en mi formación. Su influencia trasciende las aulas y permanecerá conmigo en mi carrera profesional.

También quiero agradecer a aquellos docentes que me presentaron desafíos adicionales, incluso a través de materias que no logré pasar en el primer intento. Estas experiencias, aunque difíciles en su momento, me enseñaron la importancia de la perseverancia, la resiliencia y el crecimiento personal. A través de estos obstáculos, he aprendido lecciones valiosas que van más allá del conocimiento académico, fortaleciendo mi carácter y mi determinación.

Un agradecimiento especial al grupo de investigación GrIISoft, por permitirme involucrarme en el campo de la investigación del caos matemático y la sincronización caótica. Su apoyo, orientación y la oportunidad de trabajar en proyectos innovadores han sido fundamentales en mi desarrollo académico y profesional. Esta experiencia ha enriquecido mi perspectiva y ha ampliado los horizontes de mi conocimiento.

Cada paso en este camino ha sido esencial para mi desarrollo, y estoy profundamente agradecido por todas las experiencias que he tenido en la Escuela Superior Politécnica del Chimborazo y con el grupo GrIISoft. Este logro no solo representa un título académico, sino también el esfuerzo, la dedicación y el aprendizaje que cada uno de ustedes ha fomentado en mí.

Con gratitud,

Jemmy

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

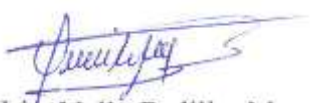
El presente estudio se embarca en la exploración de la criptografía basada en atractores caóticos, desarrollando una aplicación web destinada al cifrado y descifrado de cadenas de texto utilizando la sincronización de estos atractores. El primer paso de este estudio involucró una revisión detallada de cuatro sistemas caóticos para comprender a fondo las fórmulas de cada atractor. A través de una combinación de análisis matemático y programación, se implementó la sincronización de cada atractor en la aplicación web, utilizando la metodología SCRUMBAN, una combinación de los marcos de trabajo ágiles Scrum y Kanban. La aplicación resultante, intuitiva y fácil de usar, proporciona una interfaz eficiente para el cifrado y descifrado de cadenas de texto. En la evaluación de la aplicación, se tomaron en cuenta factores como el tiempo de sincronización, cifrado y descifrado. Las pruebas de Kruskal-Wallis, una prueba estadística no paramétrica utilizada para comparar tres o más grupos independientes de datos, revelaron diferencias significativas en los tiempos de sincronización, cifrado y descifrado entre los cuatro atractores. En términos concretos, estos resultados sugieren que al menos uno de los atractores estudiados ofrece un rendimiento sustancialmente distinto de los demás. Estos hallazgos destacan el potencial de los atractores caóticos para mejorar la seguridad de la información en la era digital. Asimismo, el trabajo realizado en esta tesis demuestra cómo se puede facilitar la implementación de la criptografía basada en atractores caóticos a través de una aplicación web, haciéndola accesible a un público más amplio. En resumen, esta tesis representa un importante paso hacia la mejora de los métodos de cifrado y descifrado de datos. Los resultados obtenidos sugieren que la selección cuidadosa de un atractor caótico puede tener un impacto significativo en la optimización de los tiempos de sincronización, cifrado y descifrado, ofreciendo una vía prometedora para futuras investigaciones en el campo de la criptografía.

Palabras clave: <CRIPTOGRAFÍA>, <ATRACTORES CAÓTICOS>, <SINCRONIZACIÓN CAÓTICA>, <CIFRADO DE TEXTO>, <DESCIFRADO DE TEXTO>, <APLICACIÓN WEB>, <SEGURIDAD DE LA INFORMACIÓN>, <SISTEMAS DINÁMICOS NO LINEALES>.

SUMMARY

The present study has to do with the exploration of cryptography based on chaotic attractors, developing a web application intended for the encryption and decryption of text strings using the synchronization of these attractors. The first step of this study involved a detailed review of four chaotic systems to fully understand the formulas of each attractor. Through a combination of mathematical analysis and programming, synchronization of each attractor was implemented in the web application, using the SCRUMBAN methodology, a combination of the agile frameworks Scrum and Kanban. The resulting intuitive and easy-to-use application provides an efficient interface for encryption and decryption of text strings. When evaluating the application, factors such as synchronization, encryption and decryption time were taken into account. Kruskal-Wallis tests, a non-parametric statistical test used to compare three or more independent sets of data, revealed significant differences in synchronization, encryption, and decryption times between the four attractors. In concrete terms, these results suggest that at least one of the attractors studied offers substantially different performance from the others. These findings highlight the potential of chaotic attractors to improve information security in the digital age. Likewise, the work carried out in this thesis demonstrates how the implementation of cryptography based on chaotic attractors can be facilitated through a web application, making it accessible to a broader audience. In summary, this thesis represents an important step towards improving data encryption and decryption methods. The results obtained suggest that the careful selection of a chaotic attractor can have a significant impact on the optimization of synchronization, encryption and decryption times, offering a promising avenue for future research in the field of cryptography.

Key words: <CRYPTOGRAPHY>, <CHAOTIC ATTRACTORS>, <CHAOTIC SYNCHRONIZATION>, <TEXT ENCRYPTION>, <TEXT DECRYPTION>, <WEB APPLICATION >, < INFORMATION SECURITY >, < NON-LINEAR DYNAMIC SYSTEMS >



Lic. Nelly Padilla. Mgs
0603818717
DOCENTE FIE

INTRODUCCIÓN

En la era de la información, la seguridad de los datos es de suma importancia. La criptografía, el arte de proteger la información transformándola en una forma incomprensible para quienes no poseen la clave adecuada, es una herramienta vital en este escenario. En los últimos años, los avances en la informática y las matemáticas han permitido la creación de algoritmos de cifrado más robustos y seguros, siendo los atractores caóticos uno de los enfoques más recientes y prometedores.

Este trabajo se centra en el desarrollo de una aplicación web para el cifrado y descifrado de cadenas de texto utilizando atractores caóticos. Los atractores caóticos, patrones complejos que emergen de sistemas dinámicos no lineales, poseen propiedades de sensibilidad a las condiciones iniciales y mezcla topológica, que se convierten en una base excelente para algoritmos de cifrado. Aprovechando estas propiedades, se puede crear un sistema de cifrado que es altamente seguro y difícil de romper.

El presente trabajo de titulación está organizado en varios capítulos que describen en detalle el desarrollo de esta aplicación web. Se discutirán los fundamentos de los sistemas de cifrado, los atractores caóticos, la implementación del algoritmo de cifrado basado en atractores caóticos y la creación de la aplicación web. También se abordará la evaluación de la eficiencia en el desempeño, seguridad del sistema de cifrado y su aplicabilidad práctica.

A través de este estudio, se espera contribuir al creciente cuerpo de estudio en criptografía basada en atractores caóticos y demostrar la aplicabilidad de este enfoque en la construcción de sistemas de cifrados seguros y eficientes. Al final, la tesis buscará responder a la pregunta central de cómo se puede desarrollar una aplicación web para el cifrado y descifrado de cadenas de texto a partir de la selección de un atractor caótico, brindando un nuevo instrumento para garantizar la seguridad de la información en la era digital.

CAPÍTULO I

1 DIAGNÓSTICO DEL PROBLEMA

1.1 Planteamiento del problema

1.1.1 *Antecedentes*

En la actualidad, la necesidad de recibir y enviar información digitalmente es importante dado que es el principal medio para ello, es rápido y permite que las personas accedan a ésta en cualquier momento. Hoy en día la mayor parte de información generada por aparatos electrónicos conectados a internet suele almacenarse en servicios digitales alojados en centros de datos conocidos como la nube digital. Dado este volumen de datos que circula por el Internet, donde una parte importante corresponde al tipo personal o sensible, es imprescindible hacer uso de mecanismos de protección de información como la criptografía (FIBK 2018).

Para proteger la información se utiliza la criptografía porque desarrolla procedimientos que permiten evitar el acceso no deseado a datos sensibles (personales, sanitarios, bancarios, etc.), de manera que quede protegida del mal uso o abusos de determinados grupos u organizaciones que pudieran hacer de ella La criptografía tiene como objetivos principales asegurar la integridad, confidencialidad y autenticidad de la información (Fuster Sabater et al. 2012).

La criptografía dio un gran salto en su desarrollo estimulado por tres hechos importantes. En primer lugar, el establecimiento del criptosistema de clave simétrica DES (Data Encryption Standard) como estándar comercial para el cifrado de la información. En segundo lugar, el protocolo de intercambio de claves de Diffie y Hellman (1976). Por último, el surgimiento de los sistemas prácticos del cifrado de clave pública RSA (1978) y ElGamal (1985) (Orúe López 2013).

Con estos hallazgos las claves o llaves de cifrado pudieron distribuirse de una manera razonablemente segura entre las partes interesadas, quedando una parte resuelto el problema de la distribución de claves, pero queda pendiente el problema de la confianza con una tercera parte certificadora, encargada de validar las claves públicas de los usuarios (Orúe López 2013).

Existen algunos métodos de cifrado de claves públicas, pero en su mayoría no ofrecen velocidades adecuadas para imágenes y archivos de gran tamaño, de modo que estos emplean el cifrado simétrico. La seguridad de estos métodos se basa en un problema matemático difícil de resolver. Los avances en las técnicas de algoritmos, teoría de números, y la computación distribuida son impredecibles, y es probable que haya que volver a cifrar grandes bases de datos y archivos con claves más largas, para mantener un grado suficiente de su seguridad (Fridrich 2011).

Para tener un cifrado seguro se utiliza la sincronización caótica, es la inducción de un régimen en el cual dos sistemas caóticos (maestro y esclavo) exhiben trayectorias idénticas ($X_m = X_s$) luego de introducir algún tipo de acoplamiento entre ellos (Rodríguez Liñán y León Morales 2007).

Por otra parte, un sistema dinámico se define como un campo vectorial en un espacio euclidiano (Espacio bidimensional o tridimensional en el que se cumplen los axiomas de Euclides[1]) $\mathbb{R}^n$, o bien de una función que va de $\mathbb{R}^n$ en sí mismo (Lacomba 2000).

Durante el siglo pasado, los científicos clasificaban a los sistemas según su grado de predictibilidad. Así, un sistema es determinístico cuando su comportamiento es bastante predecible, determinado, cuando parece seguir unas ciertas reglas y es probabilístico cuando no hay certeza de su estado futuro. No obstante, esta rústica clasificación sufrió severos impactos durante el último medio siglo. Por ejemplo, se descubrió que muchos sistemas dinámicos no lineales se comportan en ciertas condiciones de forma tan compleja que parecen probabilísticos, aunque, en realidad, son determinísticos. En otras palabras, a pesar de que las reglas son muy simples, el sistema a nivel global puede tener un comportamiento inesperado, no predecible. Se trata de un sistema caótico (Moriello 2003).

Un atractor es el conjunto de puntos hacia los cuales tiende un sistema dinámico tras un número elevado de iteraciones infinitas, y el caos viene por su gran sensibilidad a variaciones en las condiciones iniciales y a que los valores obtenidos nunca se repiten exactamente, estas definiciones juntas forman un atractor caótico (Díaz Soriano 2022).

Entre los atractores que se va a utilizar se encuentra Rossler, Lorenz, Chen y Sprott, estos comparten características similares, ya que para el sistema maestro y esclavo se necesitan tres condiciones iniciales X, Y, Z. Al final se logra la sincronización mediante la resta de los elementos de los vectores del maestro y del esclavo los cuales en un punto se reducen a 0.

Lorenz formuló un modelo tridimensional para realizar predicciones climatológicas y notó que, si el modelo se alimentaba de la observación anterior con cifras redondeadas, en lugar de las cifras reales, este se comportaba inicialmente de la misma forma, pero rápidamente comenzaban a

[1] Dados dos puntos se pueden trazar una recta que los une.
Cualquier segmento puede ser prolongado de forma no continua en una recta ilimitada en la misma dirección.
Se puede trazar una circunferencia de centro en cualquier punto y radio cualquiera.
Todos los ángulos rectos son iguales.
Por un punto exterior a una recta se puede trazar una única paralela. Guerrero (2004)

trazarse trayectorias totalmente distintas a las seguidas cuando las cifras eran las reales, lo cual generaba predicciones erróneas en las condiciones climatológicas (Moreno et al. 2016).

El modelo de Lorenz se describe en la ecuación (1).

$$\frac{dx}{dt} = a(y - x) \quad \frac{dy}{dt} = a(b - z) - y \quad \frac{dz}{dt} = xy - cx \qquad (1)$$

Donde cada punto (x; y; z) representa un estado de la atmósfera y, a, b, c son parámetros. Para analizar su evolución se debe seguir un campo de vectores, dicho sistema presenta comportamiento caótico para varios valores de los parámetros y originó todo un desarrollo en la teoría de los sistemas dinámicos caóticos (Moreno et al. 2016).

Otto Rössler diseñó el atractor que lleva su nombre en 1976, y más tarde se descubrió que las ecuaciones originalmente teóricas eran útiles para modelar el equilibrio en las reacciones químicas. Se observa en la ecuación (2), (3) y (4) (Zhang et al. 2009).

$$\frac{dx}{dt} = -y - z \qquad (2)$$

Las ecuaciones definitorias son: $\frac{dy}{dt} = x + ay$ (3)

$$\frac{dz}{dt} = b + z(x - c) \qquad (4)$$

donde x, y, z son las variables de estado y a, b, c son parámetros del sistema.

En 1999, Chen encontró otro atractor caótico, que es el dual del sistema de Lorenz y tiene una estructura similar, pero muestra comportamientos dinámicos aún más sofisticados (Lü, Chen y Zhang 2002).

Los atractores clásicos de Lorenz, Rossler, Chen y Sprott son los excitados por equilibrios inestables. Desde un punto de vista computacional, esto permite utilizar un método numérico en el que, una trayectoria iniciada desde un punto en la variedad inestable de un equilibrio alcanza un atractor y lo identifica (Jafari, Sprott y Nazarimehr 2015).

Por otro lado, se ha observado que, en varias empresas, su información ha sido expuesta públicamente debido a múltiples factores. Entre ellos, destaca que el método de encriptación empleado es familiar para el atacante, facilitando su descifrado. En algunos casos, el algoritmo de encriptación utilizado no representa un desafío considerable para el atacante o, peor aún, la información no está encriptada en absoluto. Este tipo de brechas de seguridad pueden dar lugar a

un uso malintencionado de la información, comprometiendo la integridad personal y corporativa. Además, los atacantes pueden aprovechar estos puntos débiles para implementar virus con el fin de dañar sistemas específicos (Telcel 2023).

Orue López (2013) propuso el estudio del criptoanálisis y diseño de los criptosistemas caóticos, para generar secuencias pseudoaleatorias seguros y rápidos. Lo divide en tres fases, primero se realiza un análisis teórico de las propiedades geométricas de algunos de los sistemas caóticos más empleados en el diseño de criptosistemas; en segundo lugar, se realiza el criptoanálisis de cifrados caóticos continuos basados en el análisis anterior; y, finalmente, se realizan las propuestas de diseño.

Zhu (2015) diseña y presenta un nuevo método para la transmisión segura de información mediante un sistema de comunicación caótico. La arquitectura del sistema de comunicación la construyó utilizando un transmisor y receptor Rössler. Finalmente logró obtener una señal de mensaje incrustada en el transmisor que puede ser extraída por un receptor Rössler estabilizado.

Para dar solución a la problemática planteada se presentará una aplicación web la cual va a utilizar el cifrado y descifrado de cadenas de texto a través de la sincronización caótica probando cuatro atractores distintos mencionados anteriormente, los que después se evaluará el tiempo de respuesta, seguridad y se analizarán resultados.

Este trabajo de integración curricular está dirigido a la Escuela Superior Politécnica del Chimborazo, Facultad de Informática y Electrónica, carrera Software, ya que es parte del Grupo de Investigación en Ingeniería de Software (GrIISoft) adscrito a la FIE-ESPOCH con el código IDIPI-283 y nombre de proyecto Enfoque de cifrado de objetos JSON utilizando sincronización caótica a partir del análisis de un conjunto de atractores. Aprobado mediante resolución 638. CP. 2022.

1.1.2 *Formulación del problema*

¿Cuál es la eficiencia, seguridad en el cifrado y descifrado de cadenas de texto utilizando sincronización caótica con los atractores Rossler, Lorenz, Chen y Sprott a través del desarrollo de una aplicación web?

1.1.3 *Sistematización del problema*

¿Cuáles son las características de los atractores caóticos seleccionados para el desarrollo del trabajo de integración curricular?
¿Cómo realizar la sincronización del maestro y esclavo de cada atractor caótico?

¿Cuáles son los componentes y módulos que forman parte de la aplicación web?
¿Cuáles son las estadísticas de eficiencia y seguridad de cada atractor caótico?

1.2 Justificación

1.2.1 *Justificación teórica*

La sincronización caótica es de gran interés práctico, ya que mediante ella es posible realizar importantes aplicaciones para cifrado de información en servicios de telecomunicaciones tales como: Enlaces de comunicación militar y empresas privadas, transacciones financieras, operaciones comerciales con firmas electrónicas por Internet, y otros (Rodríguez Liñán y León Morales 2007).

Se usan los sistemas caóticos para esconder información que se quiere mantener privada, ya que las señales caóticas se comportan erráticamente y parece que se está enviando sólo ruido en vez de información. De esta manera se crea una disciplina que se llama criptografía, que en resumen es un conjunto de técnicas para la escritura secreta u oculta (Library 2022).

Dado que los sistemas caóticos evolucionan aleatoriamente y generan oscilaciones multifrecuencia (desde 1 Hz hasta miles de Hz), se pueden agregar mensajes que describen el comportamiento en un número limitado de frecuencias (por ejemplo, la voz humana evoluciona entre 300 Hz y 4 Khz), por lo que el mensaje en la transmisión no se nota (Moreno et al. 2016).

El cifrado tiene algunas limitaciones prácticas visibles, tales como: No hay protección en los mensajes de entrada de los algoritmos, el cambio de clave ocurre en los mismos canales cuando se transmiten los datos, el cifrado no protege contra cambios, puede detectarse mediante múltiples controles de bits como parte de los datos encriptados (Moreno et al. 2016).

Por ello, es importante tomar en cuenta lo que Moreno et al. (2016) menciona, al utilizar un modelo de encriptación basado en la complejidad de las reglas es difícil de resolver, ya que a mayor complejidad es más trabajoso predecir el comportamiento futuro del sistema de encriptación; sin embargo, si las reglas no son lo suficientemente complejas el sistema de encriptación se vuelve vulnerable. Es por tal motivo que se necesita desarrollar algoritmos con reglas complejas para que el sistema de encriptación no sea frágil y no pueda sufrir ataques fácilmente.

Lo que ha servido de apoyo para desarrollar una aplicación web utilizando cuatro algoritmos de encriptación basado en sistemas caóticos, es que la mayoría de los sistemas de cifrado son sensibles a las condiciones iniciales y a los parámetros utilizados en la ecuación de recurrencia la cual sirve de base para un sistema caótico. En el desarrollo de la aplicación web se utilizará el

lenguaje Python para el back-end y javascript para el front-end porque Python es una gran opción para el desarrollo de software, ya que permite a los desarrolladores graficar funciones. Además, se puede utilizar para scripts web, desarrollo de GUI (Interfaz gráfica de usuario) de escritorio o ciencia de datos.

1.2.2 *Justificación aplicativa*

Esta investigación se realiza porque existe la necesidad de mejorar el nivel de seguridad en el cifrado y descifrado de cadenas de texto, se basa en la utilización de un atractor caótico ya que el vínculo entre la criptografía y los sistemas caóticos continúa siendo objeto de un intenso estudio, con el uso de los atractores se mide el tiempo de respuesta, una gráfica comparativa del texto cifrado y sin cifrar para verificar si existe cambios significativos, al finalizar se realiza el respectivo análisis.

Los módulos contemplados para esta aplicación son los siguientes:

Capa de persistencia:

- **Módulo acceso a datos:** Encargado de almacenar y recuperar las cadenas de texto cifradas.

Capa de lógica del negocio:

- **Módulo de encriptación:** Encargado de cifrar y descifrar cadenas de texto mediante la sincronización caótica.
- **Módulo controlador:** Controla como se muestra los datos en la capa presentación.
- **Módulo autenticación:** Contiene las funcionalidades Login/Logout dentro del sistema, como registrarse, autenticarse.
- **Módulo de estadísticas:** Contiene los datos estadísticos de cada ejecución realizada, la cual se verá reflejado el número de textos cifrados por cada atractor con sus respectivos resultados.

Capa de presentación:

- **Módulo de UI:** Encargado de permitir la interacción del usuario con el sistema. Contiene los archivos con código HTML CSS.
- **Módulo procesos:** Encargado de la recuperación de datos y de cómo se muestran al usuario.

El Trabajo de Integración Curricular coincide con la línea de investigación de la Escuela de Ingeniería en Software: Ciencias, programa: Seguridad de Sistemas de Información. De la misma forma también, con los lineamientos de la ESPOCH dentro de eje: TIC’s Tecnologías de la Información y Comunicación, y programa: Seguridad de Sistemas de Información. Además de ello, el trabajo cumple el objetivo 5 propuesto por el Plan Nacional de Desarrollo, el cual busca

impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria.

Forma parte del proyecto de investigación IDIPI-283 con el nombre Enfoque de cifrado de objetos JSON utilizando sincronización caótica a partir del análisis de un conjunto de atractores, aprobado mediante resolución 638. CP.2022 del consejo politécnico de la ESPOCH.

1.3 Objetivos

1.3.1 *Objetivo general*

Desarrollar una aplicación web para cifrar y descifrar cadenas de texto mediante la sincronización caótica utilizando la metodología SCRUMBAN.

1.3.2 *Objetivos específicos*

- Revisar cuatro sistemas caóticos, para entender las fórmulas de cada atractor.
- Efectuar la sincronización caótica en cada atractor seleccionado.
- Desarrollar la aplicación web para el cifrado y descifrado de cadenas de texto mediante sincronización caótica utilizando la metodología SCRUMBAN.
- Evaluar la eficiencia y seguridad en el cifrado y descifrado de cadenas de texto en la aplicación desarrollada.

CAPÍTULO II

2 MARCO TEÓRICO

Este capítulo está enfocado en la revisión y análisis de la literatura existente sobre el tema del trabajo de integración curricular, para identificar los conceptos clave como: criptografía, caos y atractores. Enfoques relevantes que se aplicarán en el estudio por ejemplo fórmulas y sincronización caótica.

2.1 Criptografía basada en clave asimétrica

En esta criptografía, cada usuario posee dos claves: una pública y otra privada. La primera la da a conocer a todos aquellos de los que desea recibir mensajes cifrados y es la que estos utilizan para cifrar la información que le van a enviar. La segunda la guarda en secreto y es la que le permite descifrar la información recibida. Como se puede deducir, ambas claves deben estar relacionadas para que cada una de ellas invierta el proceso realizado por la otra, pero esta relación ha de ser lo suficientemente compleja como para que sea imposible o, al menos, muy difícil, deducir la clave privada a partir del conocimiento de la pública (Hernández Encinas 2016).

La idea de este cifrado es que, tal como indica su nombre, la clave pública no es secreta, de forma que si alguien quiere enviar información cifrada deberá pedir la clave pública. Cuando esta se haya enviado, si alguien intercepta el mensaje solamente verá texto sin sentido, y solamente la persona con la clave privada podría descifrarla. Con esto se soluciona el problema de distribuir las claves, aunque se debe de tener en cuenta una sutileza, y es que el cifrado asimétrico es más lento debido a su complejidad extra. El autor Bea Monreal (2020) menciona que, es habitual el cifrado usando el sobre digital, que consiste en lo siguiente:

1. El emisor genera una clave privada de un uso y cifra el mensaje con ella.
2. El emisor pide al receptor su clave pública.
3. El emisor envía al receptor el mensaje y la clave de cifrado.
4. El receptor descifra el mensaje con su clave privada asociada a la clave pública que ha mandado al emisor.

A continuación, se muestra en la Figura 1-2 el proceso de cifrado:

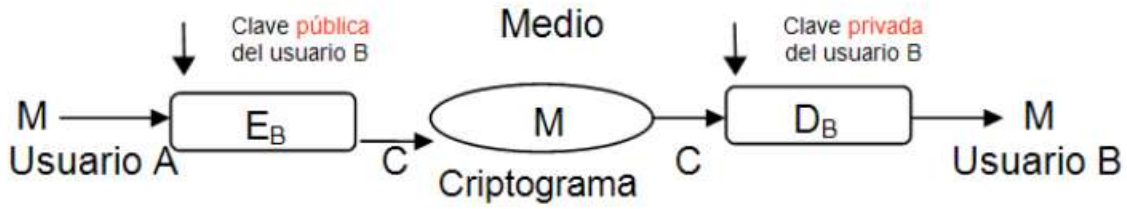


Figura 1-2: Proceso de cifrado

Fuente: (Arias 2022).

2.1.1 *RSA*

Es un algoritmo de cifrado asimétrico, debe su nombre a las iniciales de sus creadores: Ronald Rivest, Adi Shamir y Leonard Adleman. La idea de su funcionamiento lo plantea Bea Monreal (2020) de la siguiente manera:

1. Se generan dos números primos grandes p y q de tamaños similares.
2. Se obtiene $n = p * q$. Generalmente $2^{1024} \leq n \leq 2^{2048}$, por lo que p y q tendrán que ser elegidos teniendo esto en cuenta.
3. Se elige un número primo pequeño, habitualmente el 65537.
4. Se obtiene d, tal que $d * e \equiv 1 \ (mod\ \varphi\ (n))$. A tener en cuenta que $\varphi\ (n)$ es la función Phi de Euler, que, en este caso $n = p * q$, entonces $\varphi(n) = \varphi(p) * \varphi(q) = (p-1) * (q-1)$. También se debe tener presente que existe d cuando $MCD\ (e,\ \varphi(n)) = 1$ y, más en concreto, si e es primo siempre existirá. El elemento d se calcula mediante al algoritmo extendido de Euclides.
5. Se obtiene la clave pública (e, n) y la clave privada $(d. n)$.

2.1.2 *DH*

Se trata de un protocolo que permite adoptar una clave entre dos partes que no tienen contacto entre ellas, es decir, se genera una clave de un algoritmo simétrico para cifrar los mensajes entre dos partes a partir de un par de claves pública y privada en lugar de compartir una clave simétrica utilizando un algoritmo de clave pública El nombre se debe a sus creadores Whitfield Diffie y Martin Hellman. Bea Monreal (2020) muestra su funcionamiento:

1. Ambas partes se ponen de acuerdo en un primo p que será el módulo y un generador g público.
2. La primera parte elige un número $a < p$ y la segunda un $b < p$ privados.
3. La primera parte calcula $A = g^a \ mod\ p$ y se la envía la segunda. La segunda parte calcula $B = \ g^b \ mod\ p$ y se la envía a la primera.

4. La primera parte calcula $(B\ mod\ p)^a = \left(g^b\ mod\ p\right)^a = g^{b*a}\ mod\ p$. La segunda parte Calcula $(A\ mod\ p)^b = (g^a\ mod\ p)^b = g^{a*b}\ mod\ p = g^{b*a}\ mod\ p$.
Se obtiene que ambos cálculos son iguales, por lo que se puede utilizar como clave compartida.

2.2 Criptografía basada en clave simétrica

Los sistemas de cifrado tienen la particularidad de que tanto el emisor como el receptor utilizan la misma clave ya sea para cifrar o para descifrar, si bien el proceso de descifrado puede ser ligeramente diferente al de cifrado, pero no sustancialmente. Cuando sucede esto, se dice que el sistema de cifrado es de clave simétrica o de clave secreta. La razón es que en ambos extremos de la comunicación la clave es la misma y esta debe mantenerse en secreto por los dos usuarios, no debiendo compartirla con nadie (Hernández Encinas 2016).

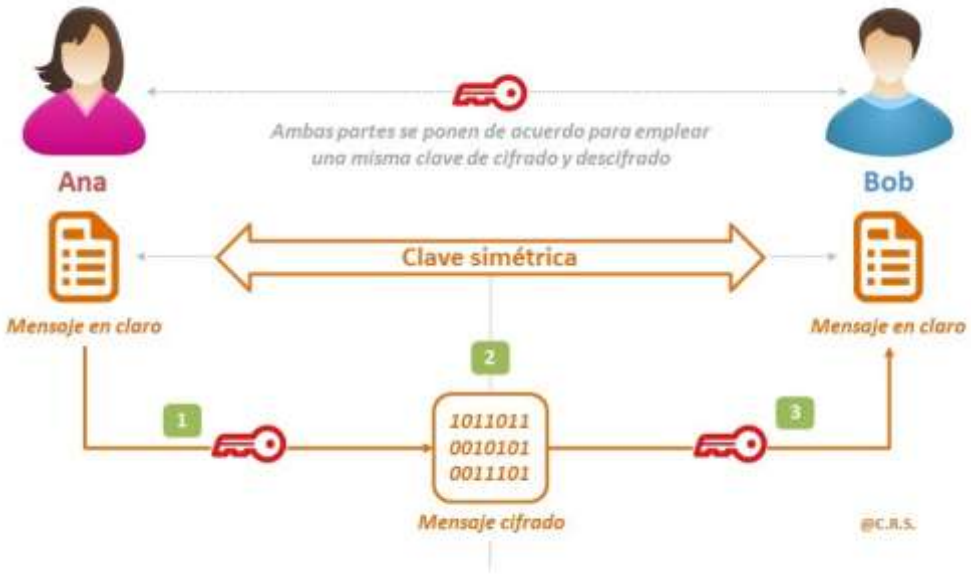


Figura 2-2: Proceso de cifrado con clave simétrica

Fuente: (Martínez 2022).

En la Figura 2-2 se observa que tanto el emisor como el receptor se ponen de acuerdo para utilizar la misma clave de cifrado, después procede a enviar el mensaje, luego el mensaje se cifra hasta llegar al receptor, dónde se utiliza la clave para descifrar y observar el contenido del mensaje.

2.2.1 *Cifrado de flujo*

Primeramente, se debe disponer de un generador de bits arbitrarios, llamado generador de flujo de clave. Generalmente la idea es que el texto en claro se cifra bit a bit, en el que cada bit se combina mediante la función XOR con uno de los bits generados. Utilizar la operación OR exclusivo (XOR) es lo habitual debido a que el cifrado y el descifrado son la misma operación (Bea Monreal 2020).

Se observa en la Figura 3-2 el proceso de cifrado de flujo:

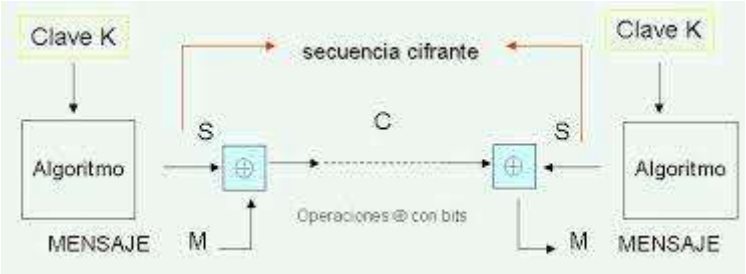


Figura 3-2: Cifrado de flujo

Fuente: (Padrón-Godínez et al. 2015).

La secuencia cifrante ideal es una secuencia infinita, determinada por una clave de manera que parezca aleatoria y que ningún enemigo pueda generarla. El cifrado de flujo y llave secreta conforman un criptosistema incondicionalmente seguro, debido al tiempo que tarda en realizarse, ver Figura 3-2. Allí se realiza la construcción de la llave larga a partir de la inicial corta, se necesita un generador pseudoaleatorio de secuencias binario. Este generador puede ser lineal o no, consiste en una semilla inicial para el generador y una secuencia cifrante o de cifrado (Padrón-Godínez et al. 2015).

2.2.2 *Cifrado de bloque*

En este caso se cifra por bloques, es decir, se divide el texto en bloques de bytes (generalmente de 8 o 16 bytes) y se cifran por separado. El texto cifrado de un bloque será del mismo tamaño que el original.

Bea Monreal (2020) menciona una ventaja de este tipo de cifrados, la cual es que permiten la reutilización de las claves, lo que no es posible en los de flujo debido al funcionamiento.

Arias (2022) resume los dos sistemas de la siguiente manera:

- Los sistemas de clave pública son más rápidos, aunque, no son necesariamente tan seguros. Ciertos tipos de ataques pueden afectarlos.
- Los sistemas de clave privada son más lentos, aunque más seguros, los algoritmos más complejos y difíciles de interpretar para otros sujetos que los no autorizados

Un ejemplo del modo de operación según Numerentur.org (2018) es CFB:

El modo CFB (Cipher Feedback Mode) utiliza la retroalimentación de segmentos de texto cifrado en los bloques de entrada para el cifrado y así generar segmentos de salida a los que se le aplica un XOR con el texto claro para producir el cifrado y viceversa. El modo CFB requiere un Vector de Inicialización (VI) como bloque de entrada inicial que no necesita ser secreto, pero debe ser aleatorio. Ver Figura 4-2.

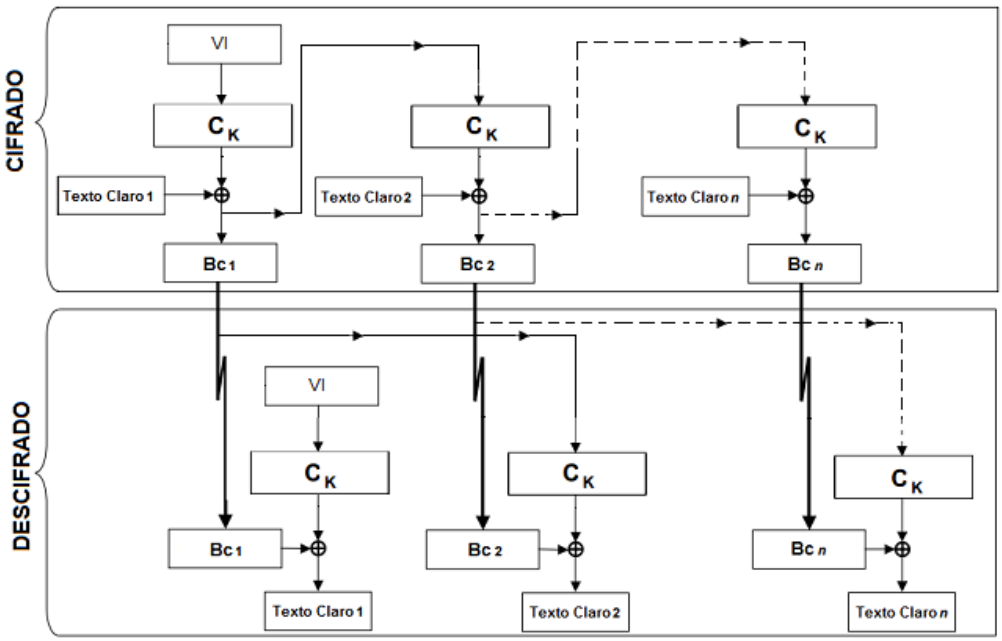


Figura 4-2: Sistema de cifrado y descifrado

Fuente: (Numerentur.org 2018).

Este modo requiere un parámetro entero, denotado L, tal que $1 \leq L \leq n$ corresponde a la longitud en bits que tiene cada segmento de texto cifrado. El valor de L a veces se incorpora al nombre del modo, por ejemplo, CFB-1 bit, CFB-8 bits (Numerentur.org 2018).

Los pasos de operación propuesto por Numerentur.org (2018) son:

1. El primer bloque de entrada es el IV.
2. Se toma el bloque y se cifra.
3. Del cifrado se toma los L bits más significativos, tenemos L_1.
4. Con L_1 y L bits del texto en claro se realiza un XOR, con ello ya se tiene el bloque terminado.
5. Los bits menos significativos $(n - L)$ del cifrado se concatenan o con los L bits del bloque terminado para formar el siguiente bloque de entrada.
6. El bloque terminado es la entrada de la siguiente iteración.

Debido a que en la criptografía asimétrica se utilizan problemas matemáticos difíciles de resolver, se ha optado por elegir la criptografía de clave simétrica, ya que se va a utilizar una clave privada que va a ser la misma para las dos partes.

2.3 Caos

Varios autores, puesto a que no hay una definición ampliamente aceptada del caos, desde sus puntos de vista prácticos lo describen como:

Ribero Medina y Ramirez Gómez (1992) Proponen la manera en que un fenómeno presenta fluctuaciones en el tiempo es a menudo descrita por una ecuación diferencial. Por ejemplo, cuando una observación de un fenómeno en el periodo n+1 es una función de la observación del período n, que se puede expresar en general en la Ecuación (5)

$$X(n+1) = F[X(n)] \qquad (5)$$

Donde $F[X]$ sea una ecuación diferencial no lineal y de primer orden.

Gracias a la primitiva computadora del meteorólogo E.N. Lorenz, pudo calcular la evolución generada por un sencillo sistema de tres ecuaciones diferenciales no lineales, mostrando que tal evolución corresponde a un comportamiento irregular y aperiódico, que luego pasó a denominarse caótico (Lombardi 2020).

Desde el punto de vista matemático, se trata de ecuaciones diferenciales ordinarias, esto quiere decir que, poseen una única variable independiente que cumplen las condiciones necesarias para asegurar la existencia y la unicidad de sus soluciones para cada conjunto de valores de las variables dependientes (Lombardi 2020).

También el mismo autor da una definición desde un punto de vista físico, el cual dice que la variable independiente representa el tiempo, las variables dependientes (variables de estado) figuran las magnitudes físicas que definen el estado del sistema, y cada solución describe la evolución temporal del mismo dadas las condiciones iniciales (Lombardi 2020).

2.3.1 *Sincronización caótica*

Los atractores extraños están presentes en los sistemas caóticos, un ejemplo de atractor extraño llamado Chúa lo presenta Zaqueros-Martínez et al. (2020) , se muestra en la Figura 5-2:

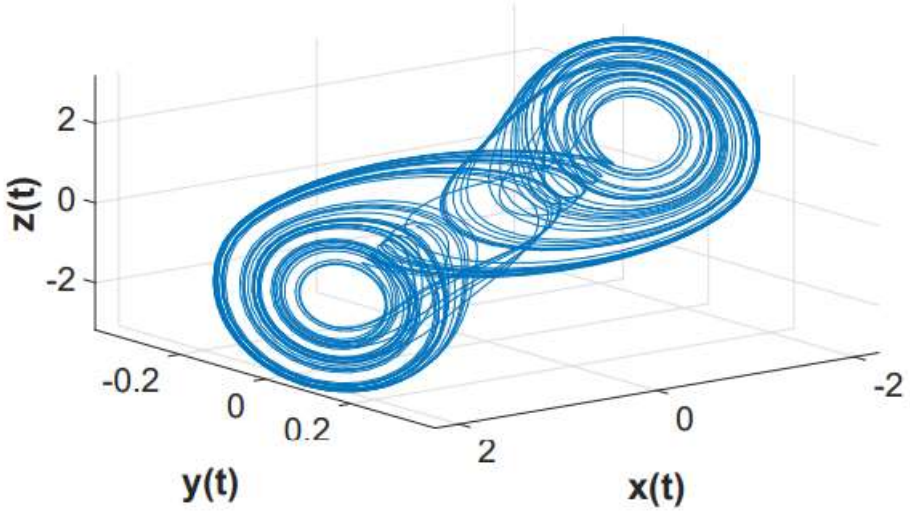


Figura 5-2: Atractor extraño del sistema caótico de Chúa

Fuente: (Zaqueros-Martínez et al. 2020).

La sincronización caótica consiste en hacer coincidir y converger en la misma trayectoria varios sistemas caóticos después de un tiempo suficiente. La idea general de la sincronización caótica utilizada en comunicaciones seguras es la siguiente. Primero, el transmisor cifra la información mediante un sistema caótico. Después, la información cifrada es enviada a través de un canal para ser recibida por el receptor. Finalmente, el receptor utiliza la sincronización para recuperar el mensaje original de la información cifrada (Zaqueros-Martínez et al. 2020).

La sincronización entre dos sistemas se consigue cuando uno de ellos cambia su trayectoria, bien hacia la seguida por el otro sistema o bien hacia una nueva trayectoria común a ambos. De manera genérica puede ser definida como una conformidad en el tiempo de dos o más procesos caóticos, caracterizada por unas métricas entre algunas variables de estos procesos. El fenómeno de sincronización también puede ser visto como una manifestación de la tendencia a la autoorganización en sistemas complejo (Santos y Garcés 2006).

Al vincular los sistemas caóticos con la criptografía se tiene criptosistemas caóticos de diversos tipos: Según Arias (2022) el tratamiento del mensaje se dividen en:

- Cifrado en bloque 64-128 bits
- Cifrado en flujo cifrado bit a bit

Según el tipo de claves se dividen en:

- Cifrado con clave secreta o simétrico

- Cifrado con clave pública asimétrico

Caos se puede utilizar para crear cifrados, generadores de números pseudoaleatorios, firmas digitales simples y oscuras, funciones hash unidireccionales, protocolos ZK, etc.

2.3.2 *Características principales que cumplen los sistemas caóticos*

El autor Asociación Nacional de Estudiantes Universitarios de Ciencias Físicas (2018) menciona las siguientes características:

- **No linealidad:** Un cambio no lineal es aquel que no se basa en una simple relación proporcional entre causa y efecto. Por lo tanto, cuando se usa para referirse a cambios, estos suelen ser bruscos, inesperados y difíciles de prever.

- **Extrema sensibilidad que poseen ante cambios muy pequeños de sus condiciones iniciales:** Existe caos cuando en un sistema dos sucesos que empiezan en condiciones iniciales muy próximas evolucionan de manera diferente, que se separan exponencialmente en el espacio de las fases. Así, se puede decir que se pierde la memoria de las condiciones iniciales de que se partía (Borondo 2022).

- **No se puede prever el comportamiento del sistema hasta que el proceso sucede o se calcula:** Las condiciones iniciales generan cambios en la gráfica, ya que si se ingresan constantemente valores va a cambiar todo el tiempo.

Otro autor Gómez et al. (2022) menciona una configuración simple para una sincronización completa se basa en el uso de un sistema maestro que actúa como transmisor y un sistema esclavo que actúa como receptor .

El esquema maestro tiene componentes (variables vectoriales) en tres direcciones; sin embargo, una de estas direcciones se utiliza para conectar el maestro y esclavo, esta variable también se conoce como el controlador. Una vez que se complete la sincronización entre estos sistemas, las variables de ambos sistemas mostrarán los mismos valores, lo que permitirá una transferencia de datos segura (Gómez et al. 2022).

2.3.3 *Atractores*

La ciencia sostiene que existe una capacidad espontánea de las cosas para organizarse, la cual sería una propiedad inherente de los sistemas complejos y dinámicos; es decir, de aquellos que poseen múltiples componentes, variadas maneras de relacionarse entre ellos y trayectorias posibles derivadas de ese movimiento caótico inicial: tarde o temprano habrá coincidencias o choques en el espacio que harán aparecer anomalías, cosas nuevas derivadas de circunstancias impredecibles, pero que constituirán una modificación potencialmente organizadora de un sistema (Baptiste 2018).

El término atractor extraño se usa para describir una región o forma hacia la cual los puntos son llevados como resultado de cierto proceso que muestra una dependencia sensible de las condiciones iniciales (es decir, puntos que inicialmente están cerca del atractor se separa exponencialmente con el tiempo) (Campuzano 2018).

2.3.3.1 *Atractor de Rossler, datos del autor y ecuaciones*

Otto E. Rössler (nacido el 20 de mayo de 1940) es un bioquímico alemán conocido por su trabajo sobre la teoría del caos y la ecuación teórica conocida como el atractor de Rössler. Él es mejor conocido por el público en general por su participación en una demanda fallida para detener al Gran Colisionador de Hadrones debido a los temores de que genere mini agujeros negros Pacheco Cruz (Pacheco Cruz 2019).

El atractor de Rössler es un sistema de tres ecuaciones diferenciales ordinarias no lineales estudiadas por el autor. Estas ecuaciones diferenciales definen un sistema dinámico del tiempo continuo que muestra dinámicas caóticas asociadas con las propiedades fractales del atractor. Algunas propiedades pueden ser deducidas a través de métodos lineales como auto vectores, pero las principales características del sistema requieren métodos no lineales como Aplicaciones de Poincaré o diagramas de bifurcación (Pacheco Cruz 2019).

Se considera al sistema de Rossler mediante las Ecuaciones (6), (7) y (8) (Gómez et al. 2022).

$$\dot{x1} = -y1 - z1 \qquad (6)$$

$$\dot{y1} = x1 + ay1 \qquad (7)$$

$$\dot{z1} = b + z1(x1 - c) \qquad (8)$$

Se sabe que en los parámetros $\begin{Bmatrix} a = 0{,}2 \\ b = 0{,}2 \\ c = 5{,}7 \end{Bmatrix}$ este sistema presenta comportamiento caótico (nótese que solo se cuenta con un término no lineal) (Ibanez 2005).

Considerando $y1$ como el controlador para acoplar el maestro con el esclavo, el esquema esclavo se puede representar mediante las Ecuaciones (9) y (10):

$$\dot{x2} = -y1 - z2 \quad (9)$$

$$\dot{z2} = b + z2(x2 - c) \quad (10)$$

Una imagen referencial de como se ve el atractor de Rossler es la que se muestra en la Figura 6-2:

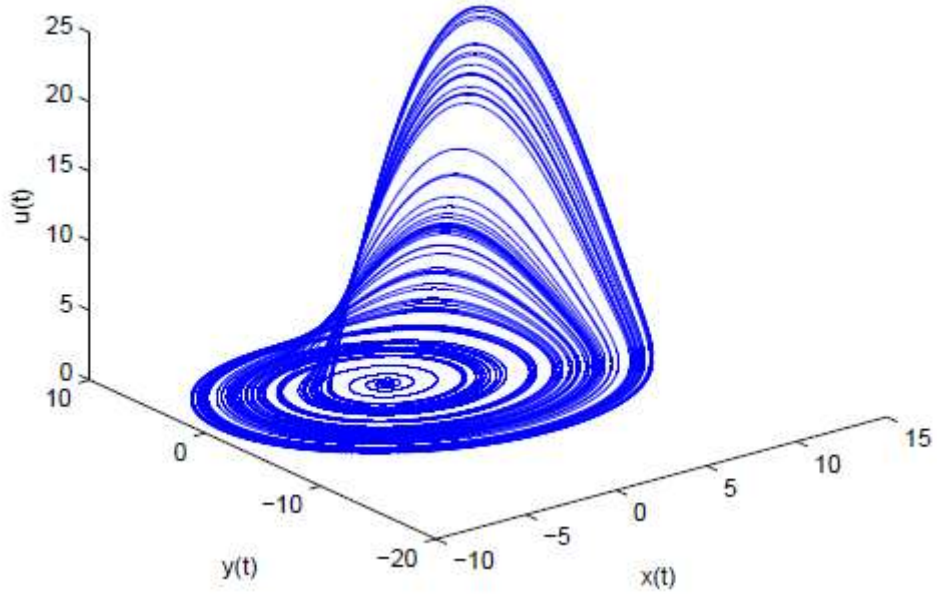


Figura 6-2: Atractor de Rossler

Fuente: (Mohammad 2022).

2.3.3.2 *Atractor de Lorenz, datos del autor y ecuaciones*

El matemático y meteorólogo Edward Lorenz está considerado pionero en la generación de la teoría del caos. Nace en Estados Unidos de Norteamérica en el condado West Hartford, Connecticut, en la segunda década del siglo XX, el 23 de mayo del año 1917 y fallece en Cambridge, Massachusetts mientras trascurría la primera década del siglo XXI, el 16 de abril de 2008. Empezó su carrera profesional como matemático en el Dartmouth College, New Hampshire, seguidamente en la Universidad de Harvard, Cambridge y una vez finalizada la Segunda Guerra Mundial, tras servir en las Fuerzas Armadas de su país como pronosticador del tiempo, se formó en meteorología en el Massachusetts Institute Tecnology (MIT), asumiendo el rol como docente a partir de 1981, labor que fue reconocida a través del otorgamiento de distinguidas premiaciones (Pacheco Cruz 2019).

Lorenz invento el término “el efecto mariposa” para indicar aquellas situaciones en las que una pequeña causa puede multiplicarse de tal modo que acabe produciendo un resultado catastrófico (Pacheco Cruz 2019).

El atractor de Lorenz, es un sistema determinístico tridimensional derivado de las ecuaciones simplificadas de rollos de convección que se producen en las ecuaciones dinámicas de la atmósfera terrestre (Pacheco Cruz 2019).

En el caso del sistema de Lorenz, el esquema maestro está representado por las Ecuaciones diferenciales ordinarias no lineales (11), (12) y (13) (Gómez et al. 2022).

$$\dot{x1} = \sigma(y1 - x1) \quad (11)$$

$$\dot{y1} = -x1z1 + \rho x1 - y1 \quad (12)$$

$$\dot{z1} = x1y1 - \beta z1 \quad (13)$$

donde $x1, y1, z1$ son las condiciones iniciales, y $\begin{Bmatrix} \sigma = 10 \\ \rho = 28 \\ \beta = 2{,}7 \end{Bmatrix}$ son los parámetros del sistema. Considerando $y1$ como el controlador para acoplar el maestro con el esclavo, el esquema esclavo se representa mediante las Ecuaciones diferenciales ordinarias no lineales (14) y (15):

$$\dot{x2} = -x2z2 + \rho x2 - y1 \quad (14)$$

$$\dot{z2} = x2y1 - \beta z2 \quad (15)$$

Tenga en cuenta que la variable $x1$ es la misma en ambos esquemas, el maestro y el esclavo; es decir, la variable x se reemplaza en el esclavo.

Una imagen referencial del sistema de Lorenz es la que se muestra en la Figura 7-2:

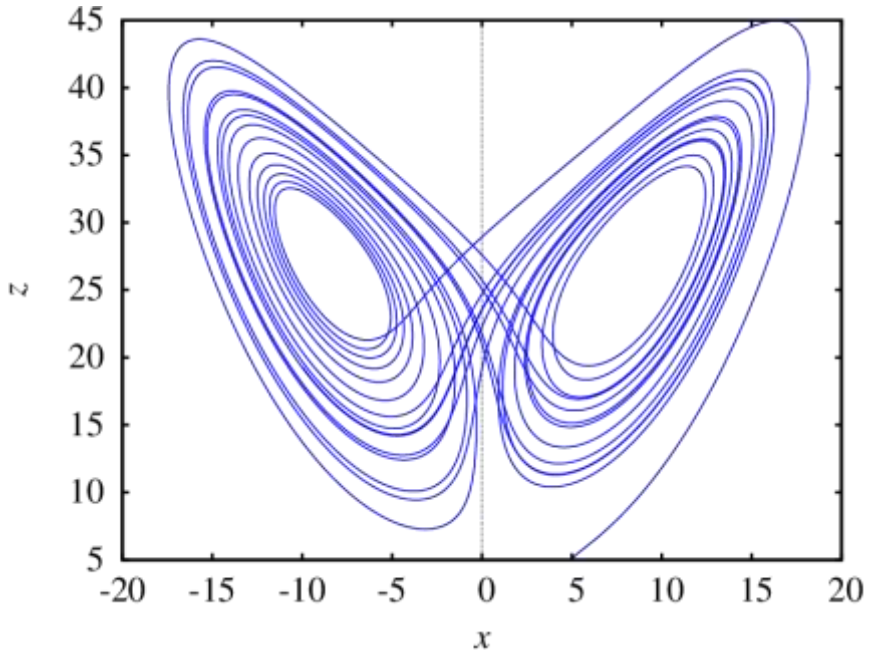


Figura 7-2: Atractor de Lorenz

Fuente: (Villate 2022).

2.3.3.3 *Atractor de Chen, datos sobre el autor y ecuaciones*

El Prof. Chen recibió el M.Sc. Licenciado en matemáticas computacionales de la Universidad Sun Yat-sen (Zhongshan), China en 1981, y Ph.D. Licenciado en matemáticas aplicadas de la Universidad de Texas A&M, EE. UU. en 1987. Trabajó en la Universidad de Rice como profesor asistente visitante en 1987-1990, en la Universidad de Houston hasta convertirse en profesor titular en 1990-1999, y luego en City University of Hong Kong como catedrático y director fundador del Center for Chaos and Complex Networks desde el año 2000 (City University of Hong Kong. 2023).

El profesor Chen fue elegido miembro del IEEE en 1997 por sus contribuciones fundamentales a la teoría y las aplicaciones del control del caos y el análisis de bifurcaciones, y se convirtió en miembro vitalicio en 2019 (City University of Hong Kong. 2023).

En 1999, Chen y Ueta encontraron un atractor caótico similar pero no equivalente, que puede considerarse dual al atractor de Lorenz en el sentido de que el atractor de Lorenz satisface la condición $a_{12}\, a_{21} > 0$ formulada por Vaněček y Čelikovský mientras que el atractor de Chen satisface un $a_{12}\, a_{21} < 0$, donde $a_{12}\, y\, a_{21}$ son los elementos correspondientes en la matriz constante $A = \left[a_{ij}\right]_{3x3}$ para la parte lineal del sistema. Muy recientemente, Lü et al. encontraron

un nuevo sistema caótico, que satisface la condición $a_{12}\ a_{21} = 0$, cerrando así la brecha entre los atractores de Lorenz y Chen (Lü, Chen y Zhang 2002).

Es un nuevo atractor caótico en un sistema autónomo tridimensional simple, que se asemeja a algunas características familiares de los atractores de Lorenz y Rossler (Chen y Ueta 1999).

Este sistema representado por las Ecuaciones (16), (17) y (18)

$$\dot{x} = a(y - x) \qquad (16)$$

$$\dot{y} = (c - a)x - xz + cy \qquad (17)$$

$$\dot{z} = xy - bz \qquad (18)$$

donde x, y, z son las condiciones iniciales del sistema y $\begin{Bmatrix} a = 35 \\ b = 3 \\ c = 28 \end{Bmatrix}$ son los parámetros del sistema.

Cuando los parámetros son $a = 35, b = 3\ y\ c = 28$ y las condiciones iniciales es $x(0) = -10, y(0) = 0,\ z(0) = 37$ el atractor es caótico y se observa su gráfica en la Figura 8-2 (Al-Azzawi y Abed 2011).

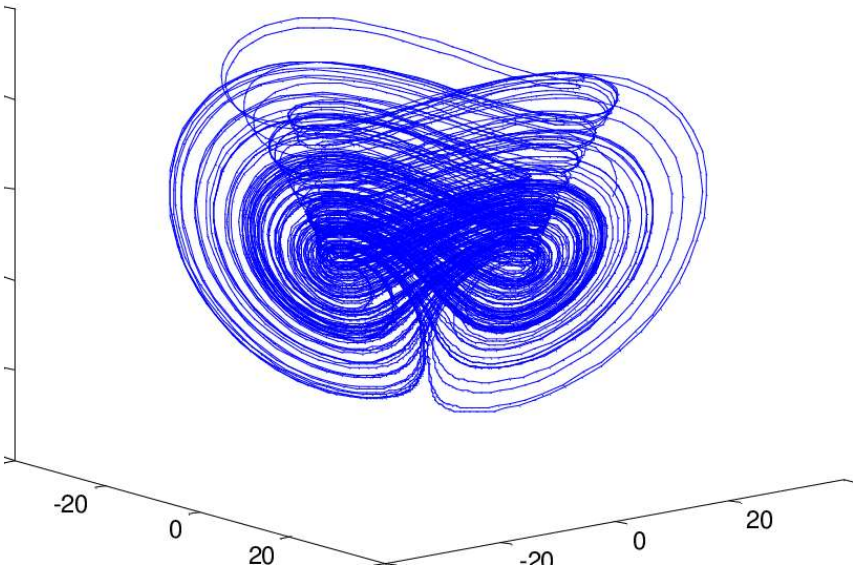


Figura 8-2: Atractor de Chen

Fuente: (Al-Azzawi y Abed 2011).

2.3.3.4 *Atractor de Sprott, datos del autor y ecuaciones*

Clint Sprott nació el 16 de septiembre de 1942 en Menfis, Tennessee. Obtuvo su licenciatura del MIT en 1964 y su Ph.D. en física de la Universidad de Wisconsin-Madison en 1969. Sus intereses profesionales son la física experimental del plasma y la teoría del caos (Sprott 2010).

A finales del siglo pasado J. C. Sprott, introdujo una ecuación que producía caos en ciertos valores de parámetros, una característica importante de esta ecuación era la siguiente: Era una ecuación diferencial de tercer orden, que podría llevarse a tres de primer orden. Sprott construyó una serie de ecuaciones, que desde un punto de vista matemático eran muy sencillas, pero sus soluciones muestran estructuras muy complejas (Paredes 2023).

Según Lai y Chen (2016) En una búsqueda numérica de sistemas caóticos que no tienen puntos de equilibrio y solo órbitas limitadas para todas las condiciones iniciales, las Ecuaciones (19), (20) y (21).

$$\dot{x} = a(y - x) \qquad (19)$$

$$\dot{y} = bxz \qquad (20)$$

$$\dot{z} = c - xy \qquad (21)$$

Con sus parámetros correspondientes a $\begin{Bmatrix} a = 5 \\ b = 2 \\ c = 1{,}6 \end{Bmatrix}$

Es obvio que el sistema tiene ecuaciones simples con tres términos lineales y dos términos no lineales. Se considera que el término no lineal es la causa principal del caos en este (Lai y Chen 2016).

Presenta dos equilibrios simétricos $O_1(\sqrt{c},\ \sqrt{c},\ 0)$ y $O_2(-\sqrt{c}, -\sqrt{c}, 0)$ Se puede verificar fácilmente que ambos equilibrios son inestables si los parámetros a, b, c son todos positivos.

Una imagen referencial del sistema de Sprott de la primera solución es la que se muestra en la Figura 9-2:

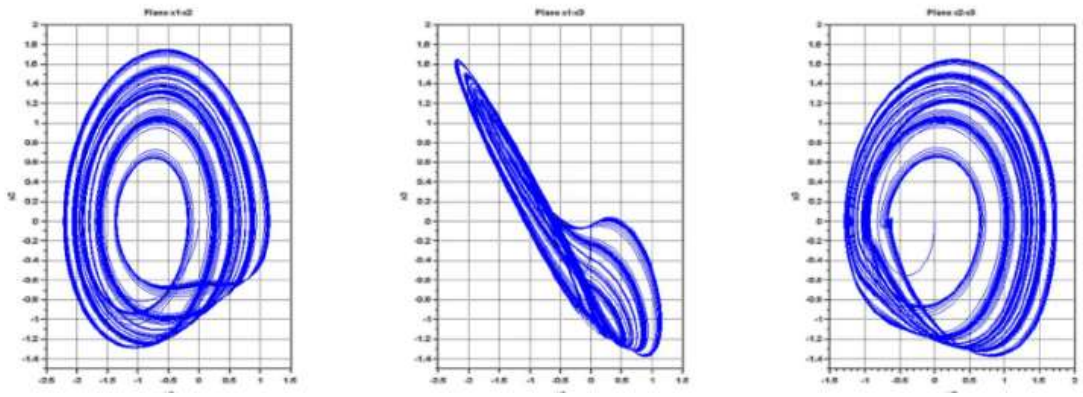


Figura 9-2: Atractor de Sprott a), en planos x1-x2, x1-x3 y x2-x3

Fuente: (Rodríguez Cruz, Rendón y Rodriguez-Liñan 2023).

2.3.4 *Cuadro resumen de los atractores caóticos*

En la Tabla 1-2 se muestra un resumen de los atractores con sus fórmulas y parámetros.

Tabla 1-2: Tabla resumen de los atractores.

Atractor	Ecuaciones	Parámetros
Rossler	$\dot{x1} = -y1 - z1$ $\dot{y1} = x1 + ay1$ $\dot{z1} = b + z1(x1 - c)$	$\begin{Bmatrix} a = 0{,}2 \\ b = 0{,}2 \\ c = 5{,}7 \end{Bmatrix}$
Lorenz	$\dot{x1} = \sigma(y1 - x1)$ $\dot{y1} = -x1z1 + \rho x1 - y1$ $\dot{z1} = x1y1 - \beta z1$	$\begin{Bmatrix} \sigma = 10 \\ \rho = 28 \\ \beta = 2{,}7 \end{Bmatrix}$
Chen	$\dot{x} = a(y - x)$ $\dot{y} = (c - a)x - xz + cy$ $\dot{z} = xy - bz$	$\begin{Bmatrix} a = 35 \\ b = 3 \\ c = 28 \end{Bmatrix}$
Sprott	$\dot{x} = a(y - x)$ $\dot{y} = bxz$ $\dot{z} = c - xy$	$\begin{Bmatrix} a = 5 \\ b = 2 \\ c = 1{,}6 \end{Bmatrix}$

Realizado por: Jemmy Puzma, 2023.

2.4 Metodologías ágiles

Las metodologías ágiles son una manera de trabajar rápida, eficaz y flexible. Su objetivo es desarrollar productos y servicios de calidad adaptados a las necesidades de unos clientes y a las preferencias de un mercado que cambian a un ritmo vertiginoso (Universidad Europea 2021).

Según Universidad Europea (2021) sus principales características son:

- La cooperación entre equipos multidisciplinares y autogestionados.
- Una alta implicación de los usuarios o clientes.
- Una comunicación fluida.
- Unas revisiones constantes gracias a la realización de entregas regulares y en plazos cortos (sprints) a lo largo del proyecto.
- La posibilidad de medir el progreso.
- La adaptación a los cambios que vayan surgiendo sobre la marcha.

Algunas metodologías ágiles más destacadas según Sotomayor (2021) son:

- Extreme Programming XP
- SCRUM
- Kanban
- Agile Inception
- Design Sprint, la metodología de Google

2.4.1 *SCRUM*

Scrum es un modelo que organiza a las personas en equipos pequeños, interdisciplinarios y autoorganizados, divide el trabajo en una lista de entregables pequeños y concretos, llamados sprint e incrementos, asigna a cada actividad de la lista un orden de prioridad que se determina en colaboración con el cliente, en base a la revisión realizada de un entregable después de cada iteración y además estima el esfuerzo relativo que tiene cada actividad (Kniberg y Skarin 2010).

Los roles más importantes de Scrum son: Product Owner (Propietario del producto), Scrum Master (facilitador) y Team (equipo de desarrollo), además divide el tiempo en iteraciones cortas de longitud fija (generalmente de 1 a 4 semanas) con código potencialmente entregable y presentado después de cada iteración. Optimiza el plan de entregas y optimiza la colaboración con el cliente basándose en conocimientos adquiridos mediante la inspección del entregable y optimiza el proceso teniendo una retrospectiva después de cada iteración (Kniberg y Skarin 2010).

Las fases de la metodología ágil SCRUM se muestran en la Figura 10-2:

Figura 10-2: Fases de la metodología SCRUM

Fuente: (GITNUX 2023).

El autor Gitnux (2023) Describe las fases de la siguiente manera:

- **Planificación del Sprint o Sprint Planning**

Es el primer paso de este método y es el más importante para poder definir cómo se va a realizar el trabajo. En esta etapa, en efecto, se asignan las tareas a cada miembro del team y se definen los plazos de entrega.

- **Encuentro con el equipo de Scrum o Scrum Team Meeting**

Se trata de breves reuniones que se realizan una vez al día para hablar de las tareas que se han o se están desarrollando, encontrar los posibles problemas y resolverlos.

- **Refinamiento del Backlog o Backlog refinement**

El Backlog es una lista de trabajo realizada en orden de prioridad para el equipo. En esta fase se hace un repaso y un refinamiento de las tareas de cada uno.

- **Revisión del Sprint o Sprint Review**

Esta es la fase de análisis y evaluación de los resultados obtenidos. Se organiza una reunión, en la cual suele participar el cliente también, y todos los miembros colaboran entre sí para establecer si hay algo para modificar.

- **Retroalimentación o Retrospective**

Es la última etapa de la metodología. Se trata de una reunión final en la que se analizan todos los aspectos del proyecto. Desde el principio hasta el final. En esta fase, el objetivo es adquirir todos los conocimientos necesarios para no cometer los mismos errores en los proyectos futuros.

Los roles de esta metodología se muestran en la Tabla 2-2

Tabla 2-2: Roles de la metodología SCRUM

ROLES	DESCRIPCIÓN
Product Owner	Responsable de representar al resto de stakeholders en el desarrollo de un producto o proyecto, comunicando la visión del producto a construir al equipo de desarrollo, y aportando una perspectiva de negocio.
Scrum Máster	Es responsable de garantizar que todo el equipo comprenda y aplique el proceso Scrum. Es el facilitador y guardián del equipo, ya que debe despejar los obstáculos e interrupciones que ocurren durante cada sprint para alcanzar sus objetivos.
Developer Team	En cada iteración, el equipo es responsable de transformar la acumulación de productos en una mayor funcionalidad del producto mediante la planificación de su propio trabajo para lograrlo. Cada miembro tiene que asignar tareas y cumplir con los plazos y la calidad acordada.

Realizado por: Jemmy Puzma, 2023

2.4.2 *Kanban*

El tablero Kanban proporciona visibilidad del proceso del software, en él muestra el trabajo asignado dividido en bloques para cada desarrollador, comunica claramente las prioridades y resalta los cuellos de botella, así el equipo se concentra en resolver los problemas que bloquean el proceso y restauran el flujo productivo. Además, limita el WIP (Work in progress, trabajo en curso) asignando limites concretos que pueden estar en el progreso en cada estado del flujo del

trabajo y mide el tiempo medio para completar elementos, optimizando el proceso para que el tiempo sea idóneo para la elaboración del trabajo (Ibarra Guzmán et al. 2014).

Consta de cinco principios básicos, los cuales se muestran en la Figura 11-2:

Figura 11-2: Principios de la metodología Kanban

Fuente: (Roca 2021).

Roca (2021) describe los 5 principios de la metodología Kanban de la siguiente manera:

- **Visualización**

Si hay algo característico en la metodología Kanban es que es completamente visual. Así, debe permitir entender perfectamente en qué momento de desarrollo se encuentra el proyecto, así como permitir el acceso a las tareas en cualquier momento para hacer las modificaciones necesarias.

- **Priorización**

Las tareas pendientes deben colocarse en un orden coherente que facilite el trabajo.

- **Mejora continua**

La metodología Kanban parte de la premisa de que siempre se puede hacer mejor. Por ello, uno de sus principios es el cambio evolutivo, pues considera que si no se modifican los hábitos se acaba perdiendo competitividad en el mercado.

- **Liderazgo en todos los niveles**

Al fin y al cabo, para implementar de forma exitosa la metodología Kanban se requiere la implicación de todos y cada uno de los miembros del equipo, no únicamente de los managers.

- **Calidad garantizada**

La metodología Kanban prioriza por encima de todo la calidad, mucho antes que la rapidez, pues no hay margen de error.

2.4.3 *Scrumban*

Scrumban es un modelo de desarrollo adecuado para proyectos de mantenimiento, así como, donde hay historias de usuarios que cambian con frecuencia.

Team (2015) presenta las principales actividades que se hacen en Scrumban:

1. **Metas u objetivos.** Aquí es donde el equipo define ampliamente sus objetivos. Una meta puede ser un objetivo amplio que el equipo espera lograr haciendo múltiples tareas más pequeñas.
2. **Cola de historias.** Aquí es donde los objetivos se dividen en múltiples historias. En esta etapa se crea una larga lista de historias.
3. **Análisis.** Aquí es donde Scrumban difiere de otros enfoques. Las historias creadas en la etapa anterior ahora se analizan, y algunas seleccionadas son aceptadas para seguir trabajando.
4. **Desarrollo.** Se comienza a trabajar en las historias seleccionadas.
5. **Pruebas.** Una vez que se ha trabajado en las historias, los resultados son probados por los equipos de control de calidad.
6. **Despliegue.** Los resultados se ponen en práctica.
7. **Hecho.** Todas las historias completadas ahora están marcadas como Hecho.

El proceso de Scrumban se muestra en la Figura 12-2:

Figura 12-2: Proceso de Scrumban

Realizado por: Jemmy Puzma, 2023.

2.4.4 *Cuadro comparativo entre las metodologías SCRUM, KANBAN Y SCRUMBAN*

A continuación, se muestra la Tabla 3-2 con algunos aspectos que se ha considerado importante para contrastar.

Tabla 3-2: Cuadro comparativo entre metodologías ágiles

	SCRUM	**KANBAN**	**SCRUMBAN**
Roles	Product Owner, Scrum Máster y Developer Team	No se requieren roles específicos	No se requieren roles específicos
Eventos	No se basa en eventos, ya que una vez que haya empezado el sprint no puede ser detenido.	Si se basa en eventos ya que el trabajo es continuo.	Si se basa en eventos ya que el trabajo es continuo alineado al flujo de trabajo y planificación.
Alcance	Sprint limita el trabajo total	El trabajo en progreso limita el trabajo actual	Limite el trabajo en curso y limite las tareas pendientes opcionales
Reuniones	Planificación de Sprint, clasificaciones diarias, revisiones de Sprint, retrospectivas.	No hay reuniones o pueden evitarse	Planificación bajo demanda
Nuevos elementos en una iteración	No es permitido	Permitido siempre y cuando se respete la cola de tareas	Permitido siempre y cuando se respete la cola de tareas

Realizado por: Jemmy Puzma, 2023

Una vez realizada la comparación entre las metodologías ágiles se ha optado por SCRUMBAN por que combina los beneficios de SCRUM y KANBAN, además esta metodología no requiere roles específicos, se basa en eventos como en las demás, pero aquí estos van alineados a la planificación, permite visualizar el alcance con las tareas pendientes y terminadas. Cumple con lo que se necesita para desarrollar una aplicación web para el cifrado y descifrado de una cadena de texto mediante sincronización caótica.

2.5 Lenguaje de programación

Un lenguaje de programación es un lenguaje formal diseñado para realizar procesos que pueden ser llevados a cabo por máquinas como las computadoras. Pueden usarse para crear programas que controlen el comportamiento físico y lógico de una máquina, para expresar algoritmos con precisión, o como modo de comunicación humana. Está formado por un conjunto de símbolos y reglas sintácticas y semánticas que definen su estructura y el significado de sus elementos y expresiones. Al proceso por el cual se escribe, se prueba, se depura, se compila (de ser necesario) y se mantiene el código fuente de un programa informático se le llama programación (Gervacio Olarte 2018).

Los lenguajes de programación permiten a las computadoras procesar de forma rápida y eficientemente grandes y complejas cantidades de información. Por ejemplo, si a una persona se le da una lista de números aleatorios que van de uno a diez mil y se le pide que los coloque en orden ascendente, es probable que tome una cantidad considerable de tiempo e incluya algunos errores, mientras que si le das la misma instrucción a una computadora utilizando un lenguaje de programación, podrás obtener la respuesta en unos cuantos segundos y sin errores (OpenWebinars 2020).

2.5.1 *Python*

Python es un lenguaje de scripting independiente de plataforma y orientado a objetos, preparado para realizar cualquier tipo de programa, desde aplicaciones Windows a servidores de red o incluso, páginas web. Es un lenguaje interpretado, lo que significa que no se necesita compilar el código fuente para poder ejecutarlo, lo que ofrece ventajas como la rapidez de desarrollo e inconvenientes como una menor velocidad (Alvarez 2003).

El autor Rivas (2021) indica algunas de las ventajas más importantes el por qué elegir este lenguaje, entre ellas son:

- **Variedad de propósito:** Este lenguaje da la posibilidad de crear muchas cosas que van desde páginas webs, pasando por inteligencia artificial o incluso aplicaciones de Data Science.
- **Multiplataforma:** Es compatible con los principales sistemas operativos.
- **Orientado a objetos:** Está orientado a objetos.
- **Multiparadigma:** Esto porque no sólo ofrece programación orientada a objetos, sino que también otros tipos de programación como la estructura, funcional o imperativa.
- **Sintaxis directa:** También cuenta con una sintaxis bastante directa y clara, haciendo que todo código escrito en Python sea fácil de entender.

- **Fácil aprendizaje:** Python es uno de los lenguajes más fáciles de aprender por los principiantes.
- **Librerías:** Posee una enorme capacidad para la utilización de librerías. Estas otorgan una gran cantidad de funcionalidades extras al código.
- **Lenguaje interpretado:** Presenta un desarrollo mucho más eficaz.
- **Alto nivel:** Presenta una mayor facilidad de uso.
- **Software libre y código abierto:** Es de uso gratuito y es libre de utilizarse en cualquier sistema operativo.

2.5.2 *Java*

Java es una plataforma informática de lenguaje de programación creada por Sun Microsystems en 1995. Ha evolucionado desde sus humildes comienzos hasta impulsar una gran parte del mundo digital actual, ya que es una plataforma fiable en la que se crean muchos servicios y aplicaciones. Los nuevos e innovadores productos y servicios digitales diseñados para el futuro también siguen basándose en este lenguaje (Java 2023).

Según 3digits (2019) las ventajas principales de utilizar java son:

- **Multiplataforma**

Java funciona en cualquier sistema operativo, lo que hace sencillo trasladar las aplicaciones a cualquier plataforma. Esto otorga escalabilidad, ya que permite ejecutar las aplicaciones en sistemas más robustos a medida que es necesario.

- **Orientación a objetos**

Lo que permite crear aplicaciones modulares y código reutilizable.

- **Código robusto**

Java es un lenguaje robusto (fiable). Java pone mucho énfasis en la comprobación temprana de todos los posibles errores y excepciones. Como parte del manejo de excepciones en Java, el compilador puede llegar a confirmar todas las posibilidades en situaciones de tiempo de ejecución, lo que da mucha fiabilidad a los clientes.

- **Open Source**

Java es Open Source. Esto significa que encontrarás una enorme cantidad de funcionalidades provistas por la propia plataforma, pero, además, encontrarás también multitud de código de terceros listo para ser usado.

- **Uso y gestión de la memoria**

Aunque los usuarios no están obligados a gestionar manualmente los problemas de memoria, pueden hacerlo si lo desean. Java realiza la gestión de la memoria de forma automática, utilizando un modo de gestión de memoria automatizado llamado recolector de basura o garbage collector.

2.5.3 *C#*

C# es un lenguaje de programación orientado a componentes, orientado a objetos. C# proporciona construcciones de lenguaje para admitir directamente estos conceptos, por lo que se trata de un lenguaje natural en el que crear y usar componentes de software. Desde su origen, C# ha agregado características para admitir nuevas cargas de trabajo y prácticas de diseño de software emergentes. En el fondo, C# es un lenguaje orientado a objetos. Defina los tipos y su comportamiento (BillWagner 2023).

Lenguajesdeprogramación (2023) menciona algunas ventajas principales de utilizar C# son:

- **Multiplataforma.** Actualmente, el lenguaje C# es de código abierto y se ha utilizado en otros IDEs, como el proyecto Mono o Xamarin, y en múltiples sistemas operativos, como puede ser OSx o Android.
- **Integración con otros lenguajes.** Cualquier lenguaje que se compile con .NET, como la nueva versión de visual basic, puede aprovecharse para usar en tu proyecto.
- **Mejora en la gestión de memoria.** Al igual que Java, en C# dispone de un recolector de basura que destruye los objetos que no se usan en memoria.
- **Tratamiento de errores.** Cualquier lenguaje de programación moderno utiliza las excepciones para controlar los posibles errores en el código.
- **Multihilo.** Puedes dividir tu código en múltiples hilos de ejecución, trabajar en paralelo y sincronizándose al final.

2.5.4 *Comparación entre los lenguajes de programación.*

En la Tabla 4-2 se muestra una comparación entre los lenguajes de programación.

Tabla 4-2: Tabla comparativa de los lenguajes de programación

Características	Python	Java	C#
Tipado de datos	Dinámico	Estático	Estático
Paradigma	Orientado a objetos, Imperativo, Funcional	Orientado a objetos	Orientado a objetos, Imperativo
Uso común	Ciencia de datos, inteligencia artificial, automatización, scripting	Aplicaciones de escritorio, aplicaciones web, juegos	Aplicaciones de escritorio, aplicaciones web, videojuegos,

			desarrollo de aplicaciones móviles
Popularidad	Muy popular	Muy popular	Popular
Comunidad	Muy activa	Muy activa	Activa
Curva de aprendizaje	Baja	Media	Media

Realizado por: Jemmy Puzma, 2023.

Una vez analizado los diferentes lenguajes de programación se ha optado por Python, ya que es dinámico, orientado a objetos, imperativo, funcional y se utiliza mayormente en ciencia de datos, inteligencia artificial, scripting. Para el desarrollo de la aplicación web de cifrado y descifrado mediante sincronización caótica se necesita de un lenguaje que permita utilizar librerías para graficar los atractores y tener una mejor visualización de la sincronización, en general que cumpla con las características mencionadas anteriormente.

2.6 Gestor de base de datos

Un Sistema Gestor de Base de Datos (SGBD) o DataBase Managenent System (DBMS) es un sistema que permite la creación, gestión y administración de bases de datos, así como la elección y manejo de las estructuras necesarias para el almacenamiento y búsqueda de información del modo más eficiente posible (INESEM 2019).

2.6.1 *MySQL*

En el gestor de base de datos se optó por MySQL, basándose en lo que manifiesta el autor Bytes (2020) las principales cualidades son:

- Es de distribución gratuita vía Internet.
- Es de código abierto, es decir, cualquier programador puede modificar su código.
- Permite crear cualquier tipo de aplicación.
- Posee privilegios de alta seguridad.
- Capaz de manejar gran volumen de datos.
- Permite la realización de consultas, las cuales son respondidas rápidamente.
- Tiene alta capacidad de soporte técnico.
- Para su funcionamiento, no es necesaria una gran cantidad de recursos, lo que se traduce en bajo costo.
- Su estructura implica capas y módulos, lo que le da alta estabilidad.
- El proceso de importación y exportación de datos es bastante sencillo.

2.6.2 *PostgreSQL*

A grandes rasgos, PostgreSQL es un gestor que trabaja con bases de datos relacionales y que está orientado a objetos. Se trata de un programa de código abierto u open source, es decir, no está bajo el control de ninguna compañía particular, sino que cuenta con una comunidad de desarrolladores que trabajan en mejorar el programa de forma desinteresada (Ayudaley 2023).

El autor menciona algunas ventajas principales por las que recomienda el uso de PostgreSQL:

- Su instalación y uso es gratis
- Disponibilidad multiplataforma
- Fácil configuración
- Gran cantidad de opciones avanzadas
- Funciona con el estándar SQL
- Sistema de alta fiabilidad y robustez
- Control de concurrencias multiversión (MVCC)
- Hot-Standby
- Query Tool
- Entradas relacionadas

2.6.3 *SQLite*

SQLite es una de las bases de datos relacionales más conocidas. Básicamente, funciona como un servidor propio e independiente, ya que el Sistema de Gerencia de Base de Datos o SGBD, se puede ejecutar en la misma instancia, eliminando así las consultas y procesos separados. Por lo tanto, la biblioteca SQLite se genera y almacena directamente en el archivo de la base de datos (HostGator 2023).

HostGator (2023) menciona que al resultar más práctico y accesible, es recomendable para:

- Aplicaciones desktop o mobile más sencillas (sin mucha funcionalidad y consumo de datos)
- Sitios más ligeros y con pocos recursos (con páginas estáticas, por ejemplo)
- Sitios o sistemas que aún no cuentan con muchos usuarios (el acceso diario promedio ronda los 100 mil)

El autor HostGator (2023) menciona algunas principales ventajas las cuales son:

- Es estable, multiplataforma y compatible con versiones anteriores.
- Su código es de dominio público y gratuito.
- No requiere instalación o configuración.

- Guarda la base de datos en un solo archivo.

2.6.4 *Comparación entre gestores de bases de datos*

En la Tabla 5-2 se muestra una comparación de los gestores de bases de datos:

Tabla 5-2: Tabla comparativa entre sistemas de gestores de bases de datos.

Característica	MySQL	PostgreSQL	SQLite
Tipo de base de datos	Relacional	Relacional	Relacional
Licencia	Open Source (GPL)	Open Source (MIT)	Dominio público
Lenguaje de consulta	SQL	SQL	SQL
Transacciones ACID	Sí	Sí	Sí
Soporte de claves foráneas	Sí	Sí	Sí
Disparadores (Triggers)	Sí	Sí	Sí
Procedimientos almacenados	Sí	Sí	Sí
Vistas	Sí	Sí	Sí
Replicación	Sí	Sí	No nativo, pero se puede lograr mediante extensiones
Escalabilidad	Escala bien en la mayoría de los casos	Escala bien en aplicaciones complejas	Limitado por su diseño, adecuado para aplicaciones pequeñas y medianas. No necesita servidor.
Compatibilidad con plataformas	Multiplataforma	Multiplataforma	Multiplataforma
Herramientas de administración	MySQL Workbench, phpMyAdmin, etc.	pgAdmin, psql, etc.	SQLite Manager, DBeaver, etc.
Soporte de almacenamiento JSON	Sí	Sí (con funciones JSON)	Sí (con funciones JSON1)
Soporte de lenguajes de programación	Amplio soporte	Amplio soporte	Soporte limitado a través de bibliotecas externas
Capacidad de almacenamiento	Máximo de 256 terabytes	Máximo de 32 terabytes	Máximo de 140 terabytes

Extensibilidad	Mediante motores de almacenamiento	Mediante extensiones	Limitado a extensiones C
Comunidad y soporte	Gran comunidad y soporte	Gran comunidad y soporte	Comunidad y soporte más pequeños
Casos de uso típicos	Aplicaciones web, sitios de comercio electrónico	Aplicaciones empresariales, análisis de datos	Aplicaciones móviles, pequeñas aplicaciones, menos ancho de banda.

Realizado por: Jemmy Puzma, 2023.

Una vez analizado los sistemas de gestores de bases de datos se ha optado por SQLite, ya que es relacional y presenta características similares a las demás, pero lo que se necesita para el desarrollo de la aplicación es una base de datos que permita almacenar datos en pequeña cantidad y que consuman menos ancho de banda, es independiente, lo que significa que no necesita un servidor.

2.7 Framework Flask

Flask es un "micro" Framework escrito en Python y desarrollado para simplificar y hacer más fácil la creación de Aplicaciones Web bajo el patrón MVC (Agency 2021).

La palabra "micro" no quiere decir que se trate de un proyecto pequeño o que sirva para hacer páginas web pequeñas, al instalar Flask se dispone de las herramientas necesarias para crear una aplicación web funcional. Es probable que en algún momento se necesite una nueva funcionalidad que no se tiene de primeras con la instalación, para eso encontrarás un gran conjunto de extensiones (plugins) que se pueden instalar fácilmente con Flask y que permitirán añadirle todas las funcionalidades que sea necesario (Agency 2021).

En cuanto al patrón MVC, este es una forma de trabajar que permite diferenciar y separar lo que es la vista (página HTML), el modelo de datos (los datos que va a tener la App), y el controlador (donde se gestionan las peticiones de la app web) (Agency 2021).

2.8 Eficiencia de desempeño

Comportamiento temporal. Los tiempos de respuesta y procesamiento y las ratios de throughput de un sistema cuando lleva a cabo sus funciones bajo condiciones determinadas en relación con un banco de pruebas (benchmark) establecido (ISO 2023).

2.8.1 *Métricas y fórmulas para medir el comportamiento temporal*

Estas métricas permiten medir los tiempos en que un software tarda en realizar una determinada actividad, desde que se inicia hasta que termina, incluyendo tiempos de prueba y operaciones (Llamuca-Quinaloa, Vera-Vincent y Tapia-Cerda 2021).

Las métricas que se utilizan para evaluar el comportamiento en el tiempo son:

- **Tiempo de sincronización:** Se refiere al tiempo que transcurre desde que se recibe una solicitud antes de que se resuelvan las ecuaciones.
- **Tiempo de cifrado:** Es la duración entre iniciar la sincronización hasta el momento en donde muestra el mensaje cifrado.
- **Tiempo de descifrado:** Se refiere a la duración entre la sincronización hasta el momento en donde se muestra el mensaje original.

En la Tabla 6-2 se muestran las fórmulas de cada métrica.

Tabla 6-2: Métricas y fórmulas del comportamiento en el tiempo.

Métrica	Fórmula	Descripción
Tiempo de sincronización	X=B-A	A= Tiempo de envío de petición antes de resolución de ecuaciones. B= Tiempo en recibir la primera respuesta.
Tiempo de cifrado	X=A-C	A= Tiempo de envío de petición antes de resolución de ecuaciones. C= Tiempo en que se cifra el mensaje.
Tiempo de descifrado	X=A-C	A= Tiempo de envío de petición antes de resolución de ecuaciones. C= Tiempo en que se descifra el mensaje

Fuente: (Llamuca-Quinaloa, Vera-Vincent y Tapia-Cerda 2021).
Realizado por: Jemmy Puzma, 2023.

2.9 Seguridad

2.9.1 *Confidencialidad*

La confidencialidad en seguridad informática es el principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización. Según UNIR (2021) dicha autorización se basa en la necesidad de conocer la información para el desempeño de su actividad laboral o cotidiana y se debe proveer tanto para:

- **La información almacenada:** ya sea digital, almacenada en repositorios, como servidores o física, como documentos en papel.
- **La información en tránsito:** información digital transmitida a través de Internet, transportada en soportes digitales de información, como pendrives, o información física transportada de un lugar a otro.

Para medir la confidencialidad se va a realizar de manera cuantitativamente mediante un coeficiente de correlación, e histogramas, en los cuales se va a graficar los datos de los textos cifrados y sin cifrar.

2.9.2 *Medir confidencialidad mediante coeficiente de correlación*

Para esto se va a utilizar la distribución del texto plano y la del texto después de descifrarlo. Se muestra en el Gráfico 1-2 la distribución de valores.

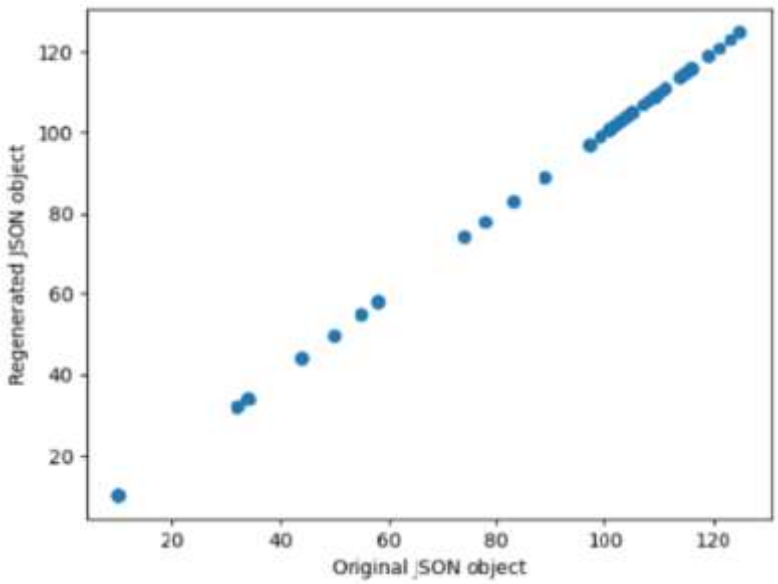


Gráfico 1-2: Gráfico de correlación de un texto plano y un texto regenerado después del descifrado

Fuente: (Gómez et al. 2022).

De igual manera, en el Gráfico 2-2 se muestra la distribución de valores de un texto plano y un texto cifrado.

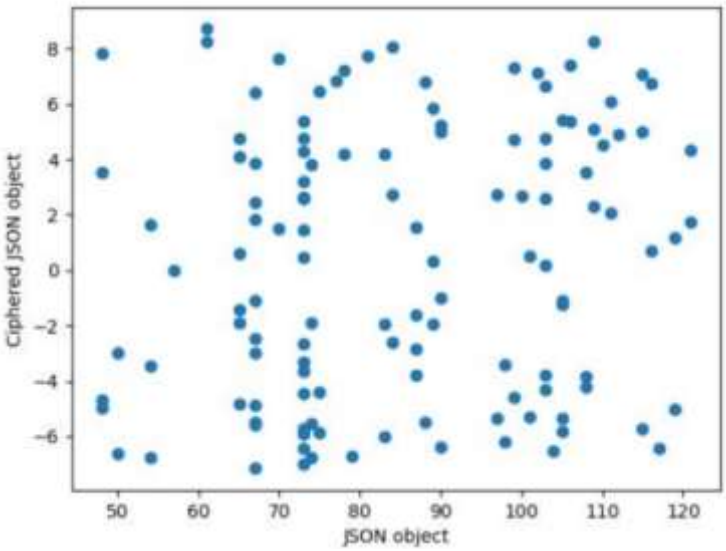


Gráfico 2-2: Gráfico de correlación entre texto sin formato y el cifrado

Fuente: (Gómez et al. 2022).

Se utiliza los gráficos de correlación para determinar el coeficiente de Pearson y realizar el respectivo análisis entre el texto cifrado y sin cifrar.

2.10 Trabajos relacionados

Cordova Ramirez et al. (2020) tuvo como objetivo el desarrollo de un sistema en la cual se propone sistematizar el proceso de la redacción y generación de historiales médicos para reducir el tiempo de firma y aprobación de estos. Se utilizó el sistema RSA (Rivest, Shamir y Adleman) y la función hash SHA-256 para crear una firma digital.

Sheikholeslam (2009) utilizó sistemas dinámicos con atractores caóticos en el cifrado. Se basó en el sistema Encryption Dynamical para generar una clave de sincronización, y conseguir que el descifrado pueda actualizarse a las condiciones iniciales antes de generar el bloque. Como resultado se consiguió realizar una modificación discreta del sistema de Lorenz.

Omar S. Gómez, Raúl H. Rosero, Juan C. Estrada-Gutiérrez, y Maricela Jiménez-Rodríguez (2022) agregó un mecanismo de seguridad a los objetos JSON mediante el uso de sincronización caótica. Y el resultado fue que este enfoque se puede aplicar como JSON Web Encryption (JWE).

Montalván (2019) desarrolló el mecanismo de cifrado basado en el algoritmo criptográfico simétrico AES (MECIB-AES) para comparar la seguridad que brinda este a la información cifrada. Como resultado se obtuvo que la implementación de las modificaciones Mix-Shift, Mix-Key y Move-C ayudó a realizar diferentes pruebas donde se aceptó la hipótesis nula la cual midió la entropía, con un nivel de confiabilidad del 95% y un error del 5%, el análisis de frecuencias presentó

variaciones en cada prueba realizada, la autocorrelación dió como resultado una mayor similitud de secuencias a favor del MECIB-AES, aunque puede tomarse como desventaja que los valores no son grandes por lo cual se consideró viable el algoritmo.

A pesar de que en el trabajo de Gómez et al. Agrega un mecanismo de seguridad a los objetos JSON mediante la sincronización caótica, no utiliza cadenas de texto para observar el cifrado y descifrado de la misma. De igual manera, en los trabajos revisados se utilizan sistemas de cifrado como RSA, SHA-256 y AES sin embargo, ninguno implementa cifrados con sistemas caóticos.

CAPÍTULO III:

3 MARCO METODOLÓGICO

3.1 Introducción

El presente capítulo contiene el tipo de estudio, métodos y las técnicas utilizadas en el desarrollo de una aplicación web para el cifrado y descifrado de cadenas de texto a partir de la selección de un atractor caótico, también la especificación de los requisitos, hipótesis, métricas de evaluación, población, muestra y define la arquitectura Modelo Vista Controlador para elaboración de esta, así como también la metodología SCRUMBAN.

3.2 Tipo de estudio

Este trabajo de integración curricular es de tipo aplicativo, cuantitativa y experimental. La parte aplicativa es debido a que tiene como objetivo abordar y resolver problemas prácticos que existen en determinados ámbitos, como el tecnológico que se utiliza para desarrollar la aplicación web de cifrado y descifrado, cuantitativa porque se necesita medir el tiempo de respuesta y la seguridad de cada texto cifrado basado los atractores caóticos seleccionados, y por último experimental en la parte donde se observa y percibe el comportamiento de cada atractor frente a la encriptación, además de ello para realizar pruebas y determinar si se ha obtenido la sincronización con cada uno de los atractores.

3.2.1 *Métodos y técnicas*

A continuación, se muestra en la Tabla 7-3 los métodos y técnicas utilizados para la elaboración del trabajo de titulación.

Tabla 7-3: Tabla de métodos y técnicas

OBJETIVO	MÉTODO	DESCRIPCIÓN	TÉCNICA	FUENTE
Revisar cuatro sistemas caóticos, para entender las fórmulas de cada atractor.	Analítico	Con el objetivo de estudiar los sistemas caóticos, sus características y fórmulas	• Revisión de Documentos	• Papers • Libros • Tesis
Efectuar la sincronización	Experimentación Observación	Verificar que se haya hecho la	• Pruebas • Observación	• Sistemas caóticos

caótica en cada atractor seleccionado.		sincronización en todos los atractores	• Revisión de documentos • Experimentación	
Desarrollar la aplicación web para el cifrado y descifrado de cadenas de texto mediante sincronización caótica utilizando la metodología SCRUMBAN.	SCRUMBAN	Es una metodología ágil que combina procesos de SCRUM y KANBAN, permite la utilización de tableros para gestionar las tareas.	• Tablero Kanban • Diagrama de casos de uso • Modelo de las vistas de arquitectura	• Revistas • Libros • Tutoriales
Evaluar la eficiencia y seguridad en el cifrado y descifrado de cadenas de texto en la aplicación desarrollada.	Analítico Estadístico	Permite recolectar datos cuantitativos para evaluar las variables de estudio mediante métricas y comprobar que se cumplan los objetivos propuestos	**Eficiencia en el desempeño** • Pruebas • Observación • Revisión de documentos **Seguridad** • Observación • Experimentación	• Aplicación web • Papers en donde evalúan las métricas de las variables. • Datos estadísticos de la aplicación

Realizado por: Jemmy Puzma, 2023.

Análisis: Para estudiar y comprender los sistemas caóticos cómo se comportan en el tiempo al momento de cifrar y descifrar una cadena de texto, también el análisis para evaluar la seguridad de estos.

Experimentación: Para poder verificar si se ha efectuado la sincronización caótica con los cuatro atractores seleccionados, de igual manera se medirá el tiempo que tarda en cifrar y descifrar una cadena de texto.

Observación: Se va a necesitar la observación cuando se esté efectuando la sincronización y se requiera verificar que todo esté correctamente realizado, también para ver la reacción de cada atractor frente a diferentes dimensiones de cadenas de textos que se pretenda cifrar y descifrar.

SCRUMBAN: Se escogió por la flexibilidad que tiene, aparte de que divide el trabajo en entregables pequeños y concretos, optimiza el plan de entregas mediante los tableros Kanban los cuales nos permiten visualizar el flujo de trabajo de una manera muy simple y ver el progreso de cada uno de las tareas y su estado.

3.3 Métodos de evaluación de las variables eficiencia en el desempeño y seguridad

Se va a evaluar, por parte de la eficiencia en el desempeño, el comportamiento temporal y por seguridad, la confidencialidad.

3.3.1 *Métricas para la evaluación del comportamiento en el tiempo*

3.3.1.1 *Valor de las métricas*

En la Tabla 8-3 se muestran las métricas que se utilizan para medir el comportamiento en el tiempo con su porcentaje.

Tabla 8-3: Tabla de métricas para evaluar el comportamiento en el tiempo con sus porcentajes.

Métrica	Porcentaje
Tiempo de sincronización	35 %
Tiempo de cifrado	35 %
Tiempo de descifrado	30 %
Total	100 %

Realizado por: Jemmy Puzma, 2023.

3.3.2 *Métrica para la evaluación de la confidencialidad*

Para medir la confidencialidad se utiliza un coeficiente correlación ya que se necesita determinar que se haya cifrado la cadena de texto, se opera el texto plano con el texto descifrado y cifrado.
En la Tabla 9-3 se muestra como está distribuido las variables para X y Y de los gráficos de correlación.

Tabla 9-3: Tabla de métrica para evaluar la seguridad mediante la confidencialidad por medio del coeficiente de correlación.

X	Y
Texto plano	Texto descifrado
Texto plano	Texto cifrado

Realizado por: Jemmy Puzma, 2023.

3.3.2.1 *Valor de las métricas*

En la Tabla 10-3 se muestran las métricas que se utilizan para medir la confidencialidad mediante el coeficiente de correlación.

Tabla 10-3: Tabla de métricas para evaluar la seguridad

Métrica	Porcentaje
Texto plano	35 %
Texto cifrado	35 %
Texto descifrado	30 %
Total	100 %

Realizado por: Jemmy Puzma, 2023.

3.4 Población y muestra

3.4.1 *Población y muestra de la eficiencia de desempeño*

Con el objetivo de medir la eficiencia de desempeño del sistema web de cifrado se consideró como población el proceso de cifrado y descifrado, el cual por cada atractor incluye:

- Tiempo de sincronización
- Tiempo de cifrado
- Tiempo de descifrado

Teniendo en cuenta los cuatro atractores, se va a escoger un aproximado de 25 muestras por cada uno.

3.4.2 *Planteamiento de la hipótesis*

H0= Los cuatro atractores arrojan valores similares en el comportamiento temporal con respecto al tiempo de sincronización, cifrado y descifrado.

H1= Al menos uno de los cuatro atractores difiere sustancialmente del resto con respecto al tiempo de sincronización, cifrado y descifrado.

3.5 Análisis previo al desarrollo del proyecto

En el **Anexo C** se puede visualizar el análisis económico, fuente de financiamiento, riesgos, recursos hardware y software, que fueron tomados en cuenta para el desarrollo del proyecto.

3.6 Desarrollo de la aplicación aplicando la metodología SCRUMBAN

Según Team (2015) la metodología cuenta con 7 etapas:

3.6.1 *Objetivos*

Desarrollar una aplicación web para cifrar y descifrar cadenas de texto mediante la sincronización caótica utilizando la metodología SCRUMBAN.

3.6.2 *Tareas por hacer*

En esta etapa se realiza una reunión con el equipo de trabajo en donde se definen las nuevas tareas o actividades a realizar, estas tareas pueden ir aumentando con cada reunión.

En la Tabla 11-3 se detallan las tareas por hacer.

Tabla 11-3: Tareas por hacer

Nro	Tareas por hacer
1	Elicitación los requerimientos funcionales y no funcionales.
2	Definir estándar de programación
3	Definir arquitectura del sistema
4	Instalar la librería en Visual Studio Code para graficar en Python, y librerías correspondientes al framework flask
5	Diseñar el esquema de la base de datos en SQLite
6	Diseñar las interfaces de la aplicación
7	Implementar cifrado de mensaje con el Atractor Rossler, Lorenz, Chen y Sprott
8	Implementar descifrado de mensaje con el Atractor Rossler, Lorenz, Chen y Sprott
9	Realizar la conexión con la base de datos
10	Gestionar usuarios registrados.
11	Realizar pruebas de validación (cifrado, descifrado, registro, informes)
12	Desplegar el sistema en un servidor.

Realizado por: Jemmy Puzma, 2023.

3.6.3 *Análisis*

Para la asignación de tareas se utilizó el software TeamHood, la cual, permite a los equipos planificar, organizar y dar seguimiento a los proyectos de manera eficiente.

3.6.3.1 *Equipo de desarrollo.*

Antes de asignar las tareas, se debe agregar los miembros del equipo de desarrollo. Debido a que este trabajo de integración curricular es realizar por un solo estudiante, este deberá cumplir con todos los roles que se le asigne, se observa el equipo en la Figura 13-3.

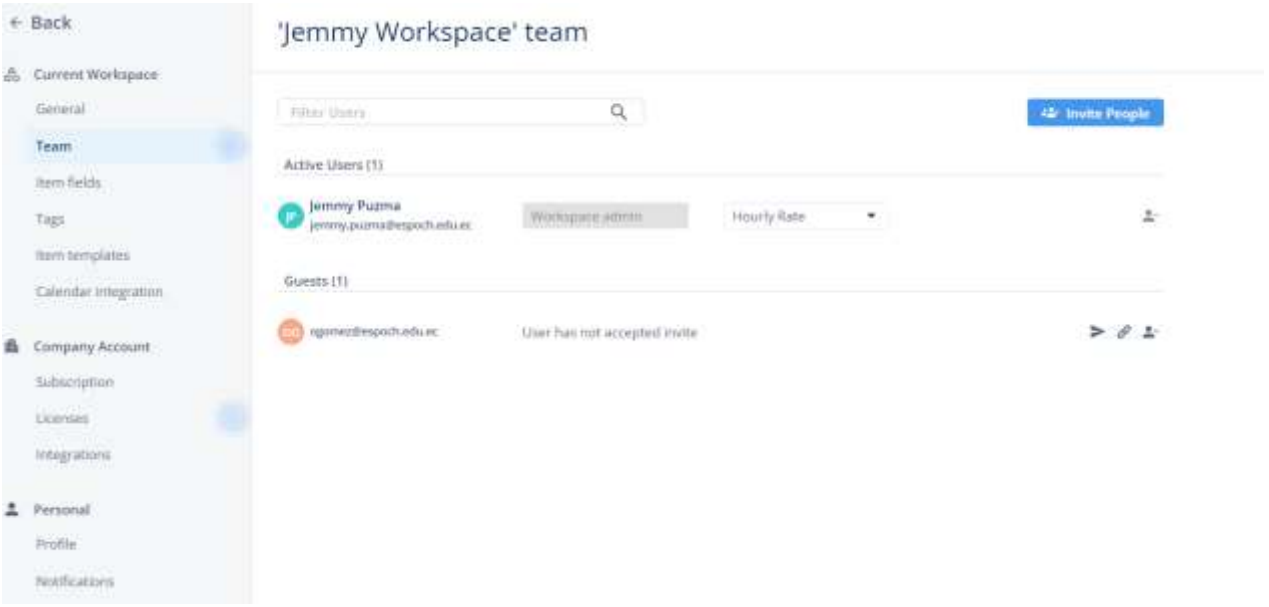


Figura 13-3: Equipo de desarrollo

Realizado por: Jemmy Puzma, 2023.

3.6.3.2 *Flujo de trabajo o Iteración*

En la Figura 14-3 muestran las iteraciones de las actividades.

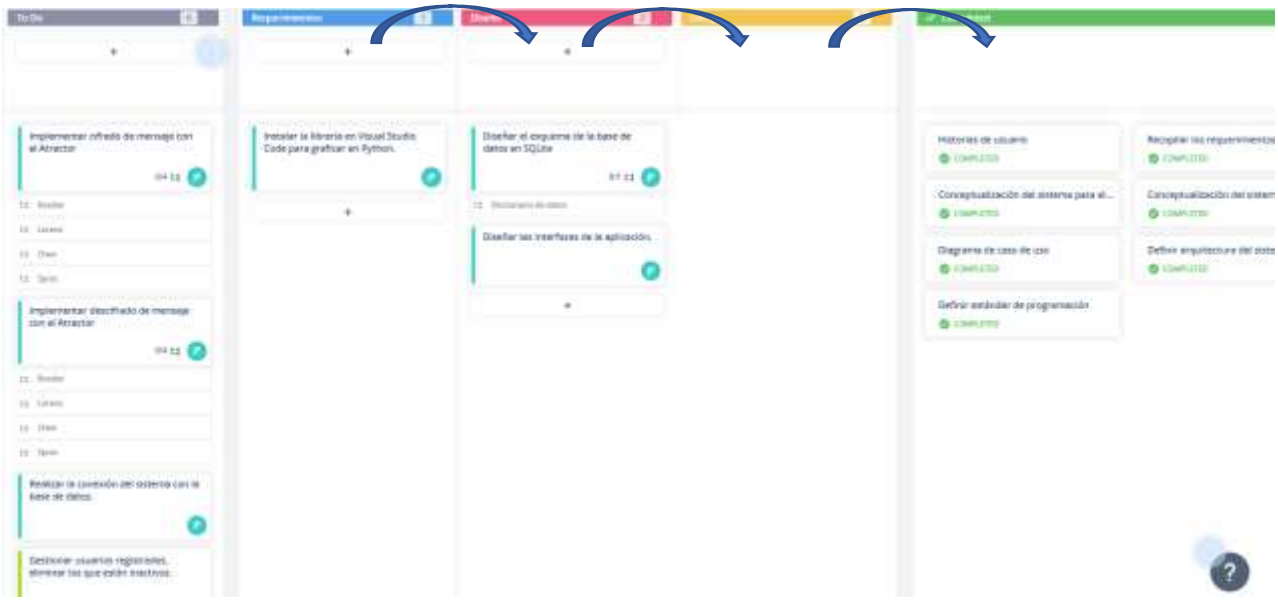


Figura 14-3: Flujo de trabajo

Realizado por: Jemmy Puzma, 2023.

3.6.3.3 *Asignación de una tarea*

Cada tarea registrada se debe asignar a un miembro del equipo, como se observa en la Figura 15-3.

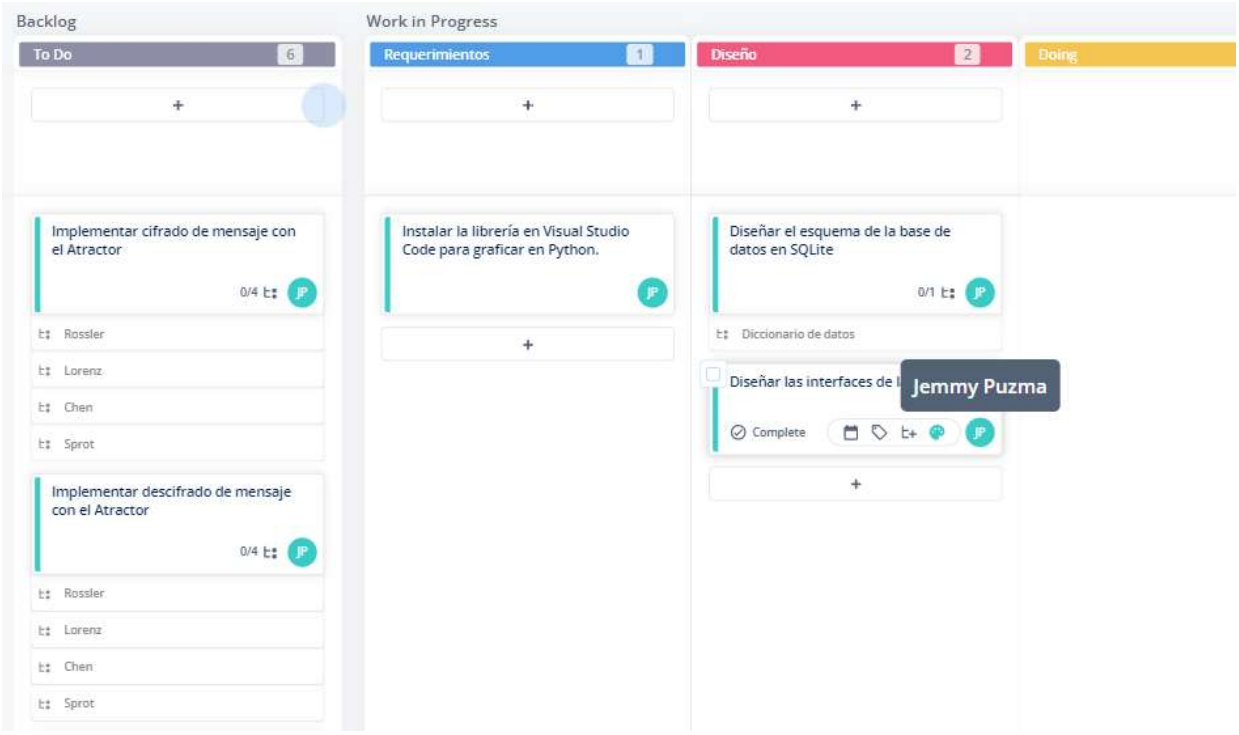


Figura 15-3: Asignación de tareas

Realizado por: Jemmy Puzma, 2023.

Una vez definida las tareas, se propone dividirlas en subtareas para tener un seguimiento óptimo. En la Figura 16-3 se muestra cómo se han dividido las tareas principales en subtareas.

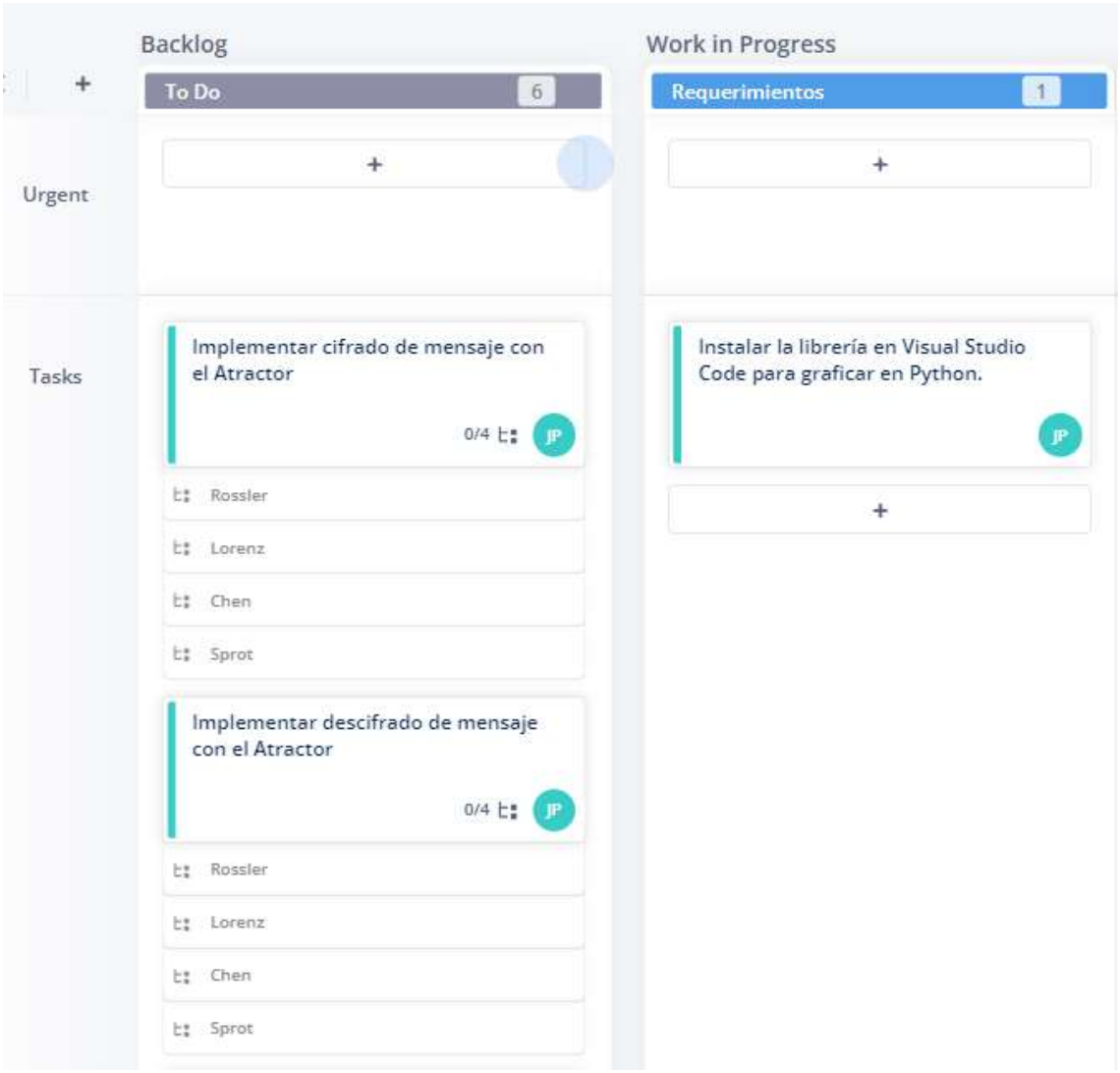


Figura 16-3: Tareas divididas en subtareas

Realizado por: Jemmy Puzma, 2023.

3.6.4 *Desarrollo*

3.6.4.1 *Elicitación de requerimientos*

Como parte de la metodología de SCRUM se ha recopilado los requerimientos mediante historias de usuario. Se puede observar en la Tabla 12-3.

Tabla 12-3: Historias de Usuario

Historias de Usuario				
ID de la historia	**Rol**	**Característica/ Funcionalidad**	**Razón/ Resultado**	**Criterio de aceptación**
ID.01	Como un usuario	Quiero poder seleccionar el	Para poder cifrar y descifrar cadenas de texto	Menú con los cuatro atractores.

		atractor con el cual trabajar.		
ID.02	Como un usuario	Quiero poder registrarme e iniciar sesión.	Para ingresar al sistema.	Login y página de registro.
ID.03	Como un usuario	Quiero poder ingresar una cadena de texto en cualquier atractor.	Para cifrar o descifrar la cadena de texto.	Página para ingresar cadenas de texto.
ID.04	Como un usuario	Quiero poder visualizar el texto cifrado, con el tiempo de sincronización y cifrado.	Para observar los datos del cifrado y descifrado.	Página con el texto cifrado y su información sobre los tiempos solicitados.
ID.05	Como un usuario	Quiero poder cerrar sesión después de utilizar el sistema.	Para volver a ingresar cuando sea necesario.	Botón de cerrar sesión.
ID.06	Como un administrador	Quiero poder iniciar sesión y registrarme.	Para ingresar al sistema.	Login y página de registrarse.
ID.07	Como un administrador	Quiero poder eliminar los usuarios, datos del cifrado y descifrado.	Para que en los resultados de los informes se utilicen datos recientes.	Eliminar un usuario.
ID.08	Como un administrador	Quiero poder generar informes estadísticos con la información del cifrado y descifrado.	Para analizar y sacar conclusiones.	Informes estadísticos.

ID.09	Como un administrador	Quiero poder observar las Ip y ubicaciones de donde inicia sesión el usuario.	Para observar que el usuario esté utilizando el sistema.	Tabla de inicio de sesiones.
ID.10	Como un administrador	Quiero poder cerrar sesión.	Para volver a ingresar en caso de que sea necesario.	Botón de cerrar sesión.

Realizado por: Jemmy Puzma, 2023.

Una vez analizadas las historias de usuario se ha realizado una clasificación entre requisitos funcionales y no funcionales. Ver **Anexo A** y **Anexo B.**

3.6.4.2 *Conceptualización del sistema para el administrador*

En la Figura 17-3 se observa que el administrador se tiene que autenticarse para ingresar a la página principal, una vez ingresado puede escoger entre las opciones: Inicio, Atractores, Usuarios, Inicios de Sesión e Informes. En la opción de Inicio podrá visualizar información del cifrado y los informes datos estadísticos, se realizará la petición en la base de datos.

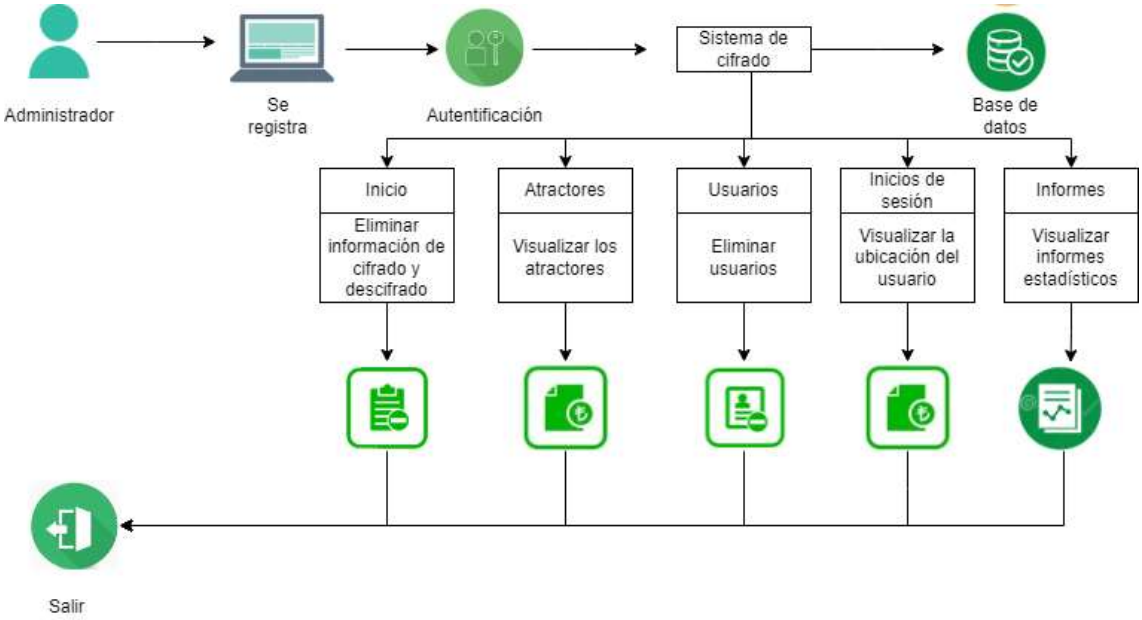


Figura 17-3: Conceptualización del sistema para el administrador

Realizado por: Jemmy Puzma, 2023.

3.6.4.3 *Conceptualización del sistema para el usuario*

Se observa en la Figura 18-3 que el usuario se autentica para ingresar al menú principal, donde constará de un inicio y opciones de cifrado, mediante Rossler, Lorenz, Chen y Sprott. En cada atractor se podrá ingresar una cadena de texto y al dar clic en el botón cifrar se mostrará información de tiempos de sincronización, cifrado, también tendrá la opción de descifrar en donde se ingresa la cadena de texto cifrada y mostrará la cadena descifrada, y el atractor utilizado con su tiempo. Se almacenará en la base de datos.

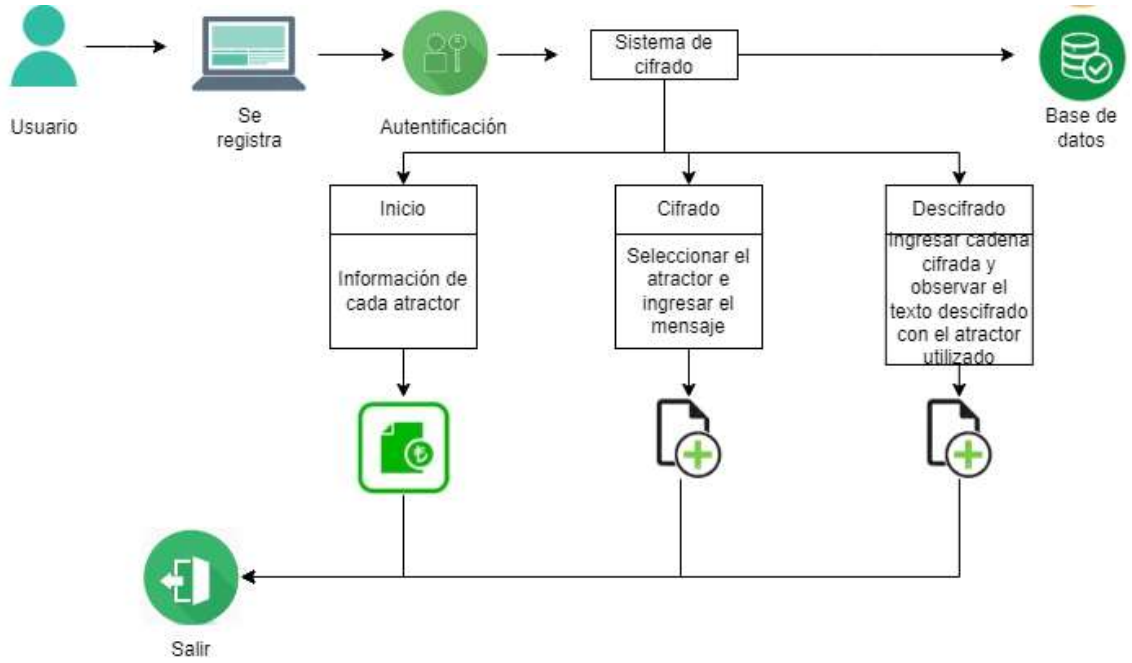


Figura 18-3: Conceptualización del sistema para usuario

Realizado por: Jemmy Puzma, 2023.

3.6.4.4 *Arquitectura MVC*

Para documentar la arquitectura se utiliza el modelo 4+1 de krutchen. Se observa en la Figura 19-3.

Figura 19-3: Modelo 4+1 de krutchen

Fuente: (Jarroba 2012).

- **Vista lógica**

En la Figura 20-3 de la vista lógica se observa el diagrama de clases que compone la aplicación web de cifrado.

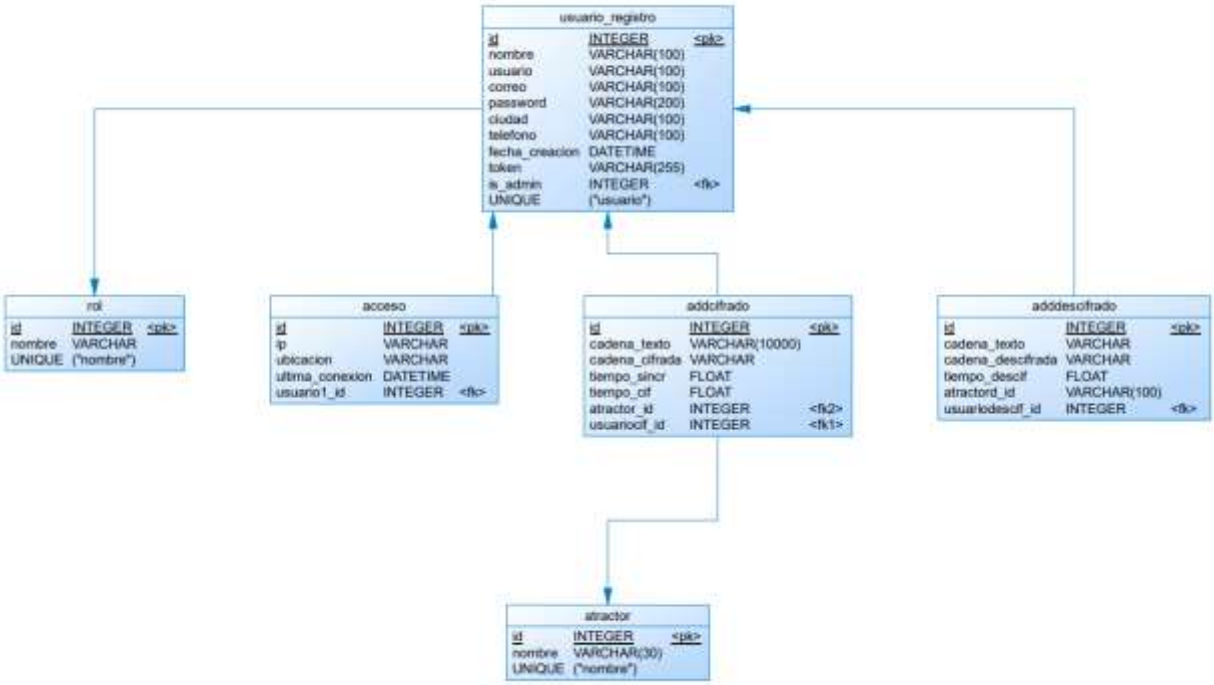


Figura 20-3: Diagrama de clases

Realizado por: Jemmy Puzma, 2023.

- **Vista de despliegue**

En esta vista se ha elegido representarla mediante el diagrama de componentes, que se visualiza en la Figura 21-3.

Figura 21-3: Diagrama de componentes

Realizado por: Jemmy Puzma, 2023.

- **Vista de procesos**

Se ha diseñado dos diagramas de actividades, en donde representan el proceso en que el usuario ingresa a la aplicación y cifra el mensaje, de igual manera para el proceso de descifrado. Ver Figura 22-3.

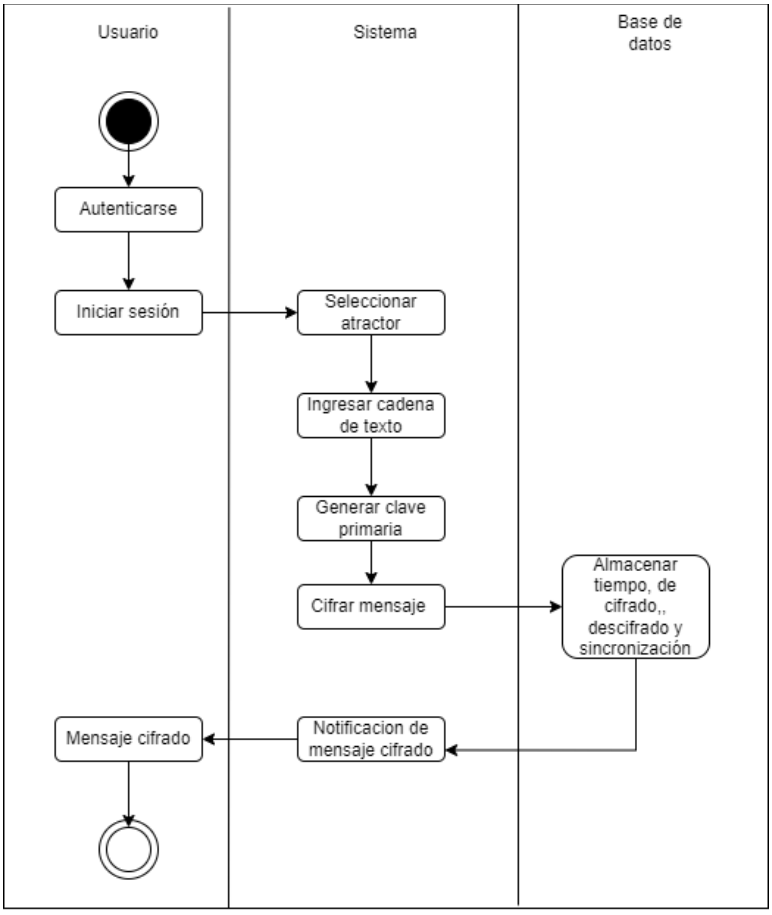


Figura 22-3: Diagrama de actividades del cifrado

Realizado por: Jemmy Puzma, 2023.

El proceso de descifrado se observa en la Figura 23-3.

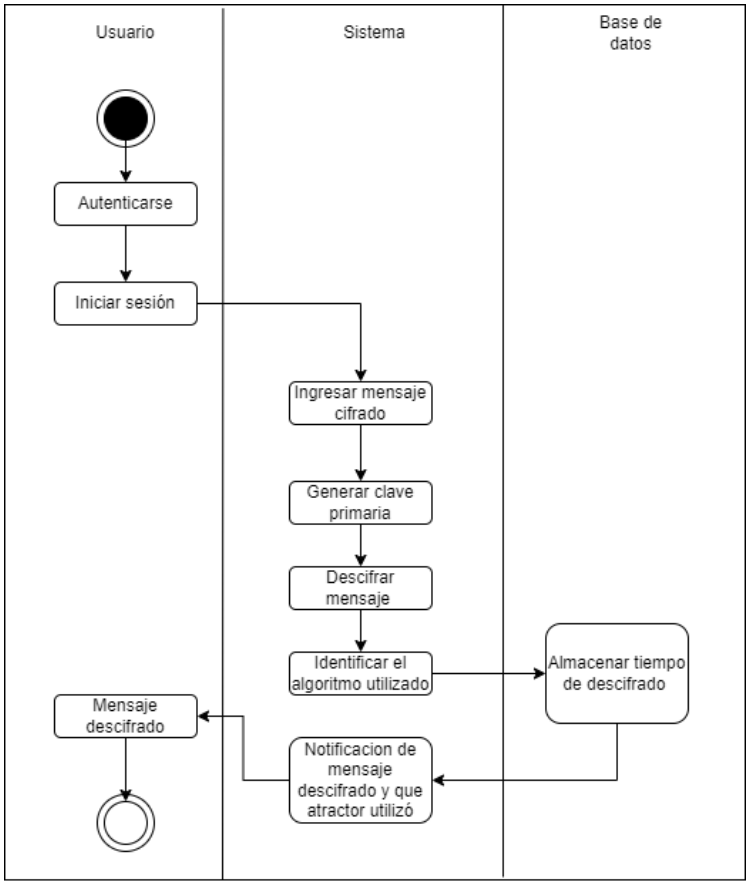


Figura 23-3: Diagrama de actividades del descifrado

Realizado por: Jemmy Puzma, 2023.

- **Vista física**

La siguiente Figura 24-3 muestra el usuario que utiliza una computadora para ingresar al sistema, y solicitar las peticiones al servidor.

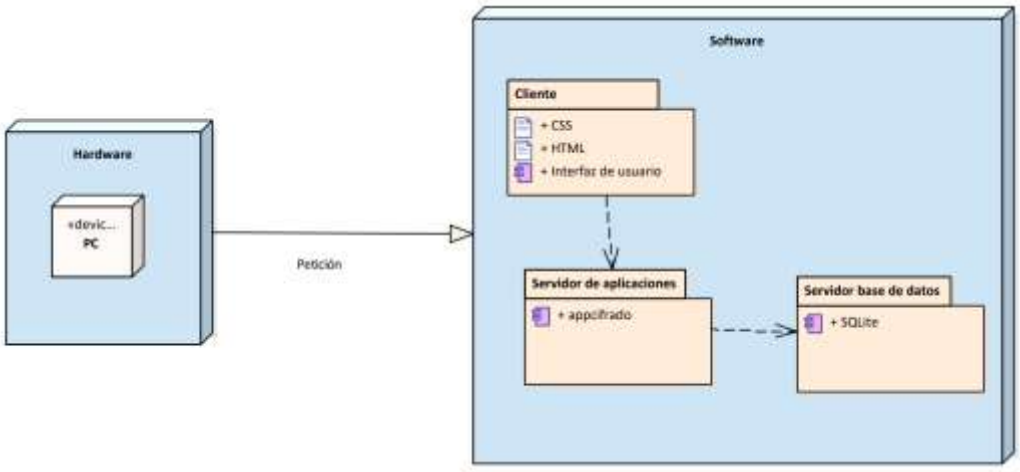


Figura 24-3: Diagrama de despliegue

Realizado por: Jemmy Puzma, 2023.

- **Vista de escenario**

Para la vista de escenario se muestra el diagrama de caso de uso, ver Figura 25-3.
Este diagrama permite observar el funcionamiento del sistema completo con las interacciones de los usuarios y administradores.

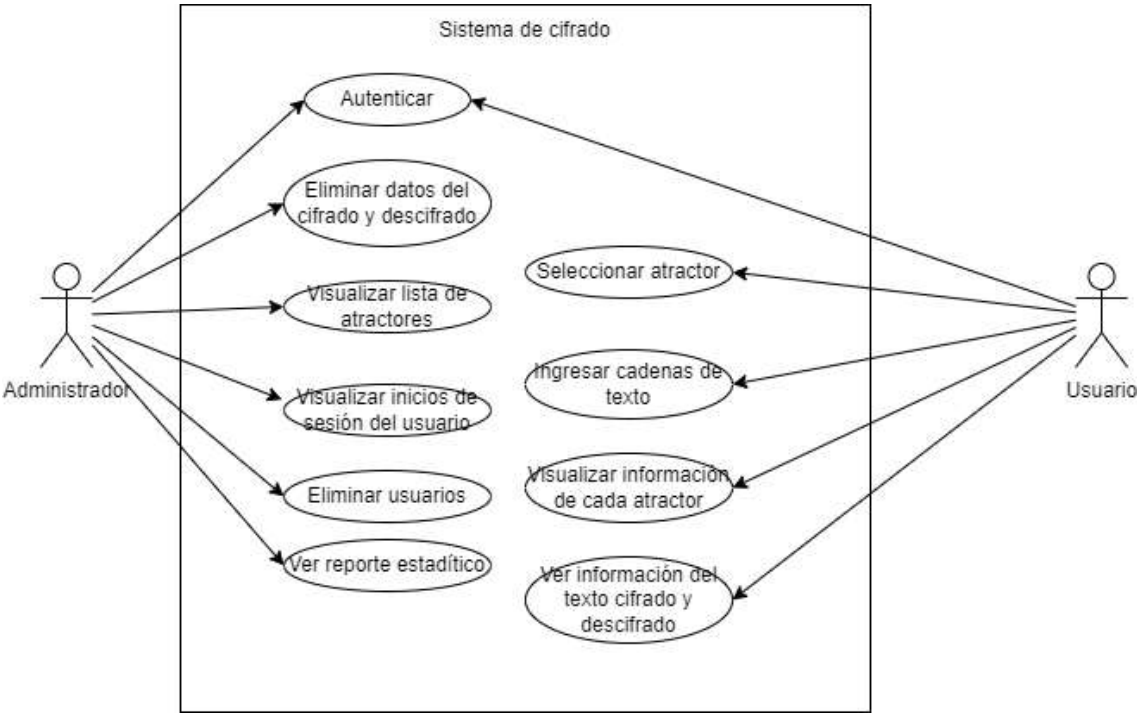


Figura 25-3: Diagrama de caso de uso

Realizado por: Jemmy Puzma, 2023.

3.6.4.5 *Estándar y convención de codificación*

Dado que el trabajo de integración curricular es parte del grupo de investigación GrIISoft es necesario definir un estándar de programación para que el equipo pueda observar un código organizado y legible. Se ha optado por PEP8 en Python que son recomendaciones que abarcan aspectos como la nomenclatura de variables, funciones y clases, la indentación, el uso de espacios en blanco, la longitud de línea y otros detalles de estilo.

Para los objetos de la base de datos se ha definido la convención SnakeCase, que es una forma de nombrar variables, funciones y otros elementos en la programación, en la cual se utiliza una combinación de palabras en minúsculas separadas por guiones bajos (_).

3.6.4.6 *Esquema de la base de datos*

Con el objetivo de almacenar información de manera organizada, se desarrolló el siguiente esquema de la base de datos en la cual se identificó diferentes entidades. Se observa el esquema físico en la Figura 26-3.

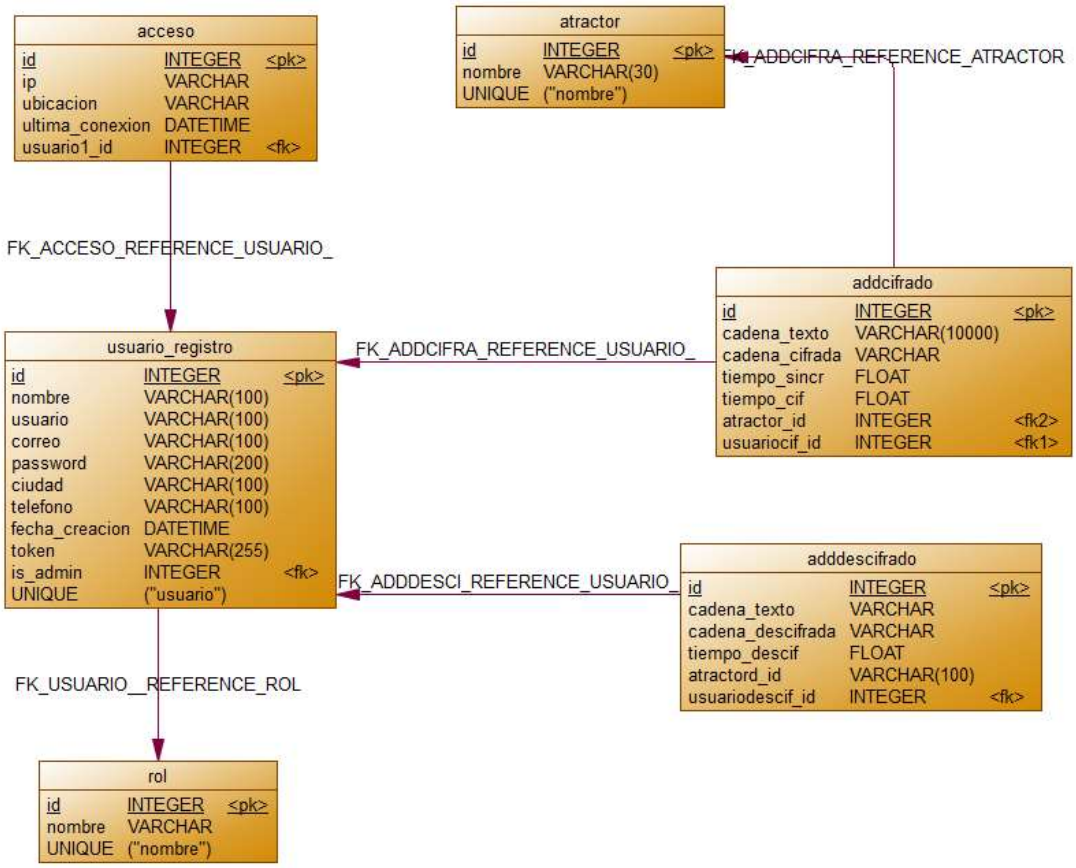


Figura 26-3: Diagrama físico de la base de datos

Realizado por: Jemmy Puzma, 2023.

3.6.4.7 *Diccionario de datos*

En la Tabla 13-3 se muestra el diccionario de datos de la tabla usuario_registro.

Tabla 13-3: Diccionario de datos de la tabla usuario_registro.

Nombre del archivo: usuario_registro **Descripción del archivo:** Persona natural que utiliza el sistema.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1

nombre	Nombre y apellido del usuario.	Varchar(100)	No	primer nombre + (primer apellido) = { [A-Z|a-z] }
usuario	Nombre de usuario o username.	Varchar(100)	No	Nombre de usuario = { [AZ|a-z] } + [0 a 9]
correo	Correo del usuario.	Varchar(100)	No	correo@example.com
password	Contraseña del usuario.	Varchar(100)	No	=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{8,}
ciudad	Ciudad de residencia del usuario.	Varchar(100)	No	ciudad = { [A-Z|a-z] }
telefono	Teléfono personal del usuario.	Varchar(100)	No	[0000000000] * permite un dígito [0 a 9] y requiere la entrada de los 10 dígitos *
fecha_creacion	Fecha en que se registra el usuario.	Datetime	No	* formato: aaaa-mm-dd *
token	Para recuperar la contraseña.	Varchar(255)	Si	Token generado
is_admin (FK)	Rol de usuario.	Integer	No	[1 | 2] * significado: 1: Admin | 2: Usuario *

Realizado por: Jemmy Puzma, 2023.

El diccionario completo de datos se encuentra en el **Anexo D.**

3.6.4.8 *Prototipo de la página principal del usuario.*

La Figura 27-3 muestra un diseño de mockup de la pantalla principal del usuario.

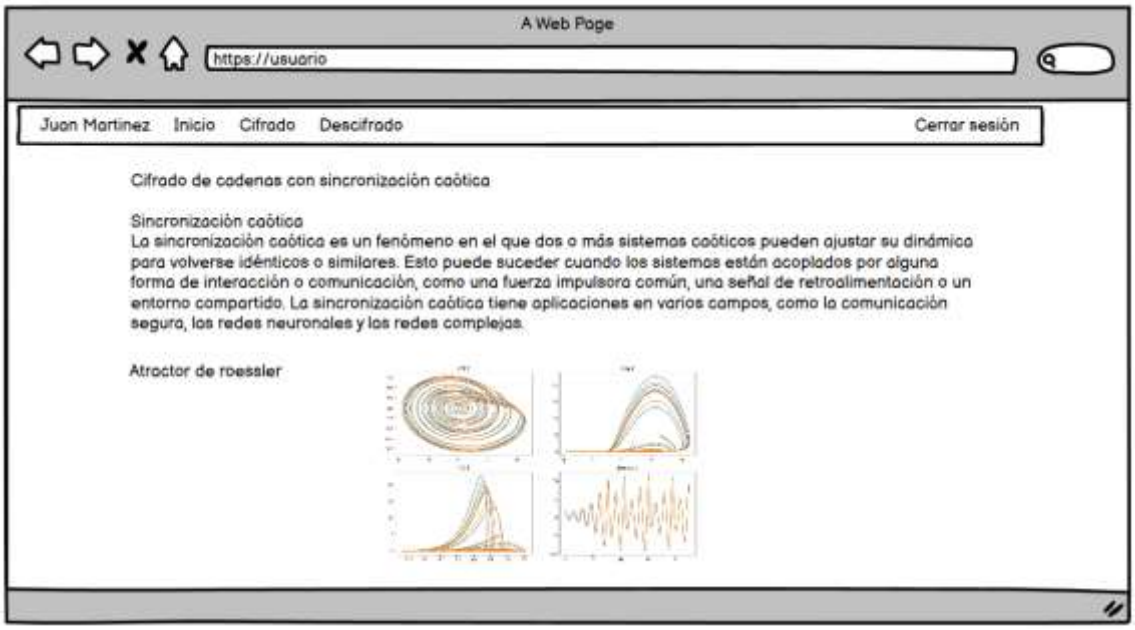


Figura 27-3: Prototipo de la página principal del usuario

Realizado por: Jemmy Puzma, 2023.

El prototipado completo se encuentra en el **Anexo E.**

3.6.5 *Pruebas*

En esta etapa se procede a realizar validaciones de cada una de las tareas asignadas y cumplidas durante el desarrollo. Se analizó los posibles errores que podría presentar el sistema, a continuación, presentamos las validaciones realizadas en el **Anexo F.**

3.6.6 *Despliegue*

Se generó una imagen Docker de la aplicación web, ver **Anexo J**.

3.6.7 *Hecho*

Una vez que se ha cumplido las tareas planteadas de acuerdo con los requerimientos funcionales y no funcionales, se da por terminada la aplicación web para cifrado y descifrado de cadenas de texto mediante la selección de un atractor caótico. Para documentar las tareas cumplidas se utilizó la herramienta Teamhood. Se visualiza a continuación en la Figura 28-3.

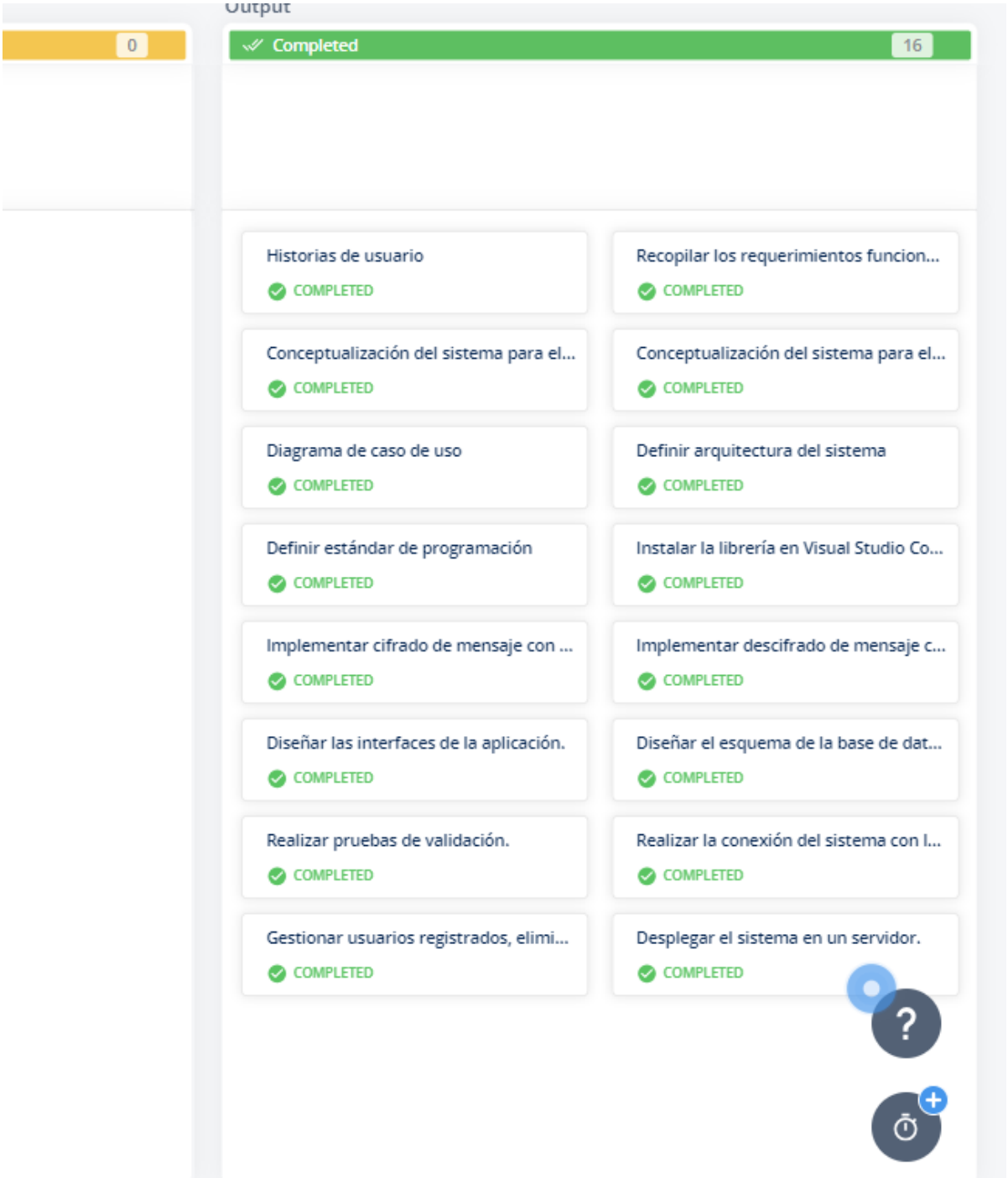


Figura 28-3: Tareas completadas

Realizado por: Jemmy Puzma, 2023.

CAPÍTULO IV:

4 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

A continuación, se presenta los resultados obtenidos con el desarrollo de la aplicación web para cifrar y descifrar cadenas de texto mediante la selección de un atractor caótico. Estos resultados se obtuvieron mediante técnicas de medición del comportamiento temporal, y la confidencialidad, según los resultados obtenidos se aplicó análisis de varianza, test no paramétrico de Kruskal Wallis y diagramas de dispersión respectivamente.

4.1 Evaluación de comportamiento temporal

Para la evaluación del comportamiento en el tiempo se ha tomado un texto de 3793 caracteres, el cual se observa en el **Anexo G.**

Los resultados que se muestran a continuación se realizaron en una computadora MSI, 8 GB de RAM, procesador Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz (8 CPUs), ~2.5GHz, disco duro 256 GB.

4.1.1 *Proceso cifrado*

4.1.1.1 *Tiempo de sincronización*

En la Tabla 14-4 se muestran los resultados de las 25 muestras por cada atractor, obteniendo el promedio de tiempo de sincronización en microsegundos.

Tabla 14-4: Promedio de tiempo de sincronización por cada atractor.

Atractor	**Promedio del tiempo de sincronización.**
Chen	213428,44 µs
Lorenz	34650,96 µs
Rossler	314535,92 µs
Sprott	74541,6 µs

Realizado por: Jemmy Puzma, 2023.

Análisis descriptivo

El siguiente Gráfico 3-4 muestra un análisis descriptivo del tiempo de sincronización de cada atractor.

```
> describeBy(tiempo_sincr, atractor_id)

 Descriptive statistics by group
group: Chen
   vars  n    mean      sd median trimmed      mad    min     max   range skew kurtosis
X1    1 25 2134284 2798315 959410 1657003 829737.1 241730 9120270 8878540 1.64      1.1
         se
X1 559662.9
------------------------------------------------------------------------
group: Lorenz
   vars  n     mean       sd median  trimmed      mad    min    max  range skew kurtosis
X1    1 25 346509.6 80955.22 339890 342223.8 88792.91 229750 525320 295570 0.39    -0.76
         se
X1 16191.04
------------------------------------------------------------------------
group: Rossler
   vars  n    mean      sd  median trimmed     mad    min     max   range skew kurtosis
X1    1 25 3145359 2202099 2776990 2982488 1309877 179980 7791330 7611350 0.81    -0.21
         se
X1 440419.7
------------------------------------------------------------------------
group: Sprott
   vars  n   mean      sd median  trimmed      mad    min     max   range skew kurtosis
X1    1 25 745416 1877016 333180 369574.8 83336.95 244760 9741480 9496720 4.39    18.11
         se
X1 375403.1
```

Gráfico 3-4: Análisis descriptivo del tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

Los resultados que se muestran están en microsegundos (μs) y permite observar cómo se comportan los tiempos de sincronización en cada atractor o grupo.

Chen: Este grupo tiene un tiempo medio de sincronización de alrededor de 2,134,284 μs (o alrededor de 2.13 segundos). Sin embargo, los tiempos de sincronización en este grupo varían significativamente, ya que la desviación estándar es bastante alta (2,798,315 μs). Esto significa que algunos sistemas se sincronizan mucho más rápido o lento que la media.

Lorenz: Este grupo tiene un tiempo medio de sincronización mucho menor, de alrededor de 346,509.6 μs (o alrededor de 0.35 segundos). Los tiempos de sincronización en este grupo parecen estar más estrechamente agrupados alrededor de la media, ya que la desviación estándar es bastante baja (80,955.22 μs). Esto indica que los sistemas en este grupo tienden a sincronizarse a una velocidad más consistente.

Rossler: Este grupo tiene el tiempo medio de sincronización más alto de todos los grupos, de alrededor de 3,145,359 μs (o alrededor de 3.15 segundos). Sin embargo, hay una considerable variabilidad en los tiempos de sincronización, como lo indica la alta desviación estándar (2,202,099 μs). Esto significa que algunos sistemas en este grupo pueden tardar mucho más tiempo en sincronizarse que otros.

Sprott: Este grupo tiene un tiempo medio de sincronización de alrededor de 745,416 µs (o alrededor de 0.75 segundos). Sin embargo, hay una considerable variabilidad en los tiempos de sincronización en este grupo, como lo indica la alta desviación estándar. Esto sugiere que algunos sistemas en este grupo pueden tardar considerablemente más tiempo en sincronizarse que otros.

En resumen, estos resultados muestran que el atractor de Rossler es el más lento en llegar a sincronizarse, siguiéndole Chen, después Sprott y culminando con el más rápido que es Lorenz.

Se presenta un diagrama de caja, el cual muestra los siguientes resultados a primera vista. Ver Gráfico 4-4.

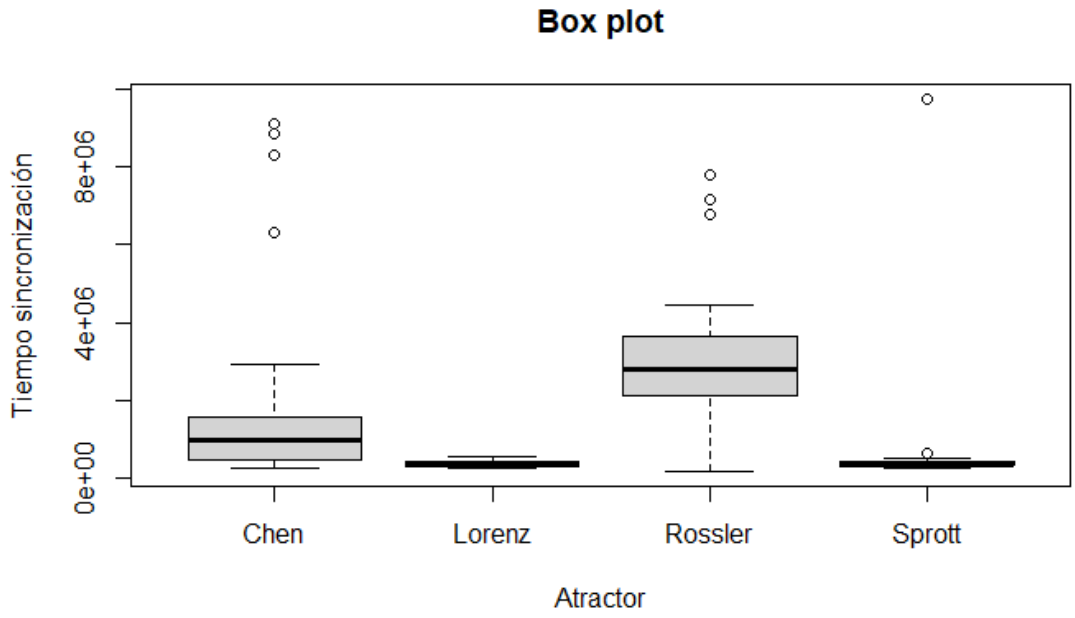


Gráfico 4-4: Diagrama de caja del tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

La mediana en Chen y Sprott está dividiendo la caja en partes desiguales de manera que tiene una asimetría positiva, esto quiere decir que los datos se concentran en la parte inferior de la distribución y la media suele ser mayor que la mediana. También presentan algunos valores atípicos en Chen, Rossler y Sprott.

Se observa que las medias son similares en los atractores de Chen y Rossler, pero en los atractores Lorenz y Sprott, no se puede determinar cuál es el más rápido para lograr la sincronización.

Análisis Inferencial

En el análisis de varianza realizado llamado (anova1) dio como resultado un valor de p = 6.59e-06, lo que muestra que existe al menos un atractor que difiere sustancialmente del resto. Se observa en el Gráfico 5-4.

```
> summary(anova1)
             Df    Sum Sq   Mean Sq F value   Pr(>F)
atractor_id   3 1.244e+14 4.146e+13   10.23 6.59e-06 ***
Residuals    96 3.890e+14 4.052e+12
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

Gráfico 5-4: Valor de p para tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

Para identificar cual o cuales son los atractores que presentan diferencias significativas, se realiza una prueba de Tukey. Al realizar la prueba se tiene los siguientes valores que se muestra en el Gráfico 6-4.

```
> TukeyHSD(anova1)
  Tukey multiple comparisons of means
    95% family-wise confidence level

Fit: aov(formula = tiempo_sincr ~ atractor_id)

$atractor_id
                     diff        lwr        upr     p adj
Lorenz-Chen    -1787774.8 -3276473.4 -299076.21 0.0118528
Rossler-Chen    1011074.8  -477623.8 2499773.39 0.2912944
Sprott-Chen    -1388868.4 -2877567.0   99830.19 0.0765634
Rossler-Lorenz  2798849.6  1310151.0 4287548.19 0.0000215
Sprott-Lorenz    398906.4 -1089792.2 1887604.99 0.8966026
Sprott-Rossler -2399943.2 -3888641.8 -911244.61 0.0003252
```

Gráfico 6-4: Valores estadísticos de las comparaciones entre los atractores basado en el tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

El atractor "Lorenz" es el más eficiente en términos de tiempo de sincronización, siendo significativamente más rápido que el atractor "Chen". Sin embargo, el atractor "Rossler" es más lento que "Lorenz", y además supera significativamente a "Chen". Estos resultados indican que "Lorenz" es el más adecuado para aplicaciones donde se requiere una sincronización rápida.

El atractor "Sprott", aunque más lento que "Chen" y más rápido que "Lorenz", no mostró diferencias significativas en comparación con ellos. Esto sugiere que el tiempo de sincronización de "Sprott" es comparable al de estos atractores.

Finalmente, "Sprott" es significativamente más rápido que "Rossler". Esta diferencia sugiere que "Rossler", aunque es eficiente en comparación con "Chen", podría no ser la opción más adecuada cuando se requiere una sincronización rápida, en comparación con los otros atractores.

Cabe señalar que estos resultados son específicos para las condiciones bajo las cuales se realizó el experimento. La eficiencia de la sincronización de los atractores podría variar en diferentes condiciones o aplicaciones. Por lo tanto, si bien "Lorenz" es el más eficiente en este escenario particular, podría no serlo en todas las situaciones.

Para tener una mejor visualización de los resultados se muestra en el Gráfico 7-4 barras generado desde la aplicación web de cifrado y descifrado de cadenas de texto mediante la selección de un atractor caótico.

Gráfico 7-4: Gráfico de barras del tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

Se demuestra que el atractor de Lorenz es el más rápido en realizar la sincronización y el atractor de Rossler es el que tarda más.

Evaluación de supuestos del modelo

Se realiza una evaluación de supuestos del modelo para determinar si fue factible realizar un análisis de varianza, o de lo contrario utilizar una prueba no paramétrica.

Para los análisis se utiliza un nivel de significancia de 0.05.

Igualdad de varianzas

Se utilizó levenetest para observar si existe una igualdad en las varianzas. Ver Gráfico 8-4.

```
> leveneTest(tiempo_sincr ~ atractor_id, cifradotabla3)
Levene's Test for Homogeneity of Variance (center = median)
      Df F value   Pr(>F)
group  3   4.791 0.003736 **
      96
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

Gráfico 8-4: Test de levene de igualdad de varianzas en tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

Dado que el p-valor (0.003736) es significativamente menor que 0.05, se puede rechazar la hipótesis nula (H0) de igualdad de varianzas entre los atractores. Esto significa que existe evidencia suficiente para afirmar que las varianzas de los tiempos de sincronización son diferentes entre al menos dos de los grupos definidos por el atractor_id.

Normalidad de los residuos del modelo

En la prueba de normalidad de Lilliefors (Kolmogorov-Smirnov) se obtuvo lo siguiente ver Gráfico 9-4.

```
> lillie.test(standard_res)

        Lilliefors (Kolmogorov-Smirnov) normality test

data:  standard_res
D = 0.31297, p-value < 2.2e-16
```

Gráfico 9-4: Prueba de normalidad de Lilliefors del tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

La hipótesis nula (H0) de la prueba de Lilliefors es que los datos siguen una distribución normal. La hipótesis alternativa (H1) es que los datos no siguen una distribución normal.

Dado que el p-valor es extremadamente pequeño (< 2.2e-16) y es menor que el nivel de significancia de 0.05, se puede concluir que hay evidencia suficiente para rechazar la hipótesis nula (H0). Es decir, los datos de la variable "standard_res" no siguen una distribución normal.

Según los resultados observados se determinó que es necesario realizar una prueba no paramétrica, en este caso se utiliza la prueba de Kruskal Wallis. Gráfico 10-4.

```
> kruskal.test(tiempo_sincr ~ atractor_id, cifradotabla3)

        Kruskal-Wallis rank sum test

data:  tiempo_sincr by atractor_id
Kruskal-Wallis chi-squared = 43.833, df = 3, p-value = 1.638e-09
```

Gráfico 10-4: Test de Kruskal Wallis para tiempo de sincronización

Realizado por: Jemmy Puzma, 2023.

La hipótesis nula (H0) de la prueba de Kruskal-Wallis es que no hay diferencias entre las medianas de los grupos definidos por el atractor_id. La hipótesis alternativa (H1) es que al menos una mediana es diferente.

Dado que el valor p obtenido en la prueba (1.638e-09) es mucho menor que el nivel de significancia de 0.05, se puede concluir que hay evidencia suficiente para rechazar la hipótesis nula (H0). Esto significa que al menos una de las medianas del tiempo de sincronización en microsegundos difiere significativamente entre los grupos definidos por el atractor_id.

4.1.1.2 *Tiempo de cifrado*

En la Tabla 15-4 se muestran los resultados de las 25 muestras por cada atractor, obteniendo el promedio de tiempo de cifrado en microsegundos.

Tabla 15-4: Tabla de promedios del tiempo de cifrado por cada atractor.

Atractor	**Promedio del tiempo de cifrado.**
Chen	200683,48 µs
Lorenz	46287,52 µs
Rossler	349716,92 µs

Sprott	74817,28 µs

Realizado por: Jemmy Puzma, 2023.

Análisis descriptivo

El siguiente Gráfico 11-4 muestra un análisis descriptivo del tiempo de cifrado de cada atractor.

```
> describeBy(tiempo_cif, atractor_id)

 Descriptive statistics by group
group: Chen
   vars  n    mean      sd median trimmed      mad    min     max   range skew kurtosis
X1    1 25 2006835 3017159 860250 1445411 846742.5 131260 9862490 9731230 1.71     1.36
         se
X1 603431.8
------------------------------------------------------------------------
group: Lorenz
   vars  n     mean       sd median  trimmed      mad  min     max   range skew kurtosis
X1    1 25 462875.2 403624.2 323420 423514.8 285578.4 6140 1442190 1436050 0.92    -0.27
         se
X1 80724.84
------------------------------------------------------------------------
group: Rossler
   vars  n    mean      sd  median trimmed     mad    min     max   range skew kurtosis
X1    1 25 3497169 2105320 3291650 3464702 2661979 348840 7000370 6651530 0.18    -1.34
         se
X1 421063.9
------------------------------------------------------------------------
group: Sprott
   vars  n     mean      sd median  trimmed      mad  min     max   range skew kurtosis
X1    1 25 748672.8 1749214 324260 404897.1 436447.8 7360 8969960 8962600 4.13    16.53
         se
X1 349842.7
```

Gráfico 11-4: Análisis descriptivo del tiempo de cifrado con cada atractor

Realizado por: Jemmy Puzma, 2023.

El atractor Rossler tiene el tiempo de cifrado promedio más largo (aproximadamente 3.5 segundos), seguido por Chen (aproximadamente 2 segundos), Sprott (aproximadamente 0.75 segundos) y Lorenz (aproximadamente 0.46 segundos). Sin embargo, hay una gran variabilidad en los tiempos de cifrado dentro de cada grupo, como lo indica la desviación estándar (sd).

La variabilidad es especialmente notable en el grupo Rossler, que tiene la mayor desviación estándar. Esto indica que, aunque el atractor Rossler puede tener un tiempo promedio de cifrado más largo, también tiene una amplia gama de tiempos de cifrado que pueden ser más cortos o largos que el promedio.

Por otro lado, el atractor Lorenz tiene la menor desviación estándar, lo que sugiere que sus tiempos de cifrado son más consistentes en comparación con los otros atractores.

El grupo Sprott presenta la mayor asimetría (skew) y curtosis, lo que sugiere una distribución muy sesgada hacia los tiempos de cifrado más cortos y una mayor concentración de tiempos de cifrado en torno a su media, con algunas excepciones notables que se alejan mucho de la media (es decir, tiempos de cifrado extremadamente largos).

En resumen, aunque el atractor Rossler tiene el mayor tiempo promedio de cifrado, también tiene la mayor variabilidad. Lorenz es el más rápido y consistente, mientras que Sprott muestra una amplia gama de tiempos de cifrado, aunque tiende a tener tiempos más cortos en general, pero con algunas excepciones de tiempos muy largos. Chen se encuentra en un término medio, con tiempos de cifrado promedio y variabilidad.

Se presenta un diagrama de caja. Ver Gráfico 12-4.

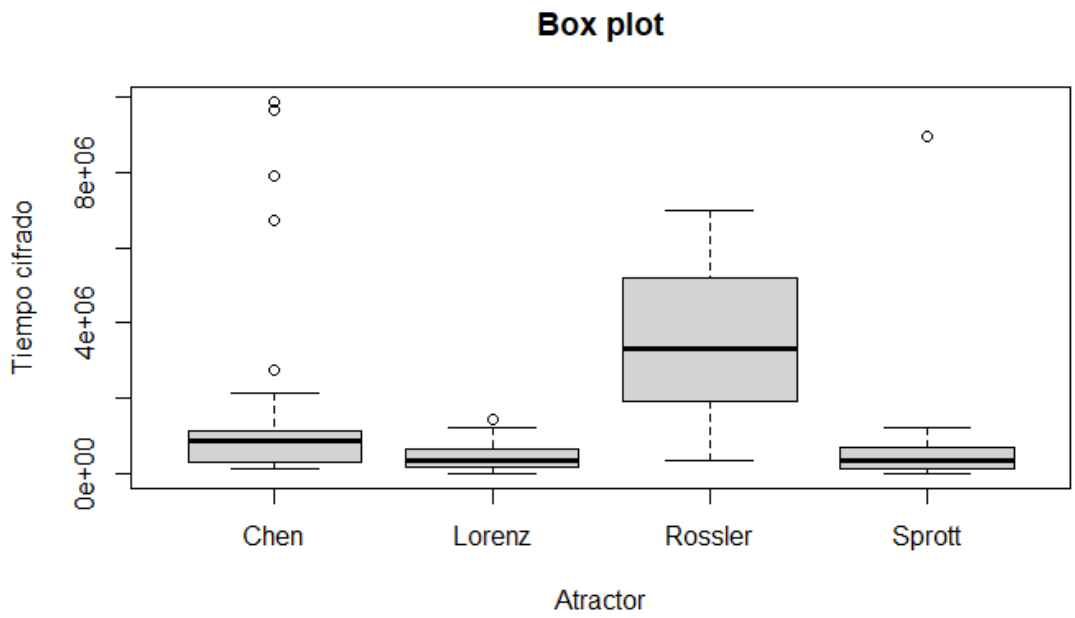


Gráfico 12-4: Diagrama de caja del tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

La mediana de los atractores está dividiendo la caja en partes desiguales de manera que Chen tiene una asimetría positiva, esto quiere decir que los datos se concentran en la parte inferior de la distribución y la media suele ser mayor que la mediana, en cambio Lorenz, Rossler y Sprott tienen una asimetría negativa, lo cual los datos se concentran en la parte superior de la distribución y la media suele ser menor que la mediana. También presentan algunos valores atípicos en Chen, Lorenz y Sprott.

A simple vista se observa que Rossler tiene mayor tiempo de cifrado, lo que indica que es más lento, en cambio entre Chen, Lorenz y Sprott, son ligeramente más rápidos, pero no se puede determinar cuál es el más rápido entre ellos. Para tener resultados exactos, se muestran los valores de cada comparación y el ANOVA entre los atractores.

Análisis inferencial

En el análisis de varianza realizado llamado (anova2) dio como resultado un valor de p = 1.74e-06, lo que muestra que existe al menos un atractor que difiere sustancialmente del resto. Se observa en el Gráfico 13-4.

```
> summary(anova2)
             Df    Sum Sq   Mean Sq F value   Pr(>F)
atractor_id   3 1.439e+14 4.798e+13   11.45 1.74e-06 ***
Residuals    96 4.022e+14 4.190e+12
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

Gráfico 13-4: Valor de p de tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

Para identificar cual o cuales son los atractores que presentan diferencias significativas, se realiza una prueba de Tukey. Al realizar la prueba se tiene los siguientes valores que se muestra en el Gráfico 14-4.

```
> TukeyHSD(anova2)
  Tukey multiple comparisons of means
    95% family-wise confidence level

Fit: aov(formula = tiempo_cif ~ atractor_id)

$atractor_id
                      diff        lwr        upr     p adj
Lorenz-Chen     -1543959.6 -3057646.7   -30272.5 0.0437923
Rossler-Chen     1490334.4   -23352.7  3004021.5 0.0552895
Sprott-Chen     -1258162.0 -2771849.1   255525.1 0.1381305
Rossler-Lorenz   3034294.0  1520606.9  4547981.1 0.0000056
Sprott-Lorenz     285797.6 -1227889.5  1799484.7 0.9603273
Sprott-Rossler  -2748496.4 -4262183.5 -1234809.3 0.0000422
```

Gráfico 14-4: Valores estadísticos de la comparación entre los atractores en base al tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

En primer lugar, Lorenz se destaca como el más eficiente, superando a Chen por un margen considerable. En términos prácticos, si se busca optimizar la velocidad de cifrado, Lorenz sería la opción preferida sobre Chen, ya que cifra en promedio 1.54 segundos más rápido. Este tipo de eficiencia puede ser particularmente valiosa en aplicaciones donde el tiempo de cifrado es crítico, como en sistemas de tiempo real o aplicaciones con grandes volúmenes de datos para cifrar.

Por otro lado, Rossler parece ser el atractor menos eficiente, mostrando un tiempo de cifrado más lento en comparación con Lorenz y Chen. Aunque no se puede afirmar con certeza estadística que Rossler sea más lento que Chen, sí se puede confirmar que es significativamente más lento que Lorenz. Por lo tanto, Rossler podría no ser la mejor opción en situaciones donde el tiempo de cifrado es un factor crítico.

Sprott, está en una posición intermedia, siendo más rápido que Chen, pero no necesariamente más rápido que Lorenz. Además, Sprott es significativamente más rápido que Rossler. Sprott podría ser una buena elección si Lorenz no está disponible.

En conclusión, este análisis indica que Lorenz y Sprott son generalmente más eficientes en términos de tiempo de cifrado en comparación con Chen y Rossler. Sin embargo, la elección del atractor más apropiado para realizar el cifrado es Lorenz y el que no es recomendable es Rossler.

Para tener una mejor visualización de los resultados se muestra un gráfico de barras generado desde la aplicación web. Gráfico 15-4.

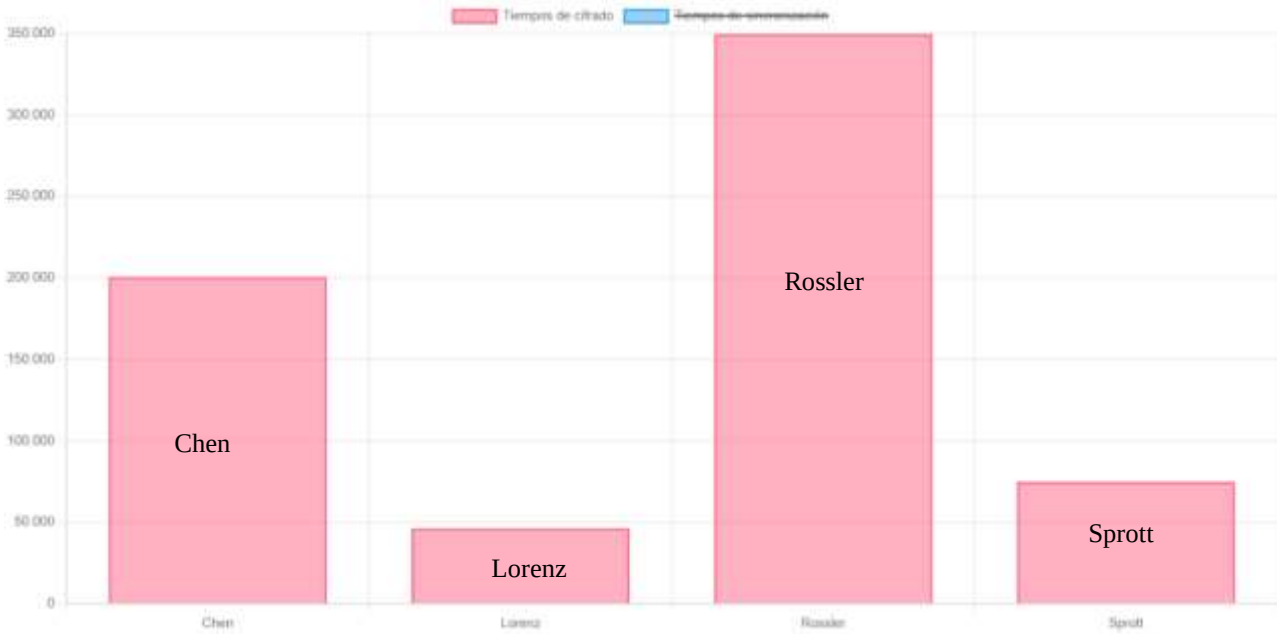


Gráfico 15-4: Gráfico de barras del tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

Se demuestra que el atractor de Lorenz es el más rápido para realizar el cifrado de cadenas de texto y Rossler es el más lento.

Evaluación de supuestos del modelo

Se realiza una evaluación de supuestos del modelo para determinar si fue factible realizar un análisis de varianza, o de lo contrario utilizar una prueba no paramétrica.

Para los análisis se utiliza un nivel de significancia de 0.05.

Igualdad de varianzas

Se utilizó levenetest para observar si existe una igualdad en las varianzas. Ver Gráfico 16-4.

```
> leveneTest(tiempo_cif ~ atractor_id, cifradotabla3)
Levene's Test for Homogeneity of Variance (center = median)
      Df F value   Pr(>F)
group  3  4.4282 0.005836 **
      96
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

Gráfico 16-4: Test de levene para la igualdad de varianzas del tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

Los resultados del test de Levene indican que existe una diferencia significativa en la variabilidad del tiempo de cifrado entre los diferentes grupos de atractores. El valor p (0.005836) es menor

que el nivel de significancia establecido (0.05), lo que significa que hay una fuerte evidencia para rechazar la hipótesis nula de que las varianzas de los tiempos de cifrado son iguales para todos los atractores.

Normalidad de los residuos del modelo

En la prueba de normalidad de Lilliefors (Kolmogorov-Smirnov) se obtuvo lo siguiente. Gráfico 17-4.

```
> lillie.test(standard_res1)

        Lilliefors (Kolmogorov-Smirnov) normality test

data:  standard_res1
D = 0.23238, p-value = 1.442e-14
```

Gráfico 17-4: Test de normalidad para el tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

El valor p en esta prueba es extremadamente bajo (1.442e-14, es decir, 0.00000000000001442). Un valor p bajo sugiere que se debe rechazar la hipótesis nula. En el caso de la prueba de Lilliefors, la hipótesis nula es que los datos siguen una distribución normal.

Según los resultados observados se determinó que es necesario realizar una prueba no paramétrica, en este caso se utiliza la prueba de Kruskal Wallis. Gráfico 18-4.

```
> kruskal.test(tiempo_cif ~ atractor_id, cifradotabla3)

        Kruskal-Wallis rank sum test

data:  tiempo_cif by atractor_id
Kruskal-Wallis chi-squared = 39.107, df = 3, p-value = 1.647e-08
```

Gráfico 18-4: Test de kruskal wallis para el tiempo de cifrado

Realizado por: Jemmy Puzma, 2023.

Dado este valor p extremadamente bajo, hay fuertes evidencias para rechazar la hipótesis de que los tiempos de cifrado son iguales para todos los atractores. Esto sugiere que al menos un atractor tiene un tiempo de cifrado mediano significativamente diferente a los demás.

4.1.2 *Proceso descifrado*

En la Tabla 16-4 se muestran los resultados de las 25 muestras por cada atractor, obteniendo el promedio de tiempo de descifrado en microsegundos.

Tabla 16-4: Resultados del proceso de descifrado.

Atractor	**Promedio del tiempo de descifrado.**
Chen	387290,32 µs
Lorenz	287799,44 µs
Rossler	379987,72 µs
Sprott	301363,72 µs

Realizado por: Jemmy Puzma, 2023.

Análisis descriptivo

El siguiente Gráfico 19-4 muestra un análisis descriptivo del tiempo de descifrado de cada atractor.

```
> describeBy(tiempo_descif, atractord_id)

 Descriptive statistics by group
group: Chen
   vars  n    mean      sd  median trimmed     mad     min     max   range skew kurtosis
X1    1 25 3872903 2100520 2843170 3718522 1318535 1882040 7528830 5646790 0.64    -1.35
       se
X1 420104
------------------------------------------------------------------------
group: Lorenz
   vars  n    mean      sd  median trimmed      mad     min     max   range skew kurtosis
X1    1 25 2877994 2234226 1861930 2492892 242316.1 1646120 8133810 6487690 1.71     1.06
        se
X1 446845.2
------------------------------------------------------------------------
group: Rossler
   vars  n    mean      sd  median trimmed     mad     min     max   range skew kurtosis
X1    1 25 3799877 1218141 3820010 3746656 1373229 1782130 6879140 5097010 0.46    -0.36
        se
X1 243628.1
------------------------------------------------------------------------
group: Sprott
   vars  n    mean      sd  median trimmed    mad     min     max   range skew kurtosis
X1    1 25 3013637 2075647 2230620 2669528 465314 1788720 7988750 6200030  1.7     1.06
        se
X1 415129.3
```

Gráfico 19-4: Análisis descriptivo del tiempo de descifrado por cada atractor

Realizado por: Jemmy Puzma, 2023.

Chen tiene la mayor media de tiempo de descifrado con 3,872,903 microsegundos, seguido muy de cerca por Rossler con un tiempo promedio de 3,799,877 microsegundos. Esto indica que ambos atractores requieren un tiempo considerable para descifrar los datos en comparación con los demás.

Por otro lado, Lorenz y Sprott tienen un tiempo promedio de descifrado más rápido, siendo 2,877,994 y 3,013,637 microsegundos respectivamente. Aunque estos dos atractores son más eficientes en términos de tiempo de descifrado en comparación con Chen y Rossler, Lorenz parece ser el más eficiente de todos.

En conclusión, si se busca eficiencia en el tiempo de descifrado, Lorenz es la opción más atractiva, seguido de Sprott. Sin embargo, si se requiere consistencia en los tiempos de descifrado, Rossler es una opción preferible, esto podría ser beneficioso en un entorno donde es importante tener una buena idea de cuánto tiempo tomará el descifrado, ya que no hay muchas variaciones inesperadas.

Para el tiempo de descifrado se presenta un diagrama de caja, el cual presenta los siguientes resultados. Ver Gráfico 20-4.

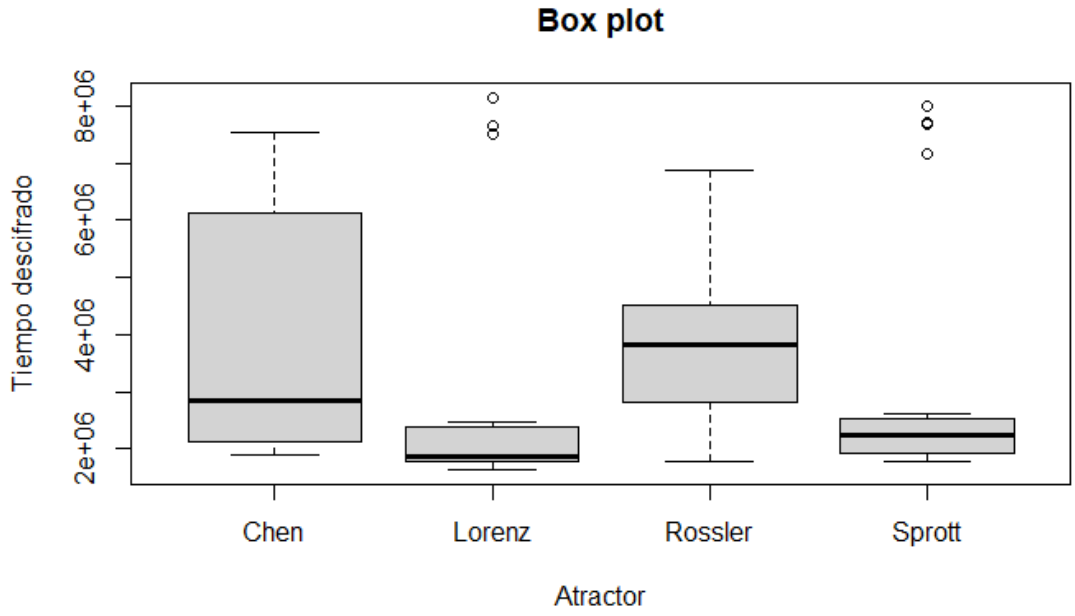


Gráfico 20-4: Diagrama de caja del tiempo de descifrado

Realizado por: Jemmy Puzma, 2023.

La mediana de los atractores está dividiendo la caja en partes desiguales de manera que Chen y Lorenz tiene una asimetría positiva, esto quiere decir que los datos se concentran en la parte inferior de la distribución y la media suele ser mayor que la mediana, en cambio Rossler y Sprott tienen una asimetría negativa, lo cual los datos se concentran en la parte superior de la distribución y la media suele ser menor que la mediana. También presentan algunos valores atípicos en Lorenz y Sprott.

A primera vista se determina que Chen proporciona la mayor cantidad del tiempo, lo que significa que es el más lento para descifrar cadenas de texto, Lorenz y Sprott se observa que son los más rápidos, ya que sus valores no difieren significativamente. Para corroborar la información se muestra a continuación un análisis inferencial. Ver Gráfico 21-4.

Análisis inferencial

En el análisis de varianza realizado llamado (anova3) dio como resultado un valor de p = 0.159, lo que muestra que existen atractores que no tienen mucha diferencia significativa. Se observa en el Gráfico 21-4.

```
> summary(anova3)
             Df    Sum Sq   Mean Sq F value Pr(>F)
atractord_id  3 2.012e+13 6.708e+12   1.766  0.159
Residuals    96 3.647e+14 3.799e+12
```

Gráfico 21-4: Valor de p del tiempo de descifrado

Realizado por: Jemmy Puzma, 2023.

En la prueba de Tukey se muestra los valores atractores que son similares.

```
> TukeyHSD(anova3)
  Tukey multiple comparisons of means
    95% family-wise confidence level

Fit: aov(formula = tiempo_descif ~ atractord_id)

$atractord_id
                    diff        lwr       upr     p adj
Lorenz-Chen    -994908.8 -2436319.7  446502.1 0.2774826
Rossler-Chen    -73026.0 -1514436.9 1368384.9 0.9991644
Sprott-Chen    -859266.0 -2300676.9  582144.9 0.4070744
Rossler-Lorenz  921882.8  -519528.1 2363293.7 0.3439655
Sprott-Lorenz   135642.8 -1305768.1 1577053.7 0.9947328
Sprott-Rossler -786240.0 -2227650.9  655170.9 0.4862781
```

Gráfico 22-4: Datos estadísticos de los atractores y tiempo descifrado

Realizado por: Jemmy Puzma, 2023.

Lorenz-Chen: La diferencia media en los tiempos de descifrado entre los atractores Lorenz y Chen es de -994908.8 microsegundos, lo que sugiere que el atractor de Lorenz es aproximadamente 1 segundo más rápido que el de Chen.

Rossler-Chen: La diferencia media entre Rossler y Chen es prácticamente nula, indicando que ambos atractores podrían tener un rendimiento muy similar en términos de tiempo de descifrado.

Sprott-Chen: Sprott parece es más rápido que Chen por un promedio de 859266 microsegundos o aproximadamente 0.86 segundos.

Rossler-Lorenz: Rossler es más lento que Lorenz en aproximadamente 0.92 segundos. Aunque este resultado podría ser importante en aplicaciones en tiempo real donde cada milisegundo cuenta, el valor p de 0.344 indica que no se puede estar seguro de esta diferencia.

Sprott-Lorenz y Sprott-Rossler: No hay evidencia suficiente para afirmar que Sprott tiene un rendimiento diferente al de Lorenz o Rossler, ya que los valores p son muy altos (p=0.994 y p=0.486, respectivamente).

En resumen, esto sugiere que los atractores no parecen diferir significativamente en sus tiempos de descifrado. Según lo analizado el atractor de Chen es el más lento para el descifrado por un segundo más que el de Rossler y el más eficiente es Lorenz.

Para tener una mejor visualización de los resultados se muestra un gráfico de barras generado desde la aplicación web. Gráfico 23-4.

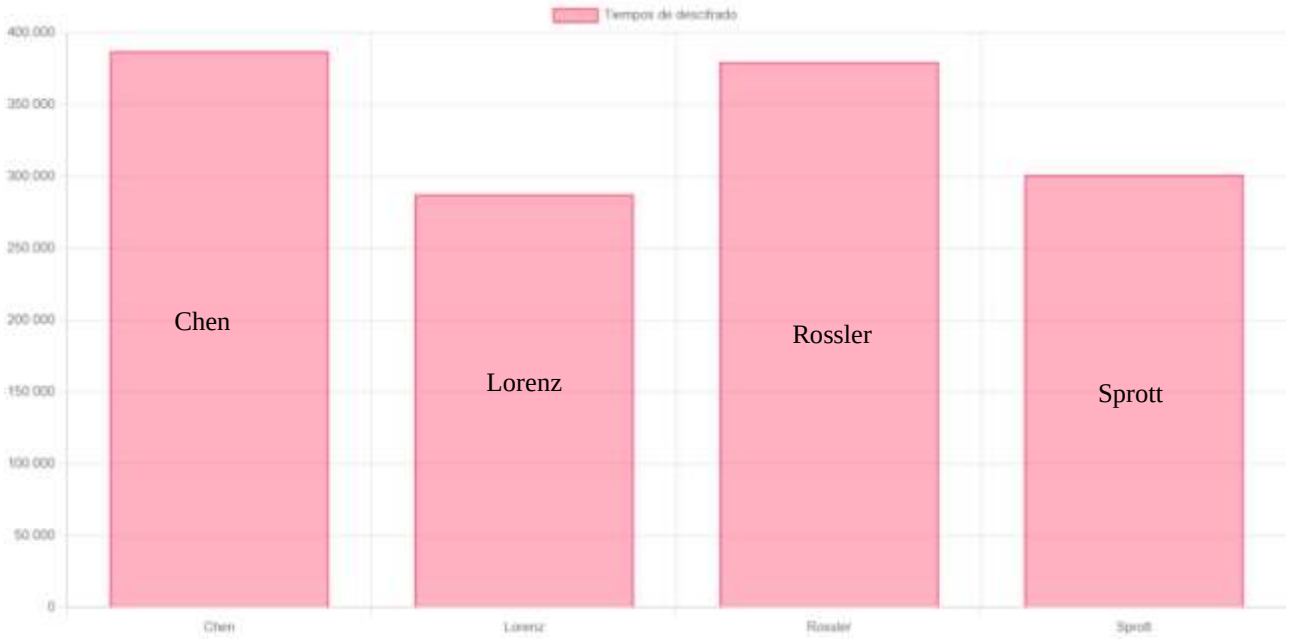


Gráfico 23-4: Gráfico de barras del tiempo de descifrado

Realizado por: Jemmy Puzma, 2023.

Se comprueba que existe una similitud entre los atractores, lo que indica que cualquier atractor es recomendado para realizar el descifrado.

Evaluación de supuestos del modelo

Se realiza una evaluación de supuestos del modelo para determinar si fue factible realizar un análisis de varianza, o de lo contrario utilizar una prueba no paramétrica.

Para los análisis se utiliza un nivel de significancia de 0.05.

Igualdad de varianzas

Se utilizó levenetest para observar si existe una igualdad en las varianzas. Ver Gráfico 24-4.

```
> leveneTest(tiempo_descif ~ atractord_id, descifradotabla3)
Levene's Test for Homogeneity of Variance (center = median)
      Df F value Pr(>F)
group  3  0.8316 0.4797
      96
```

Gráfico 24-4: Test de levene para el tiempo de descifrado

Realizado por: Jemmy Puzma, 2023.

Según la Prueba de Levene, no hay una diferencia significativa en la varianza del tiempo de descifrado entre los diferentes atractores en el conjunto de datos. Esto significa que la variabilidad del tiempo de descifrado es la misma para todos los atractores.

Normalidad de los residuos del modelo

En la prueba de normalidad de Lilliefors (Kolmogorov-Smirnov) se obtuvo lo siguiente Gráfico 25-4.

```
> lillie.test(standard_res2)

        Lilliefors (Kolmogorov-Smirnov) normality test

data:  standard_res2
D = 0.26212, p-value < 2.2e-16
```

Gráfico 25-4: Test de normalidad para el tiempo de descifrado

Realizado por: Jemmy Puzma, 2023.

El valor p de esta prueba es extremadamente bajo, menos de 2.2e-16 (esto es prácticamente cero). Un valor p muy bajo sugiere que se puede rechazar la hipótesis nula. En este caso, la hipótesis nula es que los datos siguen una distribución normal.

Según los resultados observados se determinó que es necesario realizar una prueba no paramétrica, en este caso se utiliza la prueba de Kruskal Wallis. Gráfico 26-4.

```
> kruskal.test(tiempo_descif ~ atractord_id, descifradotabla3)

        Kruskal-Wallis rank sum test

data:  tiempo_descif by atractord_id
Kruskal-Wallis chi-squared = 21.513, df = 3, p-value = 8.237e-05
```

Gráfico 26-4: Test de kruskal wallis del tiempo de descifrado

Realizado por: Jemmy Puzma, 2023.

Dado este valor p muy bajo (que es mucho menor que el nivel de significancia definido de 0.05), hay fuertes evidencias para rechazar la hipótesis de que los tiempos de descifrado son iguales para todos los atractores. Esto sugiere que al menos un atractor tiene un tiempo de descifrado mediano significativamente diferente a los demás.

4.1.3 *Resultados finales*

Una vez analizado los resultados de los tiempos de sincronización, cifrado y descifrado por cada atractor, se obtuvo que:

Tiempo de sincronización: Con un valor chi-cuadrado de 43.833 y un p-valor de 1.638e-09, hay evidencia suficiente para rechazar la hipótesis nula (H0) y concluir que hay diferencias significativas en el tiempo de sincronización entre al menos uno de los cuatro atractores.

Tiempo de cifrado: Con un valor chi-cuadrado de 39.107 y un p-valor de 1.647e-08, hay evidencia suficiente para rechazar la hipótesis nula (H0) y concluir que hay diferencias significativas en el tiempo de cifrado entre al menos uno de los cuatro atractores.

Tiempo de descifrado: Con un valor chi-cuadrado de 21.513 y un p-valor de 8.237e-05, hay evidencia suficiente para rechazar la hipótesis nula (H0) y concluir que hay diferencias significativas en el tiempo de descifrado entre al menos uno de los cuatro atractores.

En conclusión, los resultados de los tests Kruskal-Wallis para el tiempo de sincronización, cifrado y descifrado demuestran que se debe rechazar la hipótesis nula (H0) en favor de la hipótesis

alternativa (H1). Esto significa que al menos uno de los cuatro atractores difiere sustancialmente del resto en términos de tiempo de sincronización, cifrado y descifrado.

4.2 Evaluación de confidencialidad

Los resultados que se obtuvieron se basaron en una cadena de texto de 118 caracteres. Observar **Anexo G.**

4.2.1 *Atractor Rossler*

En el Gráfico 27-4 se observa la dispersión en donde se compara los valores, **Anexo I,** de cada caracter del texto plano con el texto cifrado.

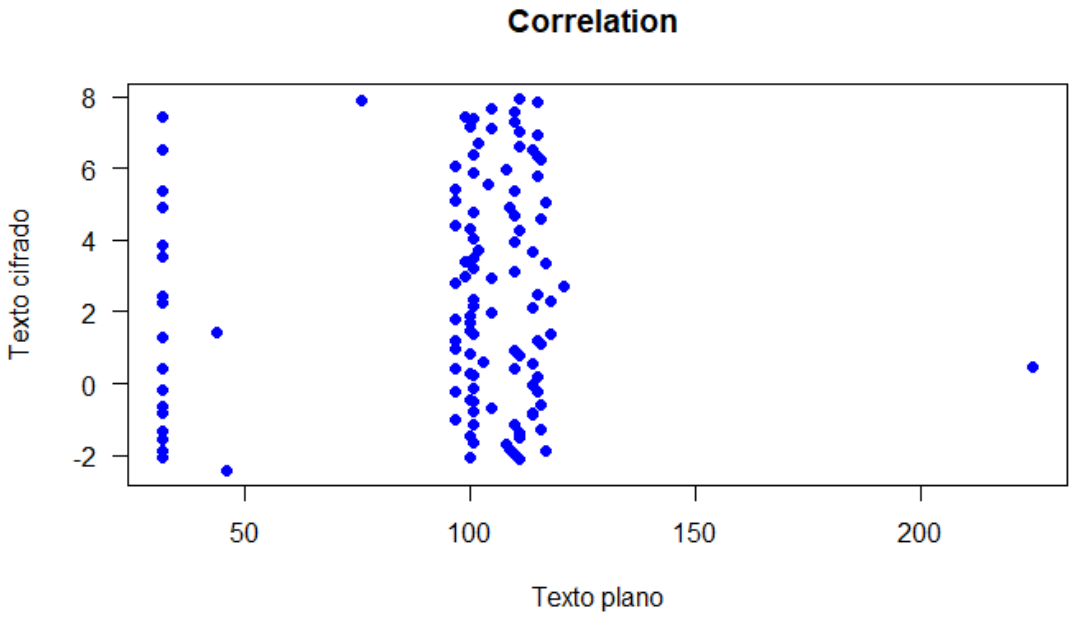


Gráfico 27-4: Gráfico de correlación entre la información del texto plano y cifrado del atractor de Rossler

Realizado por: Jemmy Puzma, 2023.

Se puede prestar atención que no tiene ninguna relación el texto plano y el texto cifrado, por lo que se determina que no existen patrones en los que se pueda lograr descifrar el mensaje sin conocer la llave.

El coeficiente de correlación de Pearson calculado fue de 0,08 con un valor p no significativo de 0,38, lo que sugiere que no hay evidencia suficiente para afirmar que existe una correlación lineal entre texto plano y texto cifrado. El coeficiente de correlación Pearson se muestra en el Gráfico 28-4.

```
> cor.test(texto_plano, texto_cifrado, method = "pearson")

        Pearson's product-moment correlation

data:  texto_plano and texto_cifrado
t = 0.87682, df = 116, p-value = 0.3824
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 -0.1011004  0.2581153
sample estimates:
      cor
0.0811418
```

Gráfico 28-4: Coeficiente de correlación de Pearson del atractor de Rossler calculado

Realizado por: Jemmy Puzma, 2023.

A continuación, se muestra el Gráfico 29-4 con la información, **Anexo I**, del texto plano y el texto regenerado después del proceso de descifrado.

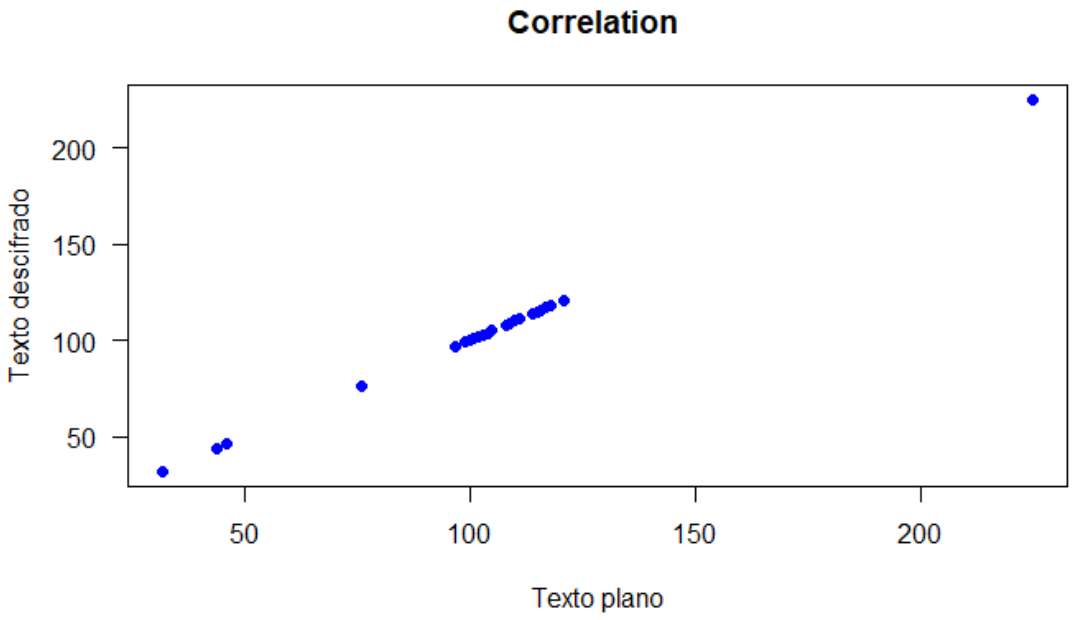


Gráfico 29-4: Gráfico de correlación de la información del texto plano y el texto regenerado después del descifrado

Realizado por: Jemmy Puzma, 2023.

El texto se regenera por completo sin perder información después de descifrarse el mensaje. Se observó un coeficiente de correlación de 1, lo que indica que hay total similitud entre el mensaje original y el descifrado. A continuación, se muestra el coeficiente calculado. Ver Gráfico 30-4.

```
> cor.test(texto_plano, texto_descifrado, method = "pearson")

        Pearson's product-moment correlation

data:  texto_plano and texto_descifrado
t = 57475, df = 116, p-value < 2.2e-16
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 1 1
sample estimates:
cor
  1
```

Gráfico 30-4: Coeficiente de Pearson entre el texto original y el descifrado

Realizado por: Jemmy Puzma, 2023.

4.2.2 *Atractor Lorenz*

En el Gráfico 31-4 se observa el gráfico de dispersión en donde se compara los valores, **Anexo I,** de cada carácter del texto plano con el texto cifrado.

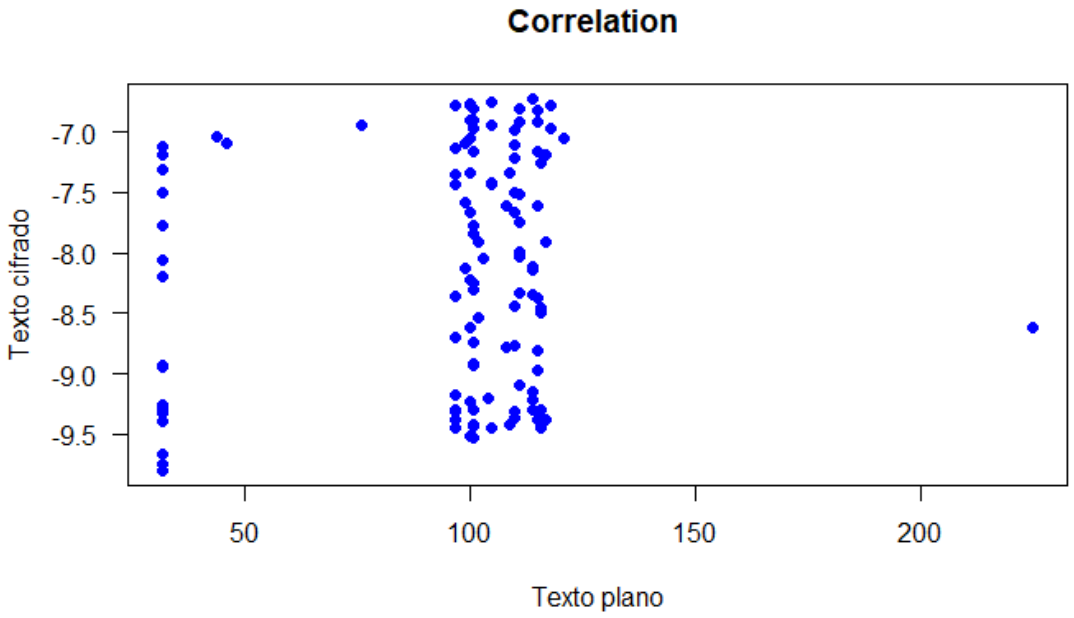


Gráfico 31-4: Gráfico de correlación de la información del texto plano y descifrado del atractor de Lorenz

Realizado por: Jemmy Puzma, 2023.

Se puede prestar atención que no tiene ninguna relación el texto plano y el texto cifrado, por lo que se determina que no existen patrones en los que se pueda lograr descifrar el mensaje sin conocer la llave.

El coeficiente de correlación de Pearson calculado fue de 0,10 con un valor p no significativo de 0,27, lo que sugiere que no hay evidencia suficiente para afirmar que existe una correlación lineal entre texto plano y texto cifrado. El coeficiente de correlación Pearson se muestra en el Gráfico 32-4.

```
> cor.test(texto_planoL, texto_cifradoL, method = "pearson")

        Pearson's product-moment correlation

data:  texto_planoL and texto_cifradoL
t = 1.1079, df = 116, p-value = 0.2702
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 -0.07991207  0.27794379
sample estimates:
      cor
0.1023254
```

Gráfico 32-4: Coeficiente de correlación Pearson con el atractor de Lorenz

Realizado por: Jemmy Puzma, 2023.

A continuación, se muestra el Gráfico 33-4 con la información, **Anexo I**, del texto plano y el texto regenerado después del proceso de descifrado.

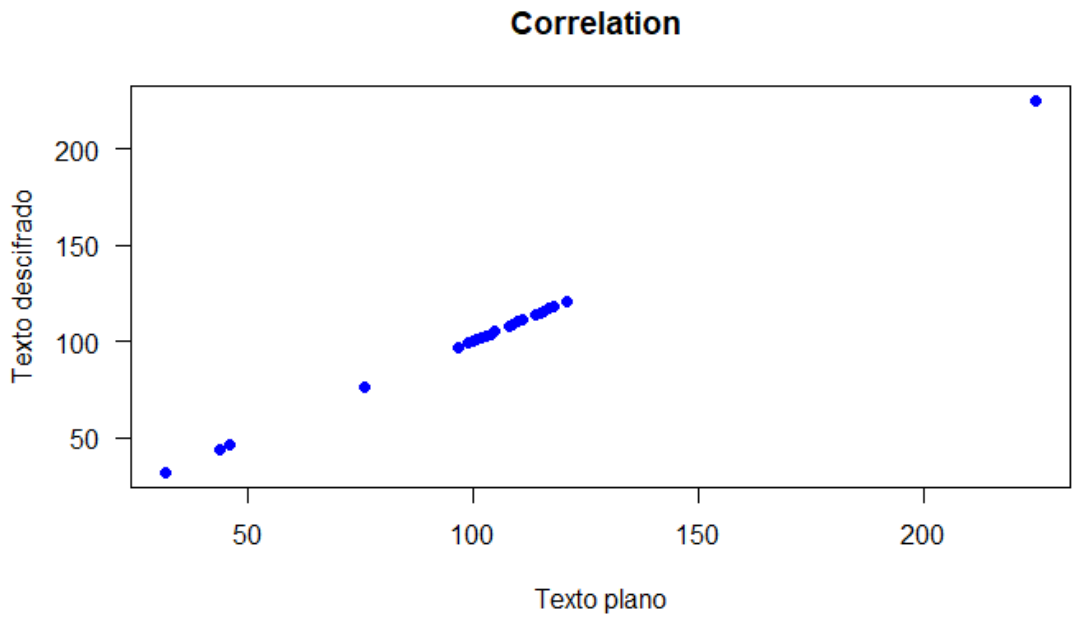


Gráfico 33-4: Gráfico de correlación del texto plano y el texto regenerado con el atractor de Lorenz

Realizado por: Jemmy Puzma, 2023.

El texto se regenera sin perder información después de descifrarse el mensaje. Se observó un coeficiente de correlación de 1, lo que indica que hay similitud entre el mensaje original y el descifrado. A continuación, se muestra el coeficiente calculado. Ver Gráfico 34-4.

```
> cor.test(texto_planoL, texto_descifradoL, method = "pearson")

        Pearson's product-moment correlation

data:  texto_planoL and texto_descifradoL
t = 57475, df = 116, p-value < 2.2e-16
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 1 1
sample estimates:
cor
  1
```

Gráfico 34-4: Coeficiente de correlación de Pearson con el atractor de Lorenz

Realizado por: Jemmy Puzma, 2023.

4.2.3 *Atractor de Chen*

En el Gráfico 35-4 se observa el gráfico de dispersión en donde se compara los valores, **Anexo I,** de cada carácter del texto plano con el texto cifrado.

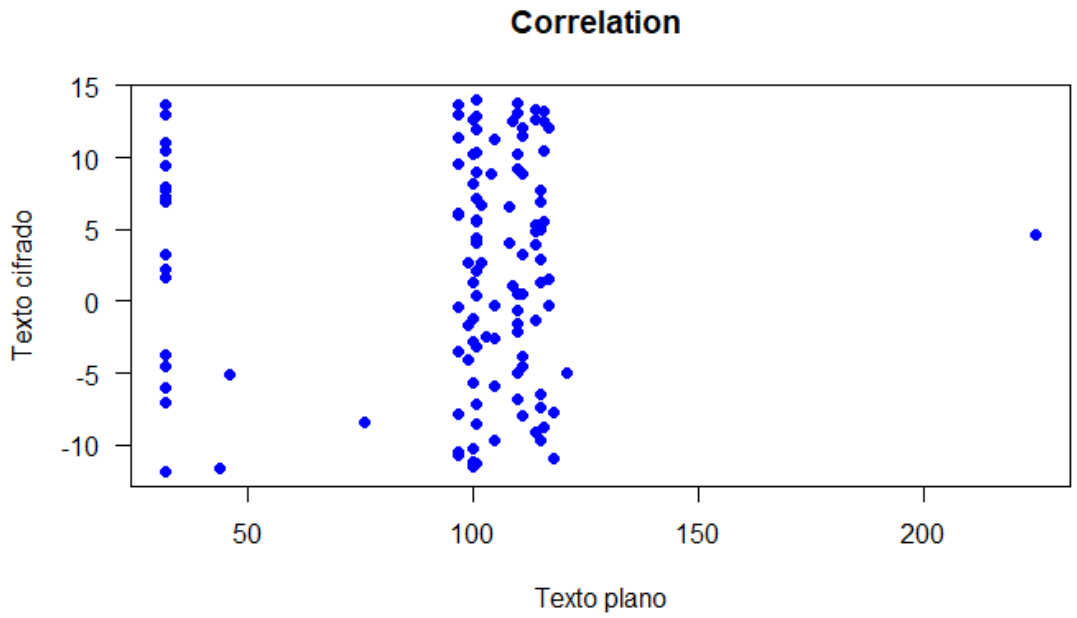


Gráfico 35-4: Gráfico de correlación con el texto plano y texto cifrado del atractor de Chen

Realizado por: Jemmy Puzma, 2023.

Se puede prestar atención que no tiene ninguna relación el texto plano y el texto cifrado, por lo que se determina que no existen patrones en los que se pueda lograr descifrar el mensaje sin conocer la llave.

El coeficiente de correlación de Pearson calculado fue de 0,0028 con un valor p no significativo de 0,97, lo que sugiere que no hay evidencia suficiente para afirmar que existe una correlación lineal entre texto plano y texto cifrado. El coeficiente de correlación Pearson se muestra en el Gráfico 36-4.

```
> cor.test(texto_planoC, texto_cifradoC, method = "pearson")

        Pearson's product-moment correlation

data:  texto_planoC and texto_cifradoC
t = 0.030538, df = 116, p-value = 0.9757
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 -0.1780153  0.1835006
sample estimates:
        cor
0.002835329
```

Gráfico 36-4: Coeficiente de Pearson con el atractor de Chen

Realizado por: Jemmy Puzma, 2023.

A continuación, se muestra el Gráfico 37-4 con la información, **Anexo I**, del texto plano y el texto regenerado después del proceso de descifrado.

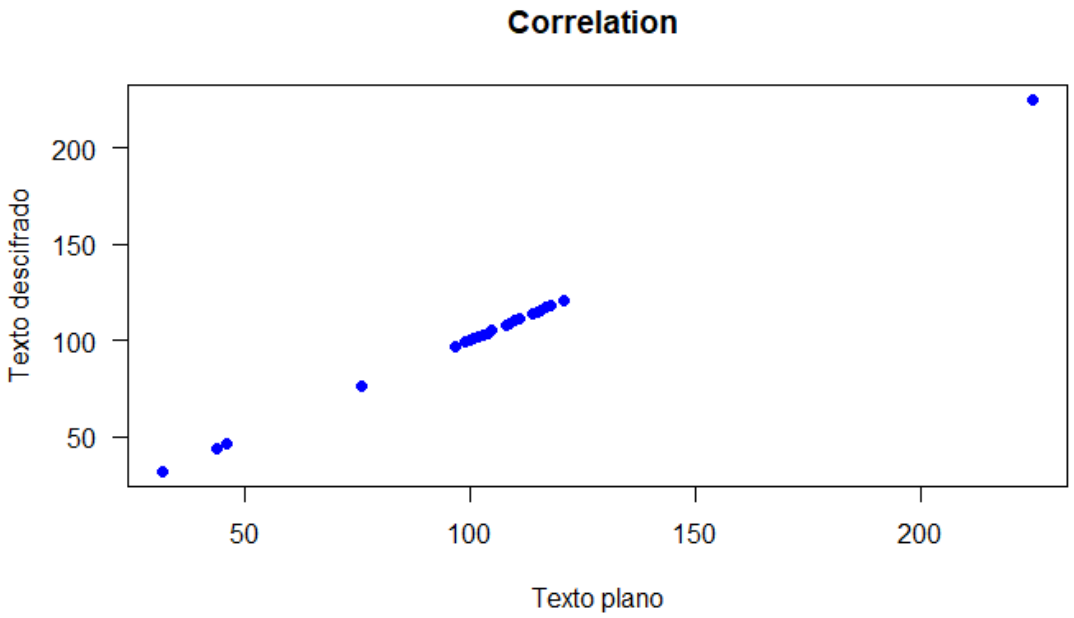


Gráfico 37-4: Gráfico de correlación entre el texto plano y descifrado del atractor de Chen

Realizado por: Jemmy Puzma, 2023.

El texto se regenera por completo sin perder información después de descifrarse el mensaje. Se observó un coeficiente de correlación de 1, lo que indica que hay total similitud entre el mensaje original y el descifrado. A continuación, se muestra el coeficiente calculado. Ver Gráfico 38-4.

```
> cor.test(texto_planoC, texto_descifradoC, method = "pearson")

        Pearson's product-moment correlation

data:  texto_planoC and texto_descifradoC
t = 57475, df = 116, p-value < 2.2e-16
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 1 1
sample estimates:
cor
  1
```

Gráfico 38-4: Coeficiente de correlación de Pearson con el atractor de Chen

Realizado por: Jemmy Puzma, 2023.

4.2.4 *Atractor de Sprott*

En el Gráfico 39-4 se observa el gráfico de dispersión en donde se compara los valores, **Anexo I,** de cada carácter del texto plano con el texto cifrado.

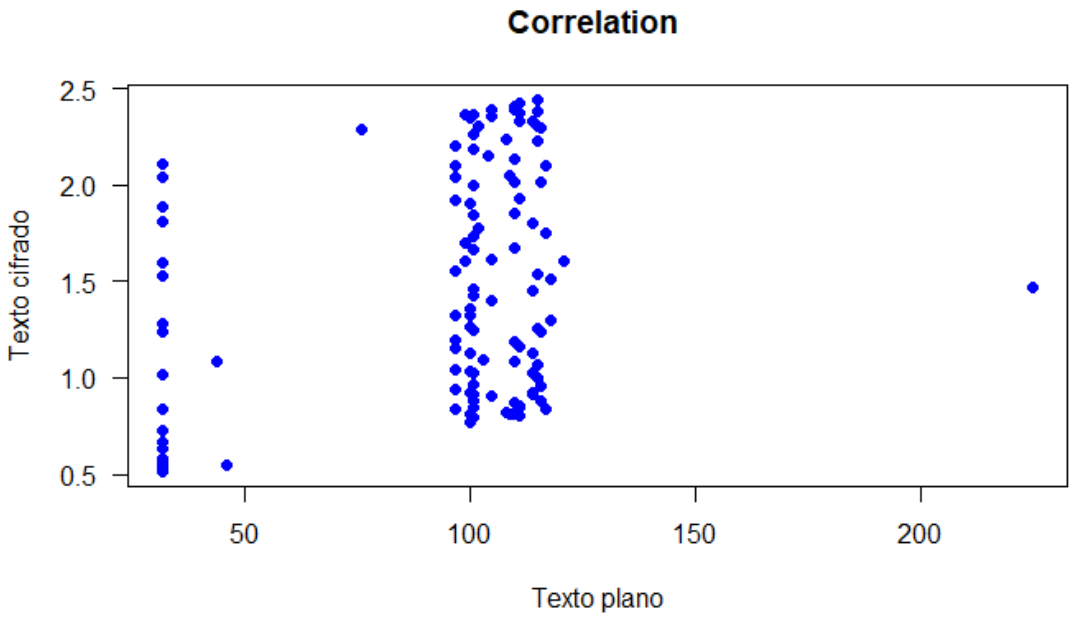


Gráfico 39-4: Gráfico de correlación de la información del texto plano con cifrado de Sprott

Realizado por: Jemmy Puzma, 2023.

Así como en los atractores anteriores, se observa que no tiene ninguna relación el texto plano y el texto cifrado, por lo que se determina que no existen patrones en los que se pueda lograr descifrar el mensaje sin conocer la llave.

El coeficiente de correlación de Pearson calculado fue de 0,24 con un valor p no significativo de 0,008, lo que sugiere que no hay evidencia suficiente para afirmar que existe una correlación lineal entre texto plano y texto cifrado. El coeficiente de correlación Pearson se muestra en el Gráfico 40-4.

```
> cor.test(texto_planoS, texto_cifradoS, method = "pearson")

        Pearson's product-moment correlation

data:  texto_planoS and texto_cifradoS
t = 2.6684, df = 116, p-value = 0.008713
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 0.0624356 0.4036921
sample estimates:
      cor
0.2404809
```

Gráfico 40-4: Coeficiente de Pearson con la información del texto plano y cifrado del atractor Rossler

Realizado por: Jemmy Puzma, 2023.

A continuación, se muestra el Gráfico 41-4 con la información, **Anexo I**, del texto plano y el texto regenerado después del proceso de descifrado.

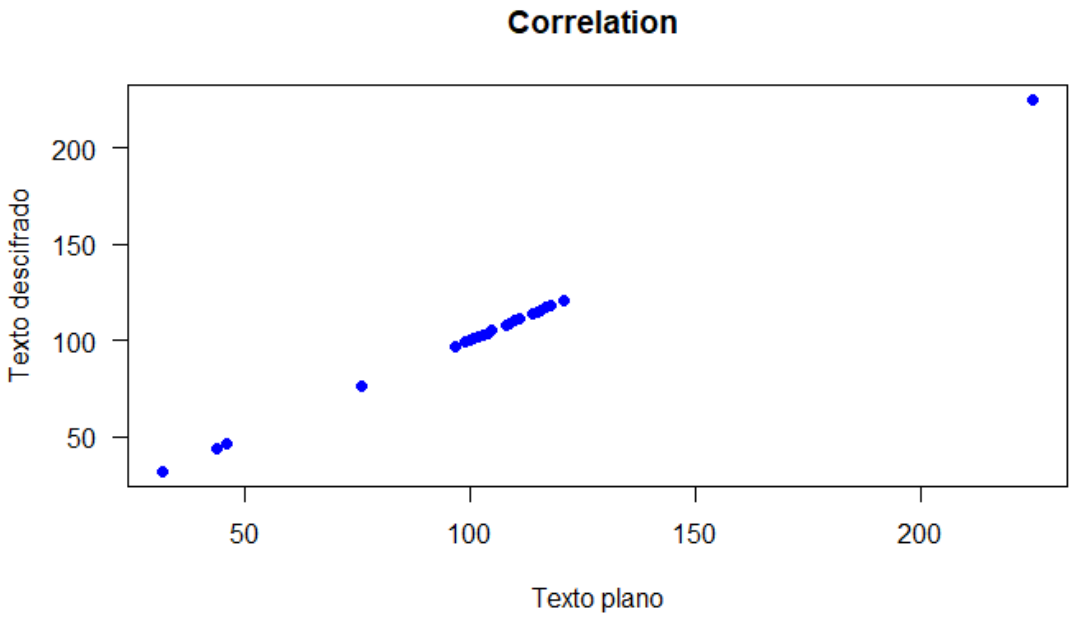


Gráfico 41-4: Gráfico de correlación de la información del texto plano y el regenerado del atractor Sprott

Realizado por: Jemmy Puzma, 2023.

El texto se regenera por completo sin perder información después de descifrarse el mensaje. Se observó un coeficiente de correlación de 1, lo que indica que hay total similitud entre el mensaje original y el descifrado. A continuación, se muestra el coeficiente calculado. Ver Gráfico 42-4.

```
> cor.test(texto_planoS, texto_descifradoS, method = "pearson")

        Pearson's product-moment correlation

data:  texto_planoS and texto_descifradoS
t = 57475, df = 116, p-value < 2.2e-16
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 1 1
sample estimates:
cor
  1
```

Gráfico 42-4: Coeficiente de Pearson de la información del texto plano y el regenerado en el atractor de Rossler

Realizado por: Jemmy Puzma, 2023.

CAPÍTULO V:

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El presente trabajo se centró en el DESARROLLO DE UNA APLICACIÓN WEB PARA EL CIFRADO Y DESCIFRADO DE CADENAS DE TEXTO A PARTIR DE LA SELECCIÓN DE UN ATRACTOR CAÓTICO. A continuación, se resumen los hallazgos principales y las conclusiones derivadas del estudio.

- A lo largo del estudio, se efectuó un análisis minucioso de cuatro sistemas caóticos esenciales: Rossler, Lorenz, Chen y Sprott. Cada sistema, con su atractor característico y comportamiento dinámico, desempeña un papel vital en la comprensión del caos. Desde la estructura en espiral del Rossler, pasando por el icónico atractor con forma de "mariposa" de Lorenz, hasta las complejidades distintivas de Chen y Sprott, estos sistemas se han destacado por su naturaleza impredecible y altamente sensible a las condiciones iniciales. Esta singularidad y complejidad los convierten en herramientas poderosas, subrayando su significado y aplicabilidad en el mundo del cifrado y descifrado. La revisión de estos sistemas no solo ha permitido un entendimiento profundo del caos, sino que también ha establecido un fundamento sólido para futuras aplicaciones y estudios en el campo de la seguridad cibernética.

- Más allá de una mera revisión teórica, el estudio se adentró en la práctica, llevando a cabo un proceso de sincronización caótica para cada uno de estos atractores. Los resultados revelaron detalles interesantes y esenciales para la implementación práctica de estos sistemas en la ciberseguridad. A través del uso del test Kruskal-Wallis, se pudo determinar diferencias significativas en los tiempos de sincronización entre los atractores. El atractor de Lorenz, con su complejo comportamiento y estructura, emergió como el más eficiente en términos de sincronización, lo que sugiere su gran potencial en aplicaciones de cifrado. Estos hallazgos no solo fortalecen la comprensión del comportamiento caótico, sino que también guían futuras investigaciones y aplicaciones en áreas críticas como la seguridad cibernética.

- El desarrollo de la aplicación web representó un desafío técnico y metodológico, que se abordó con éxito mediante el empleo de SCRUMBAN como metodología de trabajo. SCRUMBAN combina elementos de SCRUM y Kanban, dos enfoques ágiles que promueven la flexibilidad, adaptabilidad y eficiencia en la producción. Gracias a SCRUMBAN, el equipo de desarrollo pudo mantener un flujo constante de trabajo, adaptándose a cambios inesperados

y optimizando el proceso mediante la revisión y adaptación constante. El tablero Kanban, característico de esta metodología, ofreció una visión clara del progreso del proyecto, mientras que las iteraciones cortas al estilo SCRUM aseguraron la entrega continua de características valiosas y el ajuste oportuno basado en retroalimentaciones. Esta combinación resultó esencial para la adaptabilidad del equipo ante requisitos cambiantes y desafíos técnicos. Como resultado, se produjo una aplicación web robusta y funcional que se destaca no solo por su capacidad técnica sino también por su interfaz amigable y eficiente. La plataforma resultante es una herramienta inestimable que permite el cifrado y descifrado de cadenas de texto a través de la sincronización caótica, facilitando así una mayor seguridad y confiabilidad en la transmisión de información. La adopción de SCRUMBAN en este proyecto no solo reitera la importancia de las metodologías ágiles en el mundo del desarrollo de software actual, sino que también demuestra su eficacia en la creación de soluciones innovadoras y de alto impacto.

- Se llevó a cabo una evaluación rigurosa de la eficiencia y seguridad en el cifrado y descifrado en la aplicación desarrollada. Los análisis de tiempo revelaron diferencias significativas entre los atractores, subrayando la necesidad de equilibrar la velocidad y la seguridad en la elección de los métodos de cifrado. Quedando como el más eficiente en el cifrado y descifrado el atractor de Lorenz.

5.2 Recomendaciones

Este estudio y el desarrollo subsiguiente representan una valiosa contribución al campo de la seguridad informática y la criptografía. La aplicación actual se enfoca en el cifrado y descifrado de cadenas de texto.

Se recomienda extender esta tecnología a otros medios, como audios, imágenes y videos. La exploración de algoritmos y técnicas para manejar estos tipos de datos podría abrir nuevas avenidas para la protección y la seguridad en la comunicación multimedia.

Si bien este trabajo se centró en cuatro atractores específicos, hay una rica variedad de sistemas caóticos que podrían explorarse. La práctica con diferentes atractores podría revelar características únicas y beneficios adicionales en términos de eficiencia y seguridad. El análisis comparativo de diferentes atractores puede brindar una visión más completa de la aplicabilidad de la teoría del caos en la criptografía.

BIBLIOGRAFÍA

3DIGITS, S. de I.I., 2019. 3digits – Tenemos una solución – Tecnologías de la Información. [en línea]. [consulta: 21 enero 2023]. Disponible en: https://www.3digits.es/blog/Ventajas-lenguaje-JAVA.html. Palma, Mallorca, España

AGENCY, M.D., 2021. Qué es Flask (Python) y cuáles son sus principales ventajas. *Epitech Spain* [en línea]. [consulta: 2 junio 2023]. Disponible en: https://www.epitech-it.es/flask-python/.

AL-AZZAWI, S. y ABED, K.A., 2011. Using Δ - Discriminate Method to Determine the Stability and Bifurcation of Chen Chaotic System. *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. 8, DOI 10.33899/csmj.2011.163646.

ALVAREZ, M., 2003. Qué es Python. *Que es Python* [en línea]. [consulta: 21 enero 2023]. Disponible en: https://desarrolloweb.com/articulos/1325.php.

ARIAS, R., 2022. Sistema Criptográfico Caótico. [en línea]. [consulta: 13 diciembre 2022]. Disponible en: https://cnx.org/contents/q2WA_v07@1/Sistema-Criptogr%C3%A1fico-Ca%C3%B3tico.

ASOCIACIÓN NACIONAL DE ESTUDIANTES UNIVERSITARIOS DE CIENCIAS FÍSICAS, 2018. Sistemas caóticos y teoría del caos, una breve introducción - NUSGREM. *NUSGREM - Asociacion Nacional de Estudiantes de Física* [en línea]. [consulta: 8 diciembre 2022]. Disponible en: https://nusgrem.es/sistemas-caoticos-y-teoria-del-caos/.

AYUDALEY, 2023. Qué es PostgreSQL y sus principales ventajas. *Ayuda Ley Protección Datos* [en línea]. [consulta: 21 enero 2023]. Disponible en: https://ayudaleyprotecciondatos.es/bases-de-datos/que-es-postgresql-ventajas/.

BAPTISTE, B., 2018. Atractores: una explicación científica de la casualidad. [en línea]. [consulta: 8 diciembre 2022]. Disponible en: https://divulgacion.minciencias.gov.co/atractores.

BEA MONREAL, C., 2020. *Criptografía de clave simétrica y de clave asimétrica* [en línea]. 27 julio 2020. S.l.: s.n. Disponible en: https://repositori.uji.es/xmlui/bitstream/handle/10234/192200/TFG_2019_beaC.pdf?sequence=1&isAllowed=y.

BILLWAGNER, 2023. Un paseo por C#: información general. [en línea]. [consulta: 21 enero 2023]. Disponible en: https://learn.microsoft.com/es-es/dotnet/csharp/tour-of-csharp/.

BORONDO, F., 2022. Un paradigma multidisciplinar. [en línea]. S.l.: s.n., DOI https://repositorio.uam.es/bitstream/handle/10486/684812/EM_7_2.pdf?sequence=1&isAllowed=y. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/684812/EM_7_2.pdf?sequence=1&isAllowed=y.

BYTES, V., 2020. Características del MySQL: (Ventajas y desventajas). *VidaBytes* [en línea]. [consulta: 31 diciembre 2022]. Disponible en: https://vidabytes.com/caracteristicas-del-mysql/.

CAMPUZANO, J.C.P., 2018. Strange Attractors. *Strange Attractors* [en línea]. [consulta: 12 enero 2023]. Disponible en: https://jcponce.github.io/.

CHEN, G. y UETA, T., 1999. Yet Another Chaotic Attractor. *International Journal of Bifurcation and Chaos - IJBC*, vol. 9, DOI 10.1142/S0218127499001024.

CITY UNIVERSITY OF HONG KONG., 2023. Guanrong CHEN - CityU Scholars | A Research Hub of Excellence. [en línea]. [consulta: 29 mayo 2023]. Disponible en: https://scholars.cityu.edu.hk/en/persons/guanrong-chen(b84391cb-7b0f-4948-bdf3-15dfb75b9307).html.

CORDOVA RAMIREZ, J., **VEGA HUERTA, H., RODRIGUEZ RODRIGUEZ, C. y ESCOBEDO BAILÓN, F.**, 2020. Firma digital basada en criptografía asimétrica para generación de historial clínico. *3C Tecnología_Glosas de innovación aplicadas a la pyme*, ISSN 22544143. DOI 10.17993/3ctecno/2020.v9n4e36.65-85.

DÍAZ SORIANO, A., 2022. QC2. [en línea]. [consulta: 26 noviembre 2022]. Disponible en: https://www.uco.es/organiza/departamentos/quimica-fisica/quimica-fisica/MC/QC2.htm.

FIBK, 2018. En 2025 el volumen de datos será 175 veces más que en 2011. *Fundación Innovación Bankinter* [en línea]. [consulta: 9 enero 2023]. Disponible en: https://www.fundacionbankinter.org/noticias/en-2025-el-volumen-de-datos-en-el-mundo-sera-175-veces-mas-que-en-2011/.

FRIDRICH, J., 2011. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos* [en línea], [consulta: 26 noviembre 2022]. DOI 10.1142/S021812749800098X. Disponible en: https://www.worldscientific.com/doi/epdf/10.1142/S021812749800098X. world

FUSTER SABATER, A., HERNÁNDEZ ENCINAS, L., MONTOYA VITINI, F. y MUÑOZ MASQUE, J., 2012. Criptografía, protección de datos y aplicaciones. Una guía para estudiantes y profesionales - Grupo Editorial RA-MA. [en línea]. [consulta: 26 noviembre 2022]. Disponible en: https://www.ra-ma.es/libro/criptografia-proteccion-de-datos-y-aplicaciones-una-guia-para-estudiantes-y-profesionales_48492/, https://www.ra-ma.es/libro/criptografia-proteccion-de-datos-y-aplicaciones-una-guia-para-estudiantes-y-profesionales_48492/.

GERVACIO OLARTE, L., 2018. Lenguaje de Programación. *Conogasi* [en línea]. [consulta: 21 enero 2023]. Disponible en: https://conogasi.org/articulos/lenguaje-de-programacion/.

GITNUX, 2023. Metodología Scrum: qué es y cómo aplicarla • GITNUX. [en línea]. [consulta: 29 mayo 2023]. Disponible en: https://blog.gitnux.com/es/metodologia-scrum/.

GÓMEZ, O.S., ROSERO MIRANDA, R., ESTRADA-GUTIÉRREZ, J. y JIMÉNEZ-RODRÍGUEZ, M., 2022. An Approach for Securing JSON Objects through Chaotic Synchronization. *Cybernetics and Information Technologies*, vol. 22, DOI 10.2478/cait-2022-0037.

GUERRERO, B., 2004. SOBRE LA AXIOMATIZACIÓN EN MATEMÁTICAS. *Boletín de Matemáticas*, vol. 11, no. 1, ISSN 2357-6529.

HERNÁNDEZ ENCINAS, L., 2016. *La criptografía* [en línea]. S.l.: Editorial CSIC Consejo Superior de Investigaciones Científicas. [consulta: 11 enero 2023]. ISBN 978-84-00-10046-9. Disponible en: https://elibro.net/es/ereader/espoch/41843?page=83.

HOSTGATOR, 2023. SQLite: qué es, cómo funciona y cuál es la diferencia con MySQL. [en línea]. [consulta: 2 junio 2023]. Disponible en: https://www.hostgator.mx/blog/sqlite-que-es-y-diferencias-con-mysql/.

IBANEZ, C.A., 2005. Identificacio´n del sistema de Ro¨ssler: enfoque algebraico y algoritmos gene´ticos. ,

IBARRA GUZMÁN, D., CASTAÑEDAS ISLAS, U., PEREZ CORONA, C. y PEDROZA MÉNDEZ, B., 2014. Metodología ágil scrumban en el proceso de desarrollo y mantenimiento de software de la norma moprosoft - PDF Descargar libre. [en línea]. [consulta: 13 enero 2023]. Disponible en: https://docplayer.es/1449365-Metodologia-agil-scrumban-en-el-proceso-de-desarrollo-y-mantenimiento-de-software-de-la-norma-moprosoft.html.

INESEM, 2019. Los gestores de bases de datos (SGBD) más usados. *Canal Informática y TICS* [en línea]. [consulta: 21 enero 2023]. Disponible en: https://www.inesem.es/revistadigital/informatica-y-tics/los-gestores-de-bases-de-datos-mas-usados/.

ISO, 2023. ISO 25010. [en línea]. [consulta: 25 abril 2023]. Disponible en: https://iso25000.com/index.php/normas-iso-25000/iso-25010.

JAFARI, S., SPROTT, J.C. y NAZARIMEHR, F., 2015. Recent new examples of hidden attractors. *The European Physical Journal Special Topics*, vol. 224, no. 8, ISSN 1951-6355, 1951-6401. DOI 10.1140/epjst/e2015-02472-1.

JARROBA, R. [Admin, 2012. Modelo "4+1" vistas de Kruchten (para Dummies). *Jarroba* [en línea]. [consulta: 6 junio 2023]. Disponible en: https://jarroba.com/modelo-41-vistas-de-kruchten-para-dummies/.

JAVA, 2023. ¿Qué es Java y por qué lo necesito? [en línea]. [consulta: 21 enero 2023]. Disponible en: https://www.java.com/es/download/help/whatis_java.html.

KNIBERG, H. y SKARIN, M., 2010. *Kanban and Scrum: making the most of both*. s. l.: C4Media. InfoQ enterprise software development series, ISBN 978-0-557-13832-6.

LACOMBA, E., 2000. *Los sistemas dinámicos, ¿Qué son? y ¿Para qué sirven?* [en línea]. 2000. S.l.: s.n. Disponible en: https://miscelaneamatematica.org/download/tbl_articulos.pdf2.916ba74cb3eb6d5f.4c61636f6d62612e706466.pdf.

LAI, Q. y CHEN, S., 2016. Generating Multiple Chaotic Attractors from Sprott B System. *International Journal of Bifurcation and Chaos*, vol. 26, DOI 10.1142/S0218127416501777.

LENGUAJESDEPROGRAMACIÓN, 2023. ▷ Todo sobre el lenguaje de programación C# 【2023】. *Lenguajes de programación* [en línea]. [consulta: 21 enero 2023]. Disponible en: https://lenguajesdeprogramacion.net/c-sharp/.

LIBRARY, 2022. Encriptación caótica - Sistemas caoticos aplicados en telecomunicaciones. [en línea]. [consulta: 12 diciembre 2022]. Disponible en: https://1library.co/article/encriptaci%C3%B3n-ca%C3%B3tica-sistemas-caoticos-aplicados-en-telecomunicaciones.4yrk9gvz.

LLAMUCA-QUINALOA, J., VERA-VINCENT, Y. y TAPIA-CERDA, V., 2021. Análisis comparativo para medir la eficiencia de desempeño entre una aplicación web tradicional y una aplicación web progresiva. *TecnoLógicas*, vol. 24, no. 51, ISSN 2256-5337, 0123-7799. DOI 10.22430/22565337.1892.

LOMBARDI, O., 2020. La teoría del caos y el problema del determinismo. ,

LÜ, J., CHEN, G. y ZHANG, S., 2002. The compound structure of a new chaotic attractor. *Chaos, Solitons & Fractals*, vol. 14, no. 5, ISSN 0960-0779. DOI 10.1016/S0960-0779(02)00007-3.

MARTÍNEZ, D., 2022. 4.2- Cifrado de la clave simétrica. - SEGURIDAD INFORMÁTICA. [en línea]. [consulta: 29 mayo 2023]. Disponible en: https://sites.google.com/site/seguridadinformaticadavid/tema-4---criptografia/4-2--cifrado-de-la-clave-simetrica.

MOHAMMAD, A., 2022. Fig. 5 The Discrete version of Rössler attractor based on equations 15-17. *ResearchGate* [en línea]. [consulta: 13 diciembre 2022]. Disponible en: https://www.researchgate.net/figure/The-Discrete-version-of-Roessler-attractor-based-on-equations-15-17_fig3_258106019.

MONTALVÁN, C.E.R., 2019. Desarrollo de un mecanismo de cifrado basado en el algoritmo criptográfico simétrico aes. ,

MORENO, J., PARRA, F., HUÉRFANO, R., SUAREZ, C. y AMAYA, I., 2016. Modelo de Encriptación Simétrica Basada en Atractores Caóticos. *Ingeniería*, vol. 21, no. 3,

MORIELLO, S., 2003. SISTEMAS COMPLEJOS, CAOS Y VIDA ARTIFICIAL. ,

NUMERENTUR.ORG, 2018. Cifrado en bloque I – Numerentur.org. [en línea]. [consulta: 29 mayo 2023]. Disponible en: https://numerentur.org/cifrado-en-bloque/.

OPENWEBINARS, 2020. Qué es un lenguaje de programación. *OpenWebinars.net* [en línea]. [consulta: 21 enero 2023]. Disponible en: https://openwebinars.net/blog/que-es-un-lenguaje-de-programacion/.

ORÚE LÓPEZ, A.B.O., 2013. Contribución al estudio del criptoanálisis y diseño de los criptosistemas caóticos. ,

PACHECO CRUZ, E., 2019. Atarctor de Lorenz y Rossler | PDF | Teoría del caos | Atractor. *Scribd* [en línea]. [consulta: 30 diciembre 2022]. Disponible en: https://es.scribd.com/document/398824115/Atarctor-de-Lorenz-y-Rossler.

PADRÓN-GODÍNEZ, A., PRIETO MELÉNDEZ, R., BECERRA, A. y CALVA, G., 2015. VERIFICACIÓN DE LA IMPLEMENTACIÓN DE UN ALGORITMO DE FLUJO PARA MENSAJERÍA CELULAR: SECUENCIAS PSEUDOALEATORIAS. . S.l.: s.n.,

PAREDES, G., 2023. *Los Flujos Caóticos Más Simples (FCMS) Un mito entre lo complejo y lo complicado* [en línea]. 2023. S.l.: s.n. Disponible en: http://casanchi.org/mat/flujoscaoticos01.pdf.

RIBERO MEDINA, R. y RAMIREZ GÓMEZ, M., 1992. Caos: Definición, Detección y Ejemplos. [en línea], DOI https://revistas.uniandes.edu.co/doi/pdf/10.13043/dys.30.7. Disponible en: https://revistas.uniandes.edu.co/doi/pdf/10.13043/dys.30.7.

RIVAS, A., 2021. Ventajas y desventajas de Python - Qué es, definición y concepto. *Muy Tecnológicos* [en línea]. [consulta: 31 diciembre 2022]. Disponible en: https://muytecnologicos.com/diccionario-tecnologico/ventajas-y-desventajas-de-python.

ROCA, C., 2021. La metodología Kanban: ¿Qué es y cómo implementarla? (2022). *ThePower Business School* [en línea]. [consulta: 18 enero 2023]. Disponible en: https://www.thepowermba.com/es/blog/metodologia-kanban.

RODRÍGUEZ CRUZ, F., RENDÓN, C. y RODRIGUEZ-LIÑAN, A., 2023. Realización electrónica de sistemas caóticos: Parte 3, en sistemas digitales. *Ingenierias*, vol. 26, DOI 10.29105/ingenierias26.94-788.

RODRÍGUEZ LIÑÁN, J.Á. y LEÓN MORALES, J. de, 2007. Sincronización de caos mediante observadores para cifrado en comunicaciones. *Ingenierías*, vol. 10, no. 34, ISSN 1405-0676.

SANTOS, C.R.M. y GARCÉS, R.T., 2006. Los directores de la presente tesis, Dr. Claudio Rubén Mirasso Santos y Dr. Raúl Toral Garcés, titulares de la Universitat de les Illes Balears certi…can que esta tesis doctoral ha sido realizada por el Sr. Iacyel Gomes da Silva para la obtención del grado de Doctor en Física. Por ello …rman este documento. ,

SHEIKHOLESLAM, A., 2009. A chaos based encryption method using dynamical systems with strange attractors: *Proceedings of the International Conference on Security and Cryptography* [en línea]. Milan, Italy: SciTePress - Science and and Technology Publications, pp. 259-265. [consulta: 19 noviembre 2022]. ISBN 978-989-674-005-4. DOI 10.5220/0002105402590265. Disponible en: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0002105402590265.

SOTOMAYOR, S.G., 2021. Las metodologías ágiles más utilizadas y sus ventajas dentro de la empresa. *Thinking for Innovation* [en línea], [consulta: 17 enero 2023]. Disponible en: https://www.iebschool.com/blog/que-son-metodologias-agiles-agile-scrum/.

SPROTT, J.C., 2010. *Elegant chaos: algebraically simple chaotic flows*. S.l.: World Scientific.

TEAM, Y., 2015. Scrumban – An amalgamation of Scrum and Kanban. *Yodiz Project Management Blog* [en línea]. [consulta: 18 enero 2023]. Disponible en: http://www.yodiz.com/blog/scrumban-an-amalgamation-of-scrum-and-kanban/.

TELCEL, 2023. Empresas que han sufrido robo de información | Telcel Empresas. [en línea]. [consulta: 11 abril 2023]. Disponible en: https://www.telcel.com/empresas/tendencias/notas/empresas-perdidas-economicas-por-robo-informacion.

UNIR, 2021. Confidencialidad en seguridad informática, ¿en qué consiste? *UNIR* [en línea]. [consulta: 11 junio 2023]. Disponible en: https://www.unir.net/ingenieria/revista/confidencialidad-seguridad-informatica/.

UNIVERSIDAD EUROPEA, 2021. ¿Qué son las metodologías ágiles? | Blog UE. *Universidad Europea* [en línea]. [consulta: 17 enero 2023]. Disponible en: https://universidadeuropea.com/blog/metodologias-agiles/.

VILLATE, J., 2022. Sistemas caóticos &emdash; Atrator de Lorenz. [en línea]. [consulta: 13 diciembre 2022]. Disponible en: https://villate.org/dinamica/caos/slide07.html.

ZAQUEROS-MARTÍNEZ, J., RODRÍGUEZ-GÓMEZ, G., TLELO-CUATLE, E. y ORIHUELA-ESPINA, F., 2020. Sincronización de sistemas caóticos fraccionarios. ,

ZHANG, W., ZHOU, S., LI, H. y ZHU, H., 2009. Chaos in a fractional-order Rössler system. *Chaos, Solitons & Fractals*, vol. 42, no. 3, ISSN 0960-0779. DOI 10.1016/j.chaos.2009.03.069.

ZHU, Y., 2015. MATLAB Simulation Model on Chaotic Asynchronous Transmitter and Receiver.

ANEXOS

Anexo A: Requisitos funcionales

Definición de requerimientos funcionales

ID Requisito	Nombre del requisito	Característica	Descripción
RQF01	Autentificación de Usuario	El sistema permitirá registrar usuarios y administrador.	El sistema contará con un Login, dónde deberá ingresar un correo electrónico y la contraseña para ingresar. Para registrarse como nuevo usuario se pedirá que ingrese nombre, correo y contraseña.
RQF02	Menú de opciones	El sistema mostrará un menú de opciones	Se mostrará un menú con las opciones de los cuatro atractores caóticos.
RQF03	Menú de opciones administrador	El sistema mostrará un menú de opciones	El administrador podrá escoger opciones como inicio, atractores, usuarios e informes.
RQF04	Ingreso de Información	El sistema permitirá el ingreso de cadenas de texto plano.	En cualquiera de los atractores se podrá ingresar cadenas de texto, y se visualizará el texto cifrado, tiempo de sincronización, tiempo de cifrado,

			parámetros y condiciones iniciales.
RQF05	Informes	El sistema permitirá mostrar una estadística de los atractores.	Se visualizará información de textos cifrados por atractor con sus respectivos tiempos y gráficas.
RQF06	Gestión de usuarios	El sistema permitirá que el administrador elimine usuarios y datos de cifrado/ descifrado. Además, podrá observar los inicios de sesión en el sistema con su IP y ubicación.	El administrador estará a cargo de los usuarios que se hayan registrado y a la vez eliminarlos, de igual manera los datos de cifrado y descifrado.
RQF07	Cerrar Sesión	El sistema permitirá cerrar sesión	Una vez utilizado el sistema se permitirá cerrar sesión.

Anexo B: Requisitos no funcionales

Se ha definido los requisitos no funcionales

ID Requisito	**Nombre del requisito**	**Característica**	**Descripción**
RQNF01	Usabilidad	Sistema agradable para el usuario	El sistema deberá ser sencillo, intuitivo, de fácil aprendizaje. Y cumplir con los requerimientos.
RQNF02	Seguridad	Sistema que protege la información	El sistema contará con un control de acceso seguro de la

			información y datos personales, recuperación de contraseñas
RQNF03	Funcionalidad	Responde todas las peticiones.	El sistema deberá responder a todas las peticiones del usuario.

Anexo C Análisis previo al desarrollo del proyecto

Análisis económico

Se muestra el presupuesto que se necesita para el desarrollo de la aplicación web de cifrado y descifrado.

Descripción	**Valor Unitario**	**Total**
Laptop MSI GF63 Thin 10SC	$ 1200,00	$ 1200,00
Material de Oficina	$ 50,00	$ 50,00
Servicio de Internet por 6 meses	$ 30,00	$ 80,00
Servicios básicos por 6 meses	$ 15,00	$ 90,00
Licencias	$ 30,00	$ 30,00
Alimentación	$ 50,00	$ 300,00
Alojamiento en la nube	$ 5,00	$30,00
Transporte	$ 24,00	$ 144,00
Total		**$ 2024,00**

Fuente de financiamiento

El estudiante con sus propios recursos financia lo detallado en la tabla anterior

Recursos Hardware

Se detallan los equipos y recursos utilizados para el desarrollo del presente trabajo de titulación.

Hardware	Características	Utilidad
Internet	Netlife, fibra óptica 40 MB	Para poder buscar información en fuentes confiables.
Computadora	MSI	Para poder realizar las investigaciones y trabajar en la aplicación web. Revisar tesis, anteproyectos, libros, etc. Almacenar información. Utilizar un IDE para poder programar en el lenguaje deseado.
Memoria RAM	8 GB	
Procesador	Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz (8 CPUs), ~2.5GHz	
Disco Duro	256 GB	

Recursos Software

Se observa los recursos software utilizados para el desarrollo del presente trabajo de titulación.

Característica	Software	Utilidad
Sistema Operativo	Windows 11 Home 64 bits	Gestionar todos los recursos del computador.
Base de Datos	SQLite	Crear, gestionar y almacenar datos a través de varios motores de almacenamiento
Mockups	Balsamiq Mockups	Realizar bocetos de las pantallas pertenecientes a los módulos a utilizar.
IDE de desarrollo	Visual Studio Code	Permite trabajar con cualquier lenguaje de programación.
Lenguaje de programación	Python	Para realizar la aplicación web y la sincronización de los atractores caóticos.
Tecnología de programación	HTML5	Sirve como referencia del software que conecta con la elaboración de páginas web

		en sus diferentes versiones, define una estructura básica y un código (denominado HTML) para la definición de contenido de una página web, como texto, imágenes, vídeos, juegos, entre otros.
Tableros Kanban	TeamHood	Roles y actividades
Diagrama de caso de uso	Draw.io	Para graficar todo el funcionamiento del sistema con sus roles de usuario.
Vistas de modelo 4+1	Enterprise Architect	Para documentar las vistas de la arquitectura.

Riesgos

Se realizó un análisis de los posibles riesgos que puedan afectar en el desarrollo de la aplicación web, los mismos se detallan a continuación:

ID Riesgo	Descripción	Porcentaje de probabilidad	Porcentaje de impacto	Técnicas de mitigación	Plan de contingencia	Consecuencias
R001	Requisitos incompletos o ambiguos.	40%	90%	1.El estudiante y docente deben tener claro la funcionalidad de la aplicación 2. Incorporar los nuevos requerimientos o cambios para que se cumpla la funcionalidad	Detener el proyecto momentáneamente para evitar problemas.	Se entrega un proyecto que no cumple con los objetivos planteados en el anteproyecto aprobado.

				solicitada		
R002	Falta de documentación en el código fuente	30%	50%	1.Realizar comentarios en cada procedimiento o función realizada. 2.Basarse en un estándar de programación para tener un código fuente legible.	Notificar al director del trabajo de titulación que estándar de codificación se va a utilizar (PEP8)	El desarrollador que desee basarse en el código elaborado no va a comprender fácilmente lo que realiza cada función.
R003	Mal diseño de la base de datos.	30%	90%	Realizar un esquema lógico de la base de datos analizando los requerimientos	Rediseñar la base de datos	Fallas en la manipulación de datos o los datos no son correctos.
R004	Daños en equipos de cómputo	50%	100%	Realizar copias de seguridad periódicamente.	Plan de comunicación que permita informar rápidamente a las partes interesadas de lo sucedido. Recuperación de equipos.	Retraso en la entrega de la aplicación y pérdida de información
R005	Fallo en la sincronización de los sistemas caóticos	20%	80%	Revisar las fórmulas que estén correctamente expresadas.	Asegurarse que la sincronización de los sistemas caóticos se	No se va a poder realizar el cifrado y descifrado de cadenas de texto.

					realice como se espera.	
R006	Cambio de tecnologías empleadas.	20%	90%	Definir las tecnologías antes de codificar.	Notificar al director del trabajo de titulación del cambio.	Pérdida de tiempo en el proyecto. No entregar en el tiempo especificado.
R007	Alcance de las pruebas no definido completamente.	40%	75%	1.Aclarar dudas y recibir apoyo por parte del jefe de proyecto 2.Aprobación del plan de pruebas por parte de los interesados del proyecto.	Definir en un documento concretamente las pruebas que se van a realizar y su respectivo alcance.	No se puede comprobar por completo que la aplicación cumpla con los objetivos.
R008	Demoras excesivas en la reparación de defectos encontrados en las pruebas.	40%	60%	1.Una vez encontrado un defecto, se debe enfocar los recursos y mayor tiempo para poder resolverlo 2. Realizar reuniones para llegar a una solución a dicho problema	Encontrar un error y tratar de resolverlo de una forma eficaz y eficiente para evitar demoras	El proyecto no termina en la fecha acordada

Anexo D: Diccionario de datos

Usuario_Registro

Nombre del archivo: usuario_registro **Descripción del archivo:** Persona natural que utiliza el sistema.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1
nombre	Nombre y apellido del usuario.	Varchar(100)	No	primer nombre + (primer apellido) = { [A-Z|a-z] }
usuario	Nombre de usuario o username.	Varchar(100)	No	Nombre de usuario = { [AZ|a-z] } + [0 a 9]
correo	Correo del usuario.	Varchar(100)	No	correo@example.com
password	Contraseña del usuario.	Varchar(100)	No	=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{8,}
ciudad	Ciudad de residencia del usuario.	Varchar(100)	No	ciudad = { [A-Z|a-z] }
telefono	Teléfono personal del usuario.	Varchar(100)	No	[0000000000] * permite un dígito [0 a 9] y requiere la entrada de los 10 dígitos *
fecha_creacion	Fecha en que se registra el usuario.	Datetime	No	* formato: aaaa-mm-dd *
token	Para recuperar la contraseña.	Varchar(255)	Si	Token generado
is_admin (FK)	Rol de usuario.	Integer	No	[1 | 2] * significado: 1: Admin | 2:

				Usuario *

Acceso

Nombre del archivo: acceso **Descripción del archivo:** Registro de inicios de sesión.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1
ip	Dirección ip del dispositivo que se utiliza para ingresar.	Varchar	No	[0.0.0.0]
ubicacion	Ubicación en tiempo real del usuario que ingresa.	Varchar	No	Ubicacion = { [AZ|a-z] }
ultima_conexion	Fecha y hora del último inicio de sesión.	Datetime	No	* formato: aaaa-mm-dd *
usuario1_id (FK)	Id usuario	Integer	No	Mayores a 0 de la tabla usuario_registro

Rol

Nombre del archivo: rol **Descripción del archivo:** Roles de usuario.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1
nombre	Nombre del rol.	Varchar	No	Nombre= { [AZ|a-z] }

Atractor

Nombre del archivo: atractor **Descripción del archivo:** Atractores utilizados.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1
nombre	Nombre del atractor.	Varchar	No	Nombre= { [AZ|a-z] }

Addcifrado

Nombre del archivo: addcifrado **Descripción del archivo:** Tabla que almacena información del cifrado.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1
cadena_texto	Cadena de texto que se quiere cifrar.	Varchar	No	Cadena_texto = { [AZ|a-z] }
cadena_cifrada	Cadena de texto cifrada.	Varchar	No	Ubicacion = { [AZ|a-z] }
tiempo_sincr	Tiempo en microsegundos de sincronización.	Datetime	No	* formato: aaaa-mm-dd *
tiempo_cif	Tiempo en microsegundos de cifrado.	Datetime	No	* formato: aaaa-mm-dd *
atractor_id (FK)	Id atractor	Integer	No	[1-4] de la tabla atractores
usuariocif_id (FK)	Id usuario	Integer	No	Mayores a 0 de la tabla usuario_registro

Adddescifrado

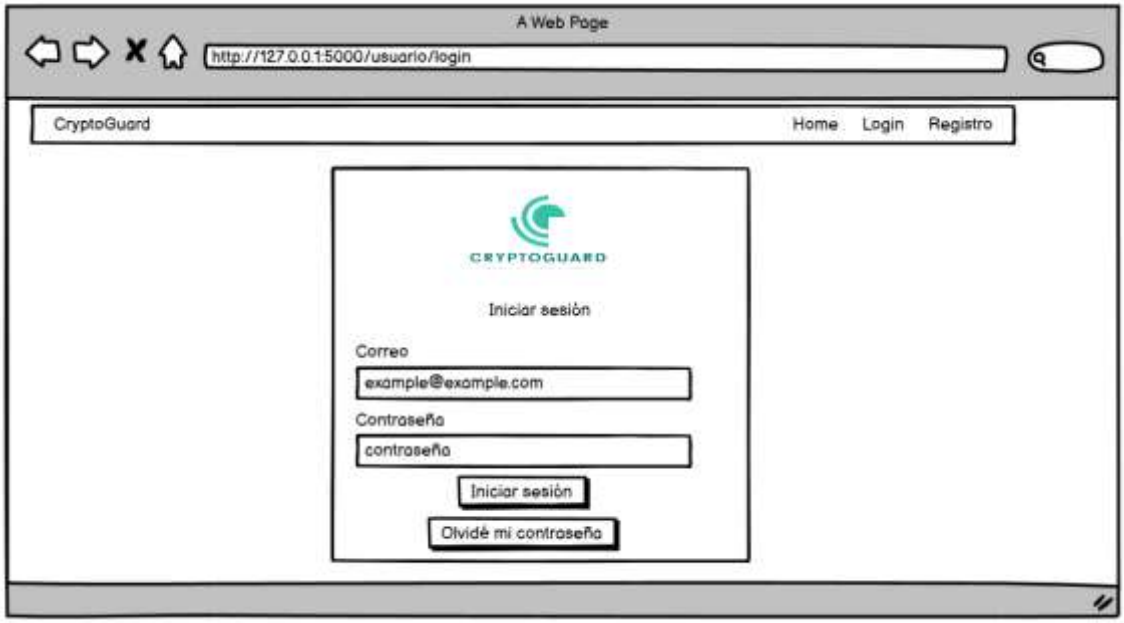
Nombre del archivo: adddescifrado **Descripción del archivo:** Tabla que almacena información del descifrado.				
Nombre del campo	**Descripción**	**Tipo de dato y tamaño**	**Permite NULL**	**Valor permitido del dato**
id (PK)	Identificador.	Integer	No	Mayores a 0 *Es auto incremental 1,1
cadena_texto	Cadena de texto que se quiere descifrar.	Varchar	No	Cadena_texto = { [AZ|a-z] }
cadena_descifrada	Cadena de texto descifrada.	Varchar	No	Ubicacion = { [AZ|a-z] }
tiempo_descif	Tiempo en microsegundos de descifrado.	Datetime	No	* formato: aaaa-mm-dd *
atractor_id (FK)	Id atractor	Integer	No	[1-4] de la tabla atractores
usuariocif_id (FK)	Id usuario	Integer	No	Mayores a 0 de la tabla usuario_registro

Anexo E: Prototipado o mockups

Usuario

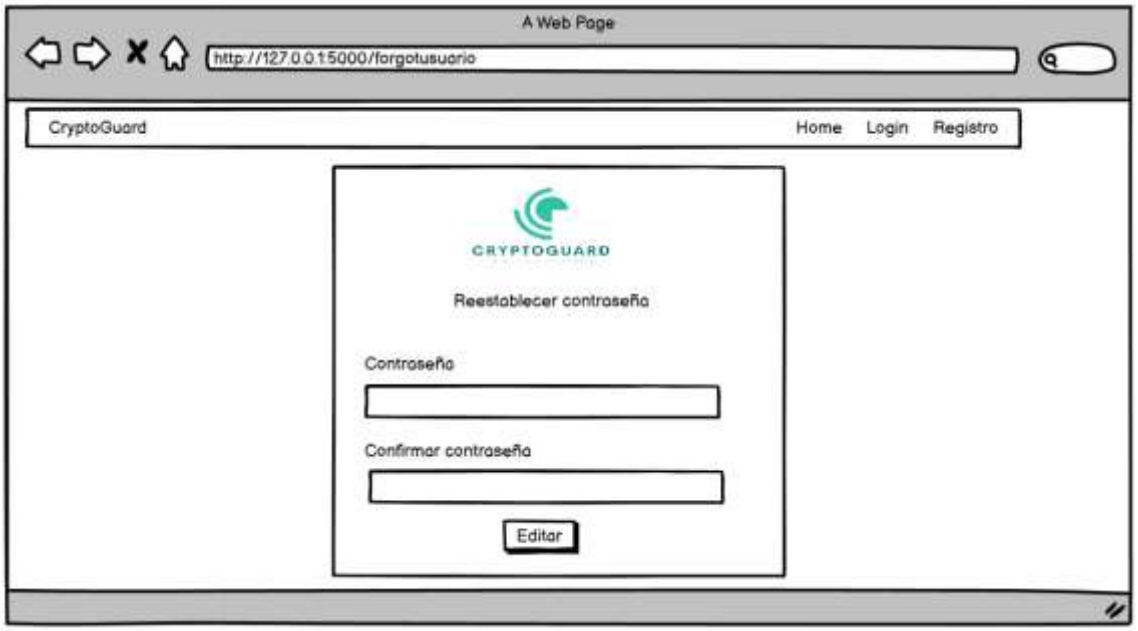
Home

Login

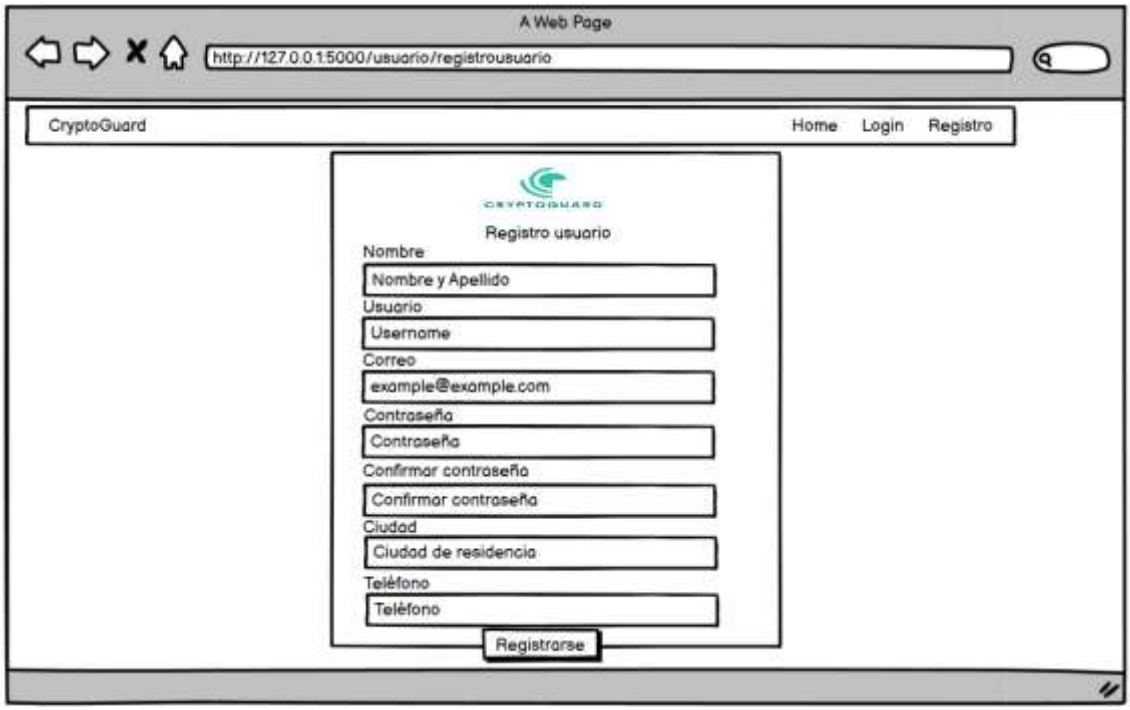


Olvidé mi contraseña

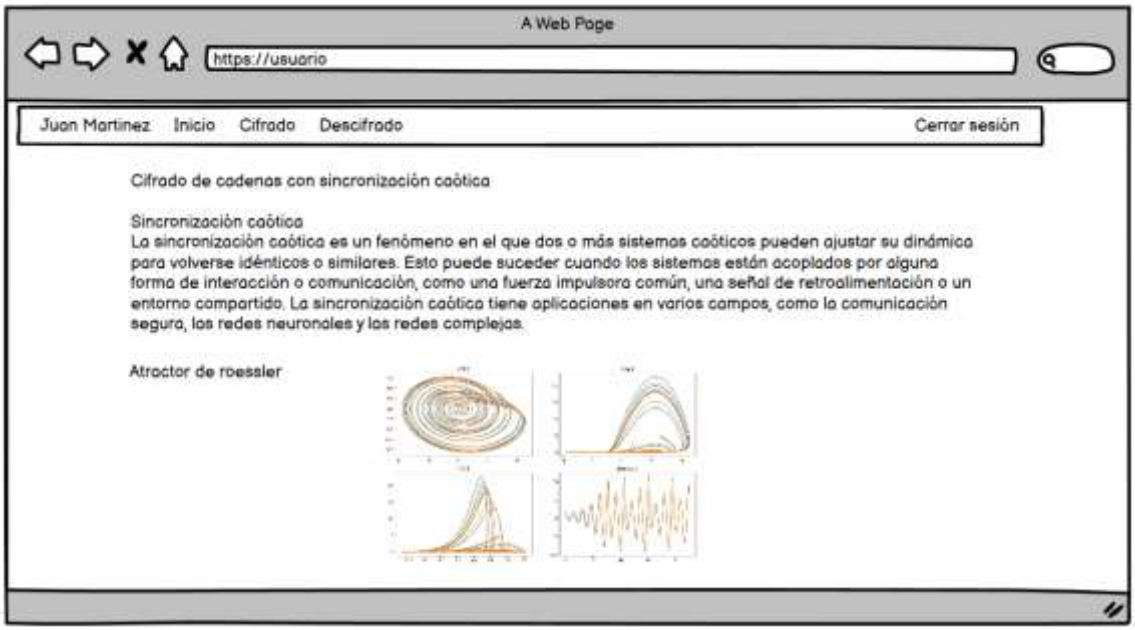
Cambiar contraseña



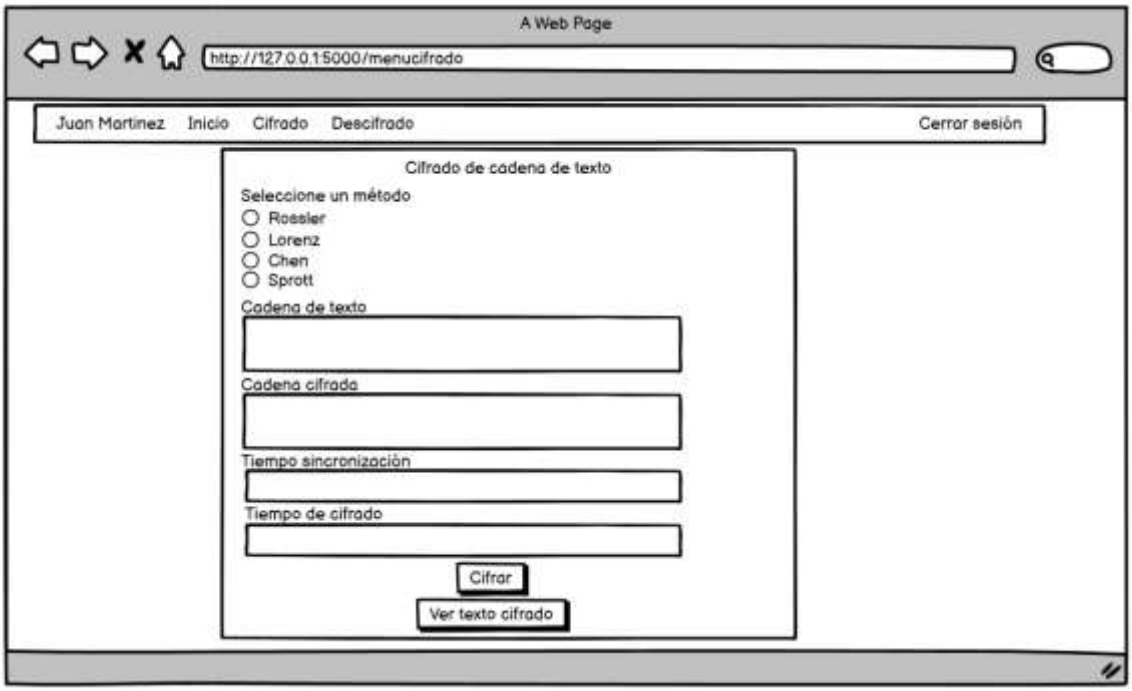
Registro



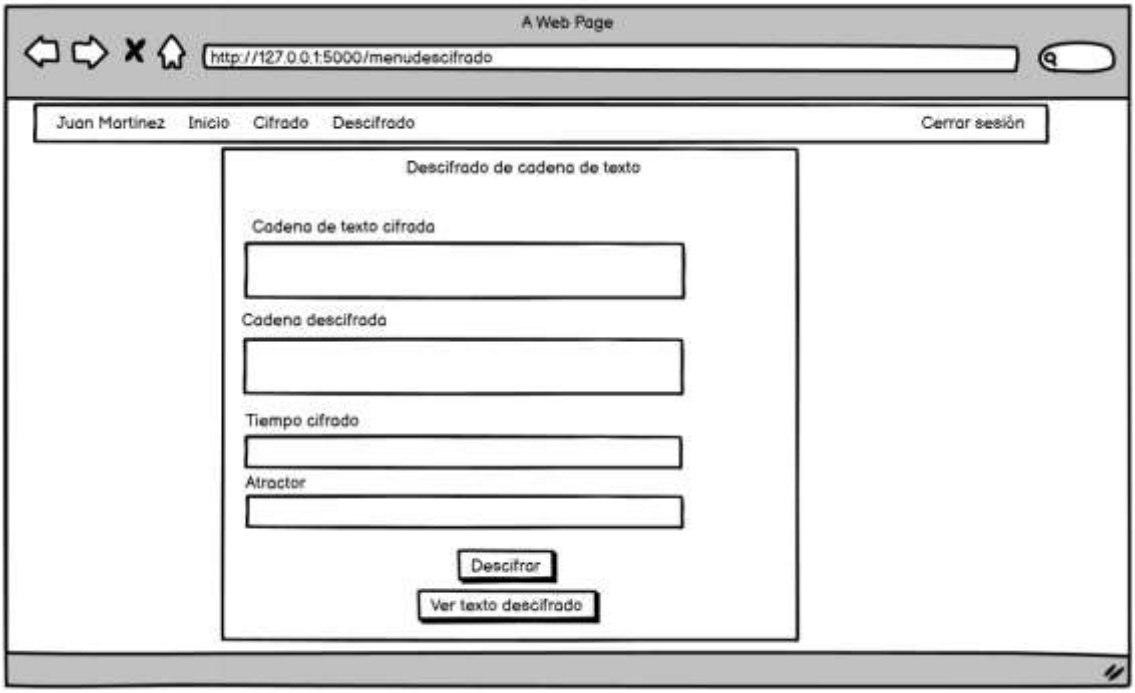
Página de inicio



Cifrado



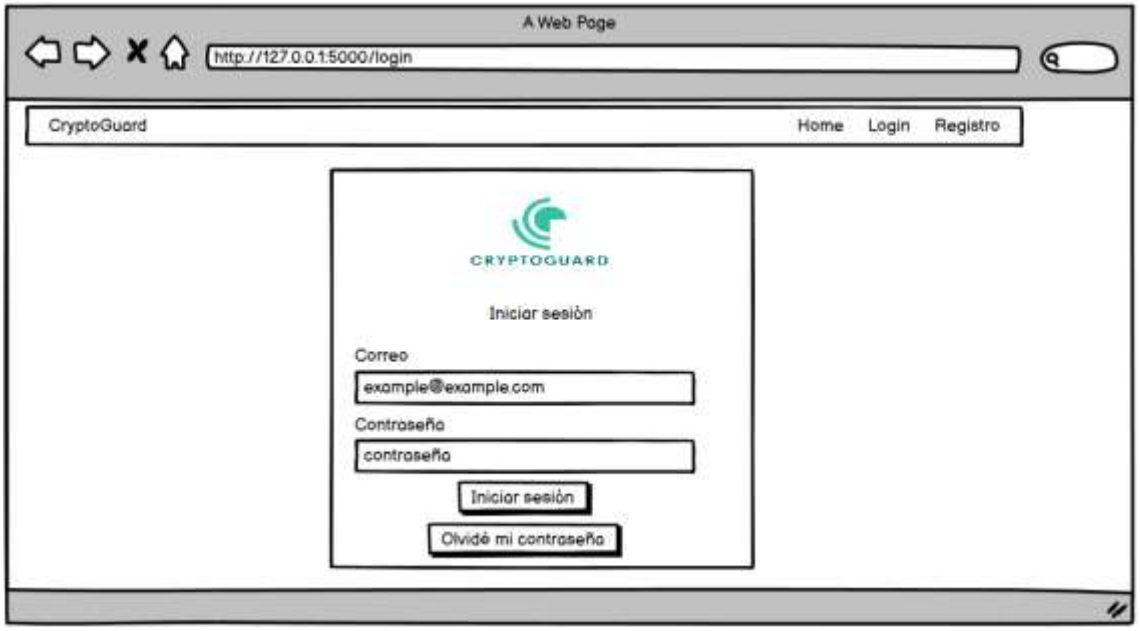
Descifrado



Administrador

Home

Login

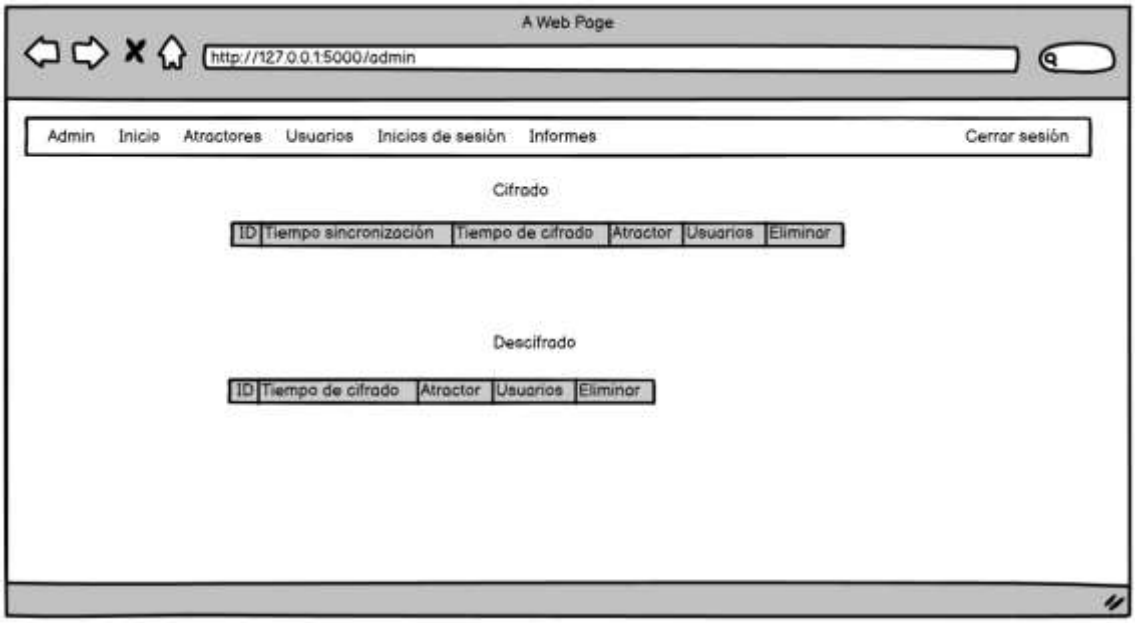


Olvidé contraseña

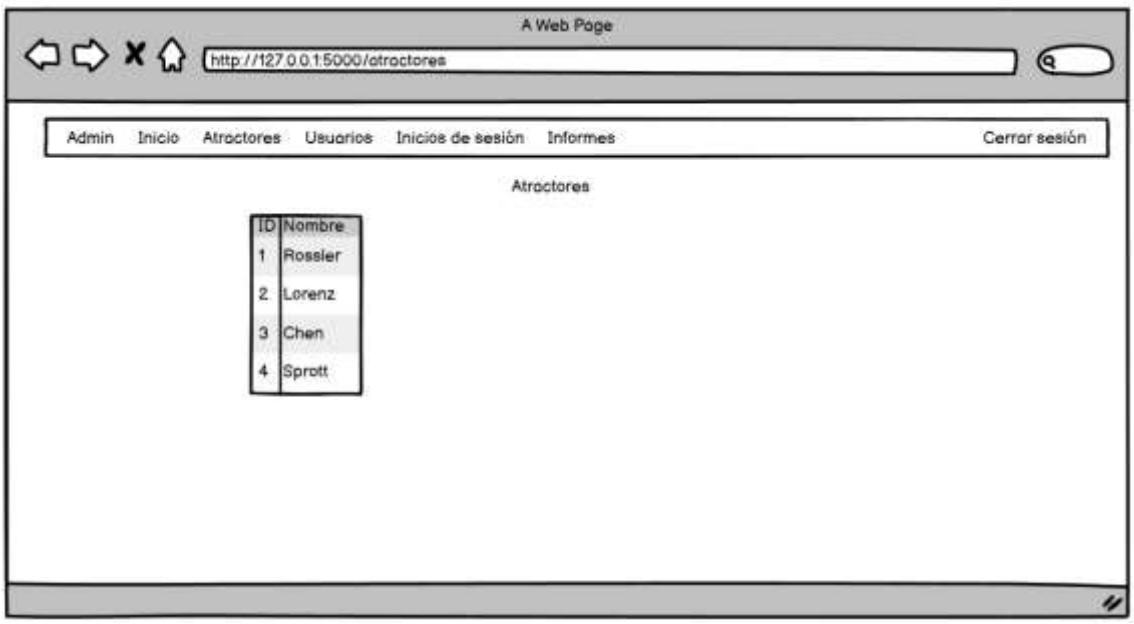
Cambiar contraseña

Registro admin

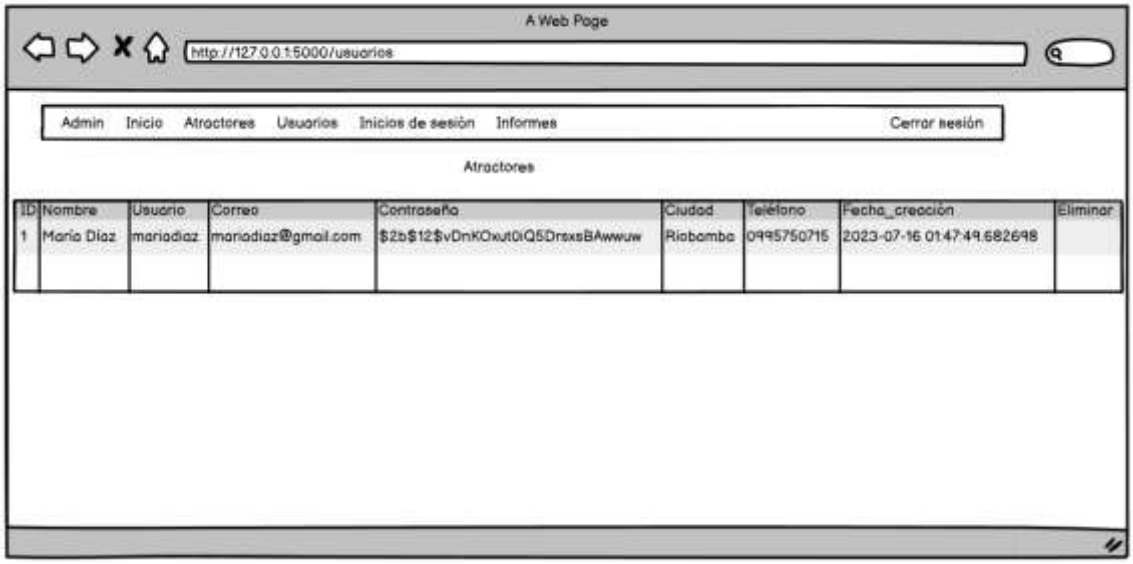
Página principal



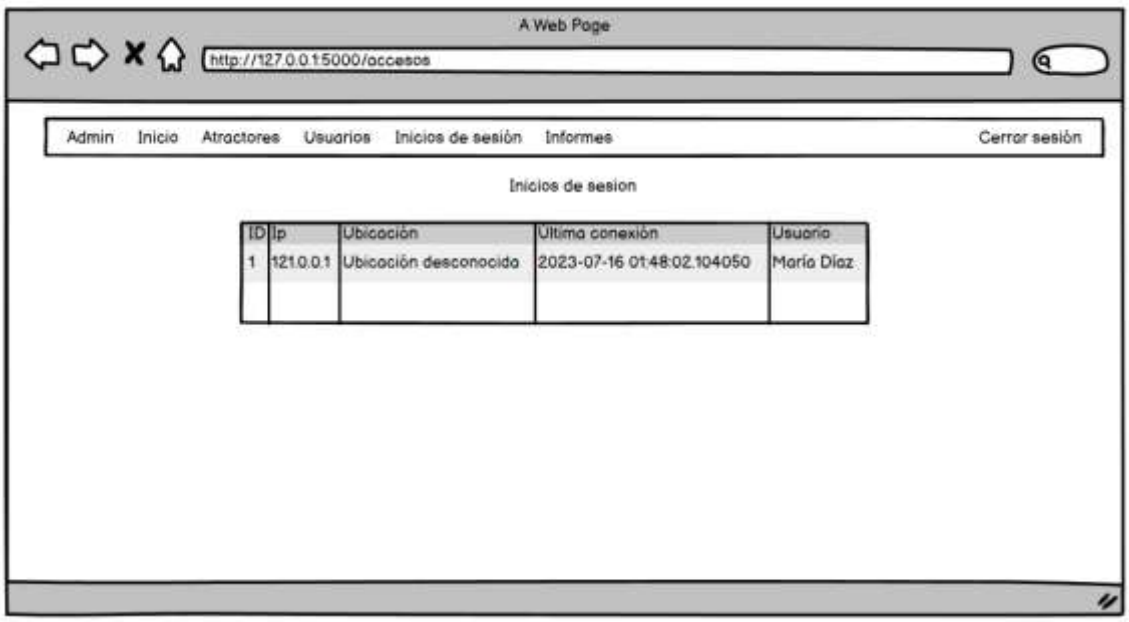
Atractores



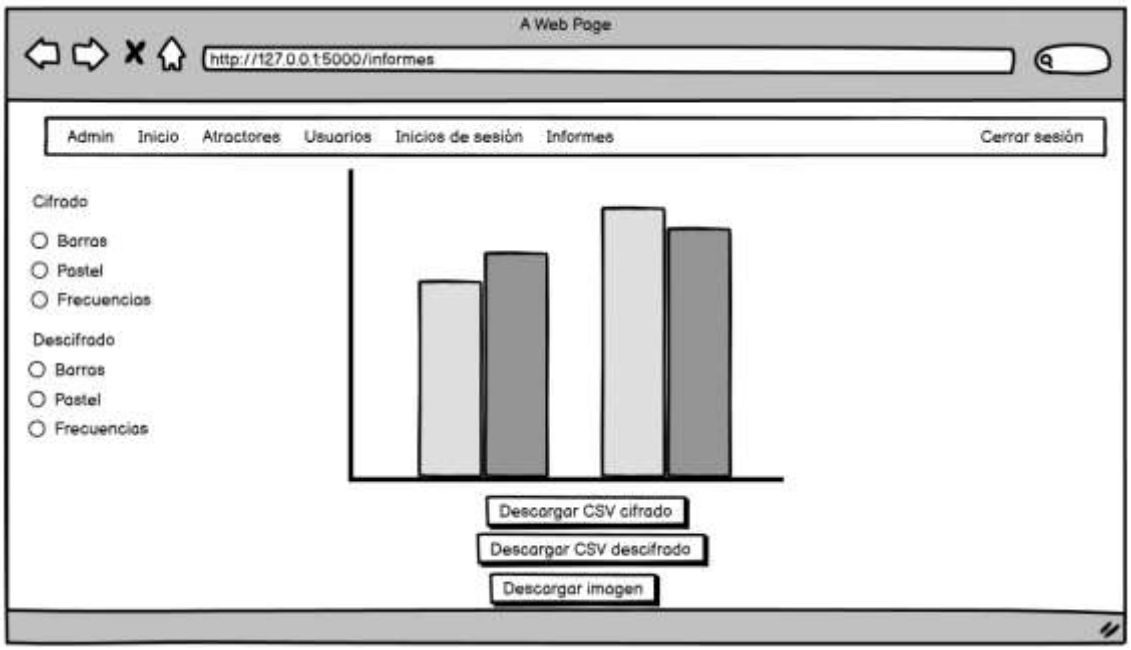
Usuarios



Inicios de sesión



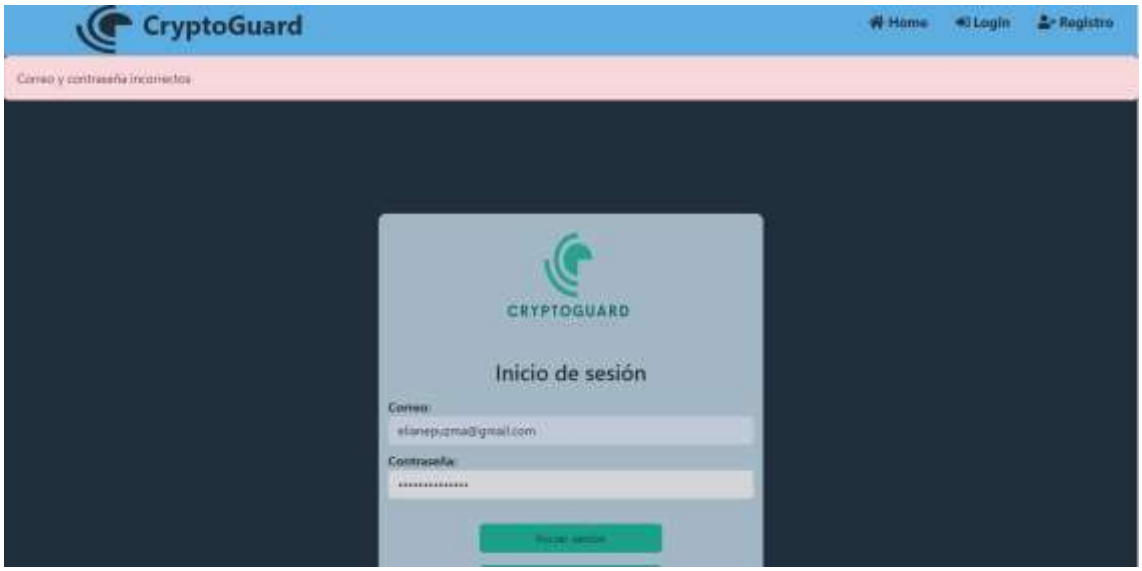
Informes



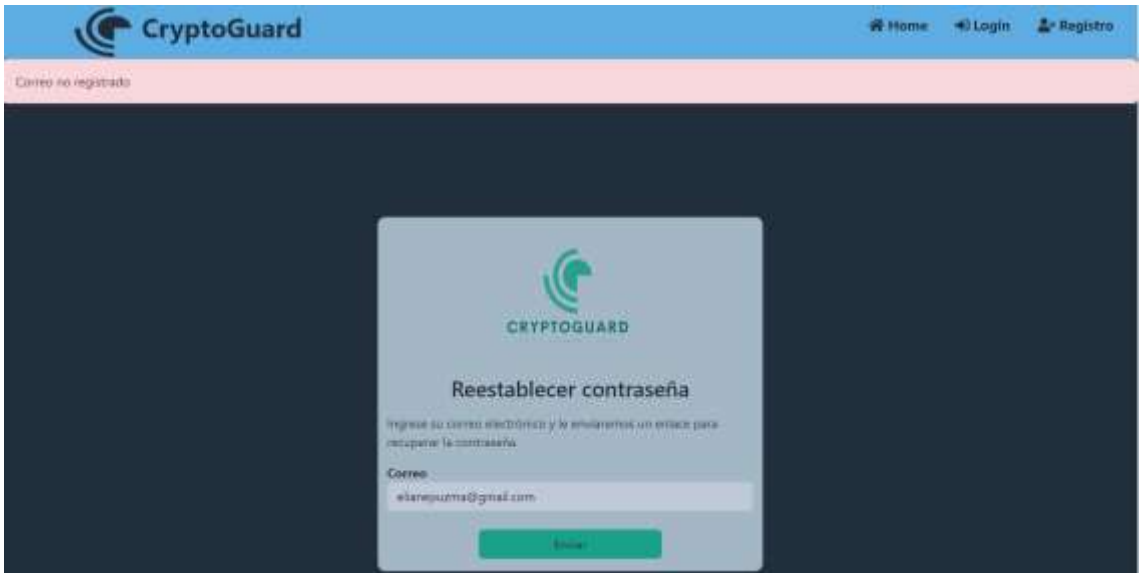
Anexo F: Pruebas

Usuario

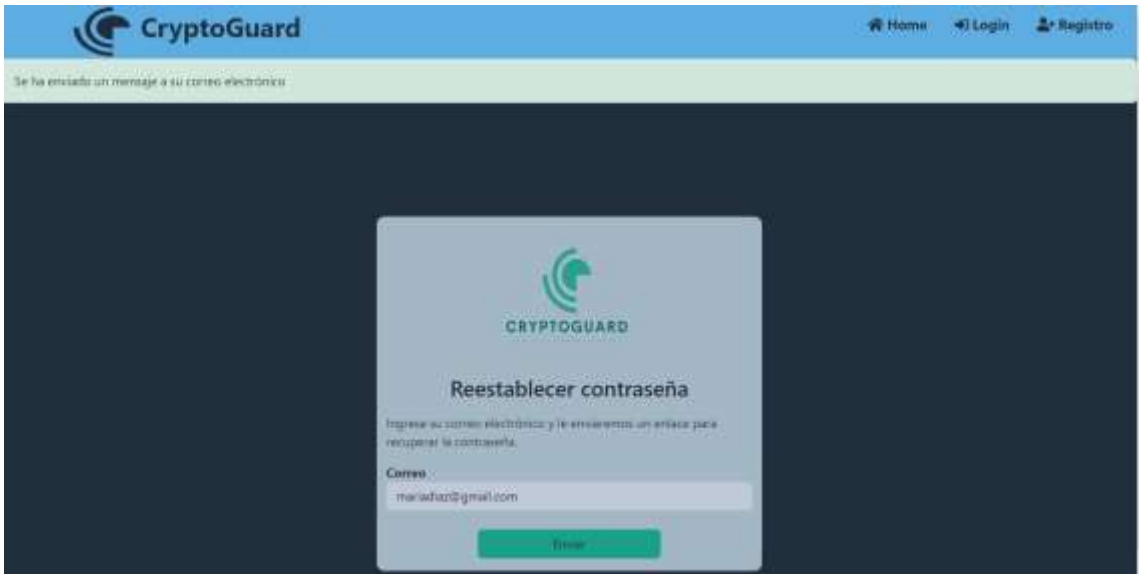
1. Al iniciar sesión se verifica que el correo ingresado esté registrado en la base de datos de igual manera la contraseña.



2. Si el usuario se olvida la contraseña puede recuperarla, ingresando el correo registrado, si el correo ingresado para recuperar la contraseña muestra un mensaje de error.



3. Cuando se ingresa un correo registrado, se envía de manera automática un correo con un enlace donde se podrá recuperar la contraseña.



Solicitud de contraseña olvidada

anahipuzma22@gmail.com
para mariadiaz

Estimado usuario mariadiaz@gmail.com,

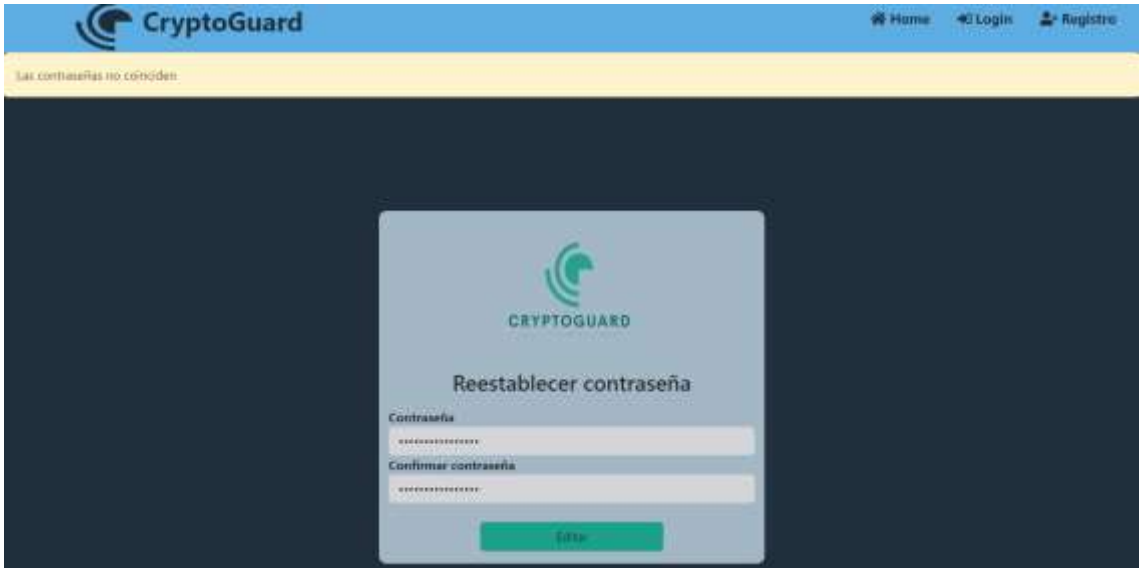
Le agradecemos por tomarse su tiempo. Haga clic en el enlace de abajo para cambiar la contraseña:

http://127.0.0.1:5000/resetusuario/1acdcfba-b61a-4b31-b396-556648a02f56

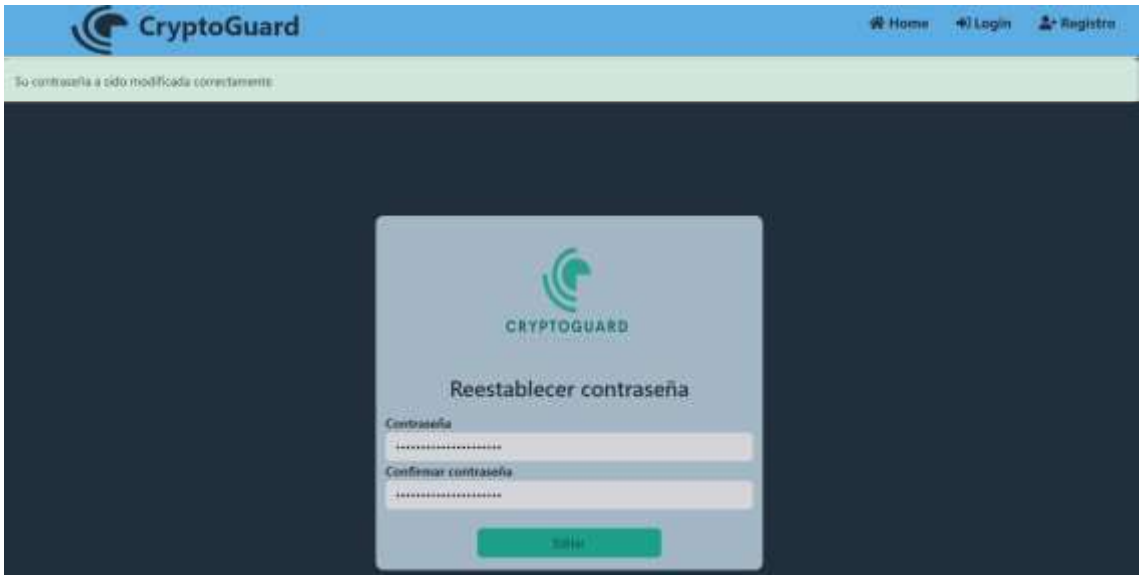
Gracias por subscribirse.

Sistema de cifrado password reset team.

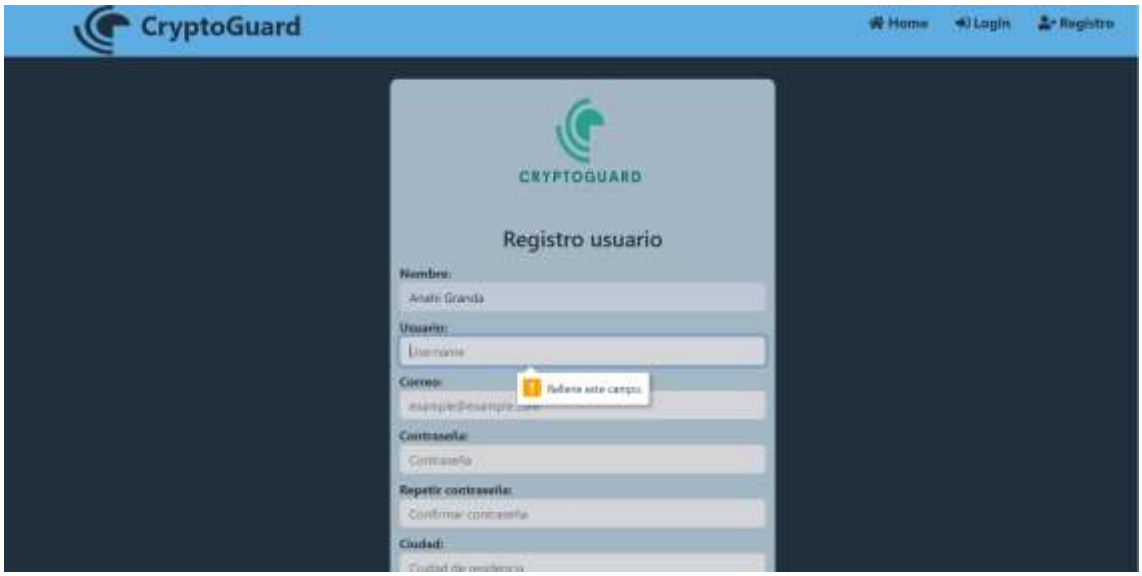
4. Al momento de ingresar la nueva contraseña deben coincidir las dos veces que se pide que ingresen o sino va a mostrar un mensaje de alerta.



5. Cuando las contraseñas coincidan se modificará en la base de datos.



6. Para la parte de registro el usuario debe llenar todos los campos que se solicita.

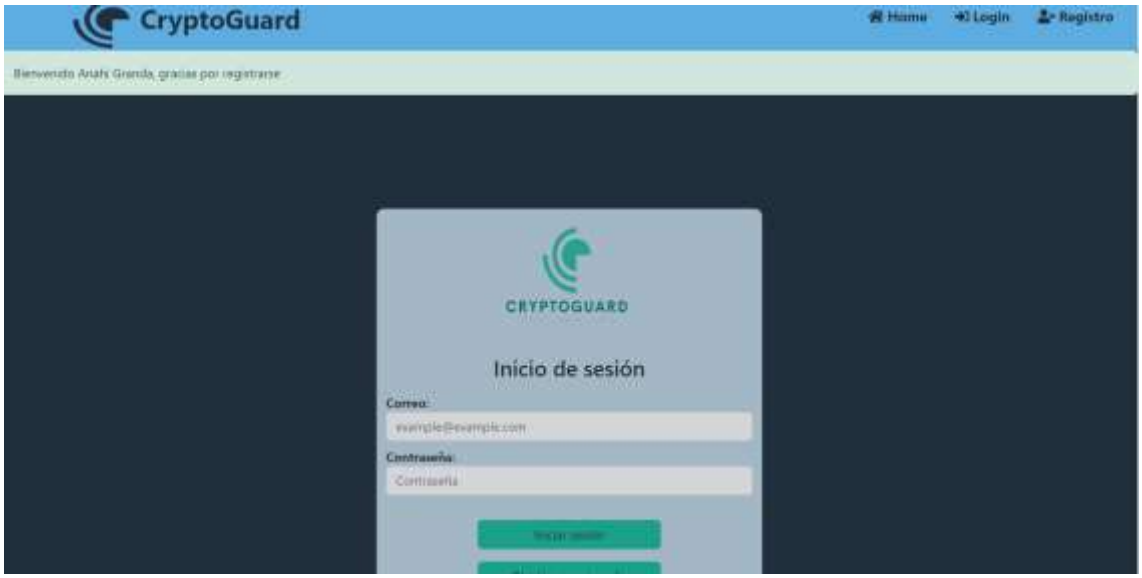


7. La contraseña debe tener mínimo ocho caracteres, incluyendo números, mayúsculas, minúsculas y un carácter especial. Además, las contraseñas deben coincidir y se verificará que el usuario y correo no esté en uso.

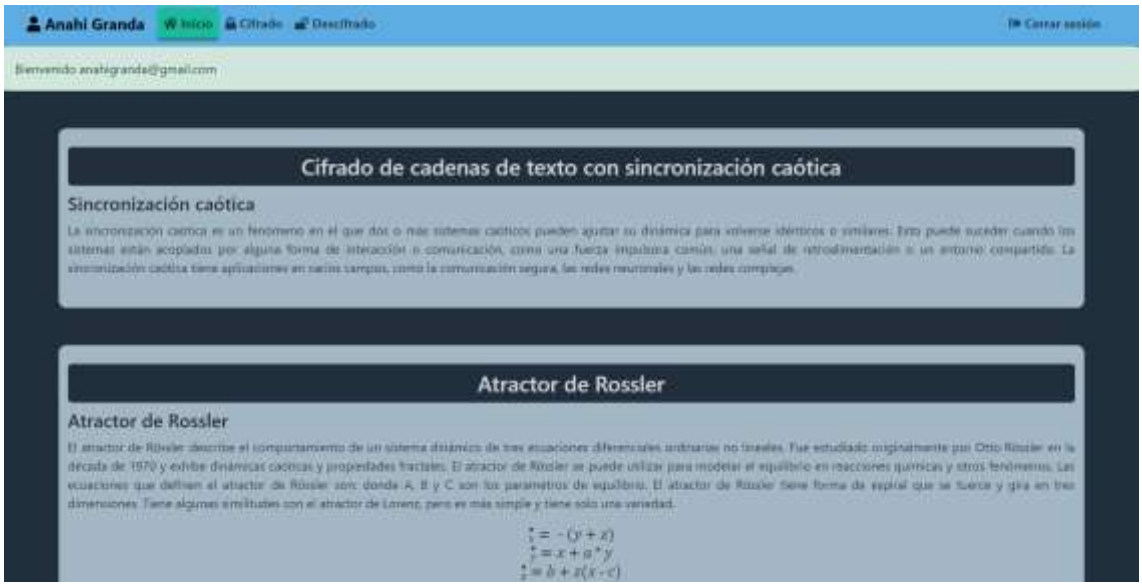

CRYPTOGUARD
Registro usuario
Nombre:
Anahi Granda
Usuario:
anahigranda
Correo:
anahi@gmail.com
Contraseña:
Prolonga este texto a 8 caracteres o más (en este momento tiene 6 caracteres).
Ciudad:
Ciudad de residencia

8. Se verifica que el correo ingresado sea válido o tenga la notación example@example.com

9. Una vez registrado muestra un mensaje satisfactorio y se dirige al inicio de sesión

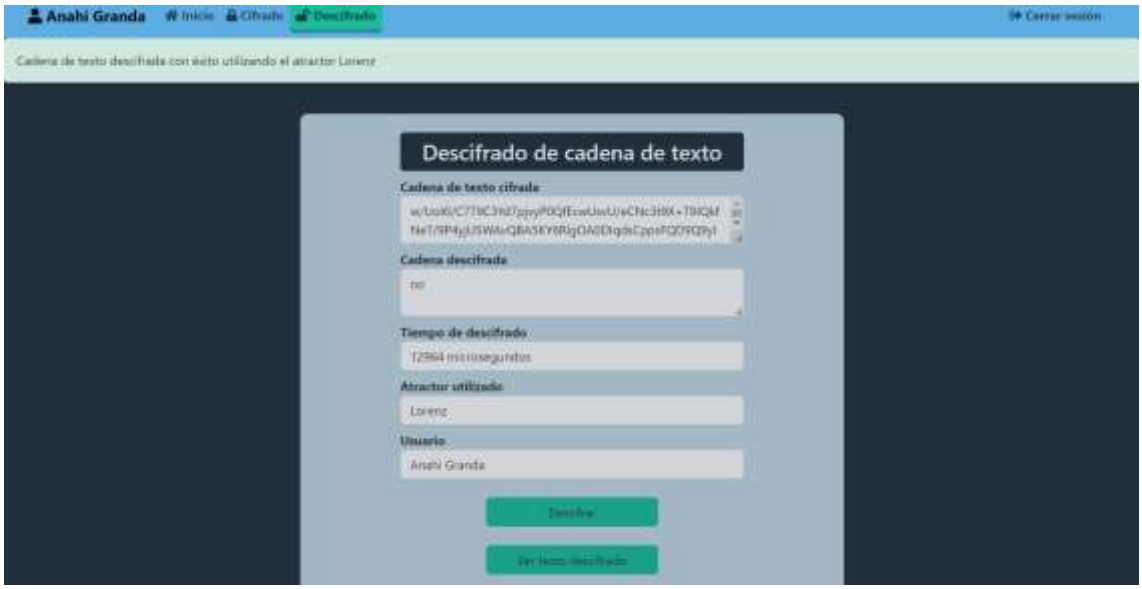


10. Se ingresa sesión y se muestra la página principal con el menú cifrado y descifrado.



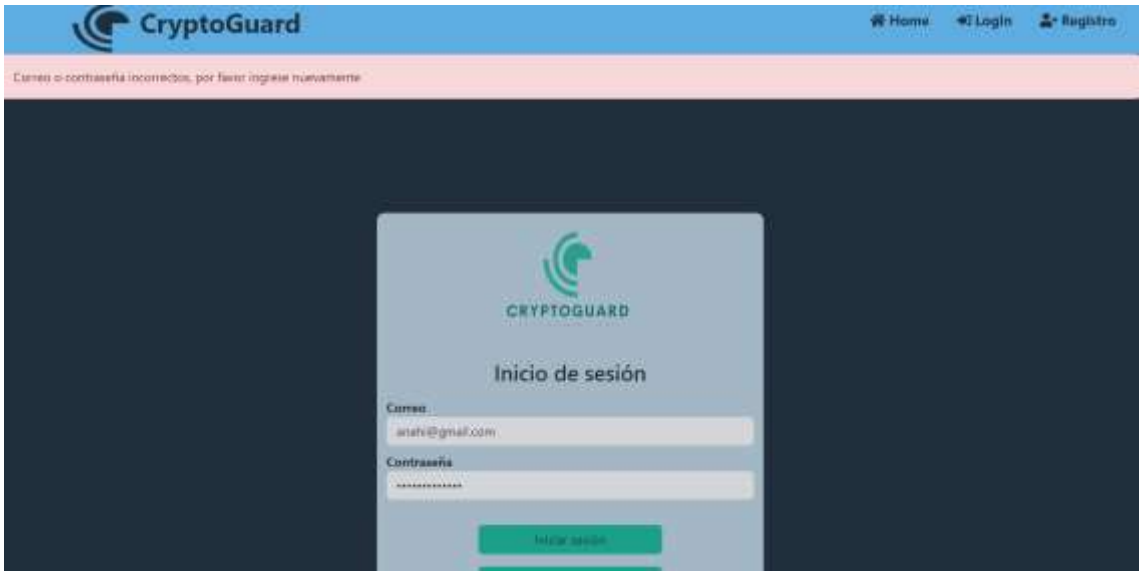
11. En el menú cifrado hay cuatro opciones, Rossler, Lorenz, Chen y Sprott, se muestra el mensaje cifrado con sus tiempos respectivos.

12. Para descifrar se ingresa el texto cifrado y se observa la cadena de texto que descifró la aplicación web.

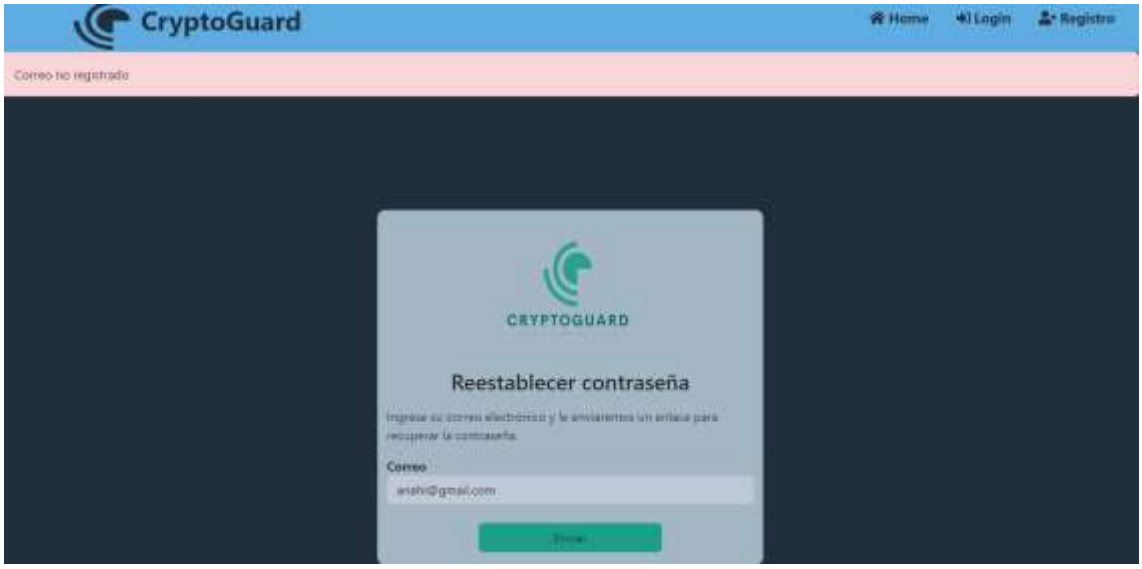


Administrador

13. Al inicio de sesión el correo o contraseña debe estar registrado en la base de datos o mostrará un mensaje de error.

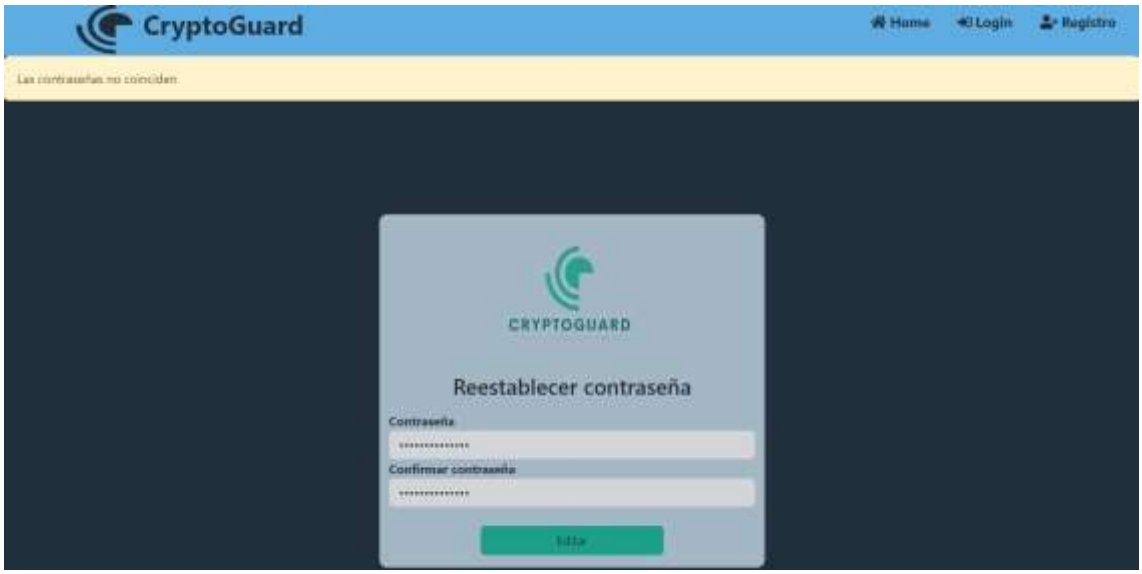


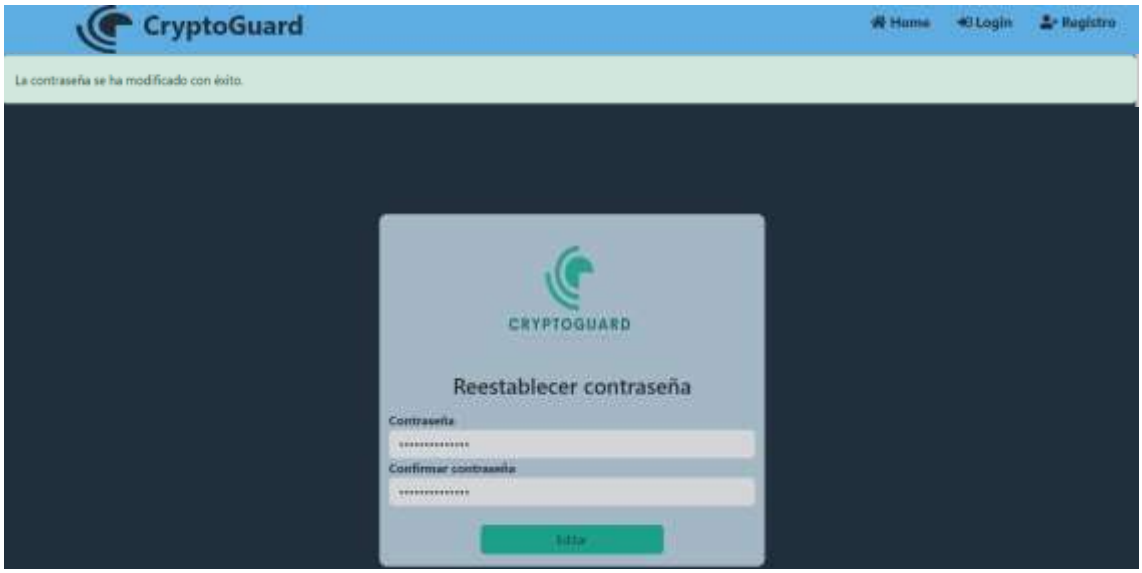
14. Si el administrador olvidó la contraseña, debe ingresar un correo registrado o si no se muestra un mensaje de error.



15. Una vez verificado el correo se enviará un mensaje con el enlace de recuperación de contraseña.

16. Las contraseñas deben coincidir o se va a mostrar un mensaje de alerta.





17. En el registro se deben llenar todos los campos.

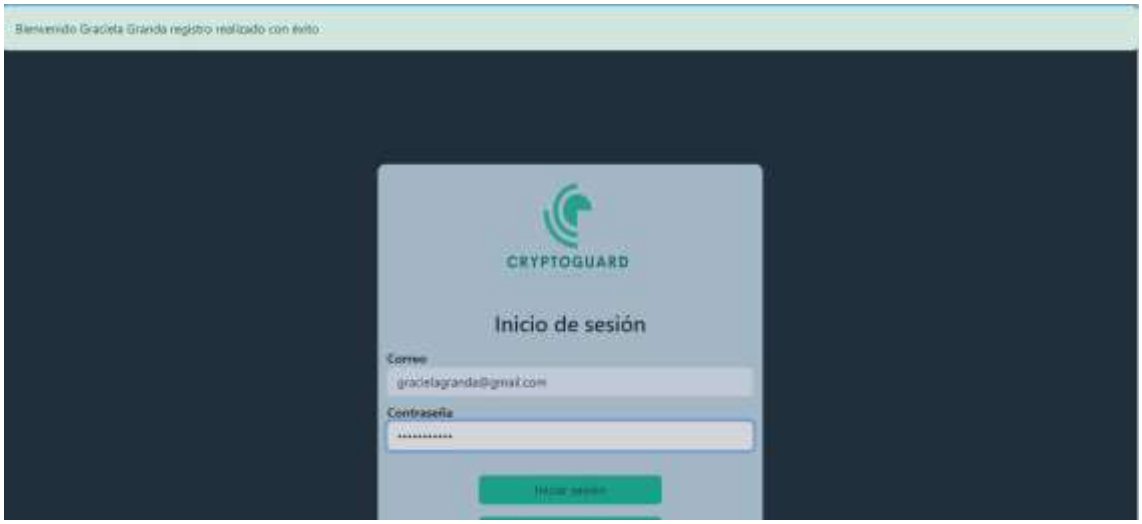
18. La contraseña tiene que ser mínimo ocho caracteres, entre mayúsculas, minúsculas, números y un carácter especial.


CRYPTOGUARD
Registro administrador
Nombre
Graciela Granda
Correo
gracielagranda@gmail.com
Contraseña
Prolonga este texto a 8 caracteres o más (en este momento tiene 7 caracteres).
Registrarse


CRYPTOGUARD
Registro administrador
Nombre
Graciela Granda
Correo
gracielagranda@gmail.com
Contraseña
La contraseña debe contener al menos una letra mayúscula, una letra minúscula, un número, un carácter especial.
Repetir contraseña
Registrarse

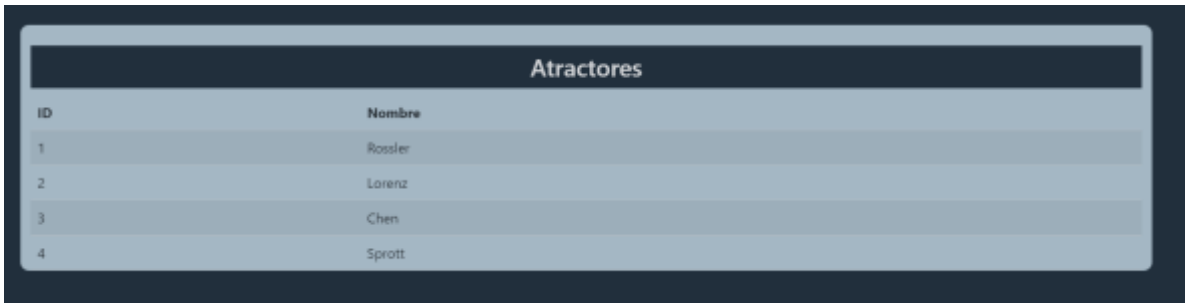
19. Si el correo ingresado ya pertenece a otro administrador, se muestra una notificación.

20. Si ya se registró el administrador, puede iniciar sesión.



21. Se muestra la página principal del administrador con su respectivo menú.

Permite observar los atractores que se está utilizando.

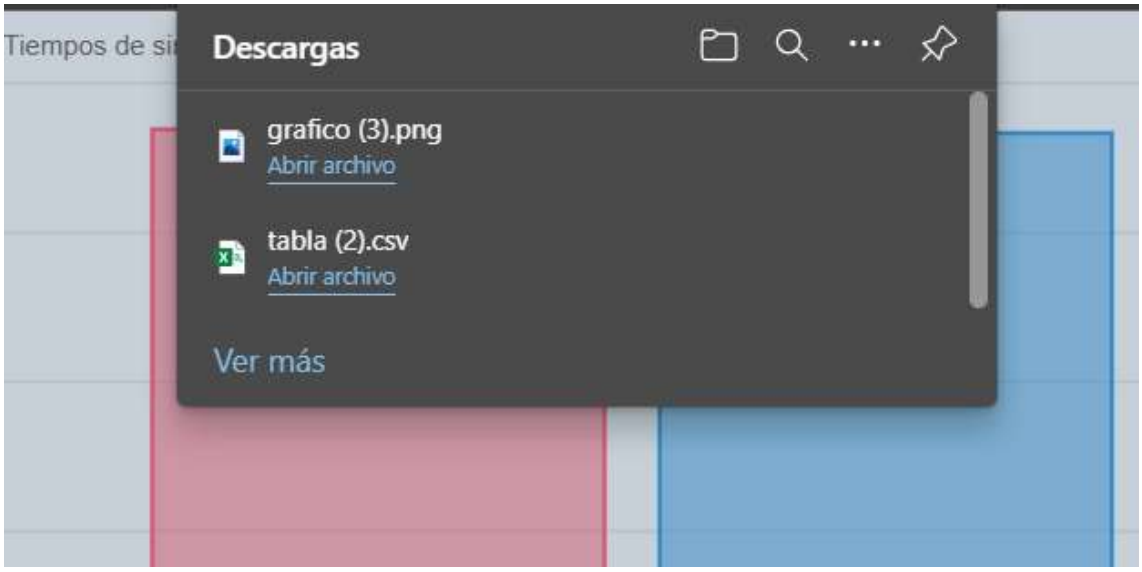


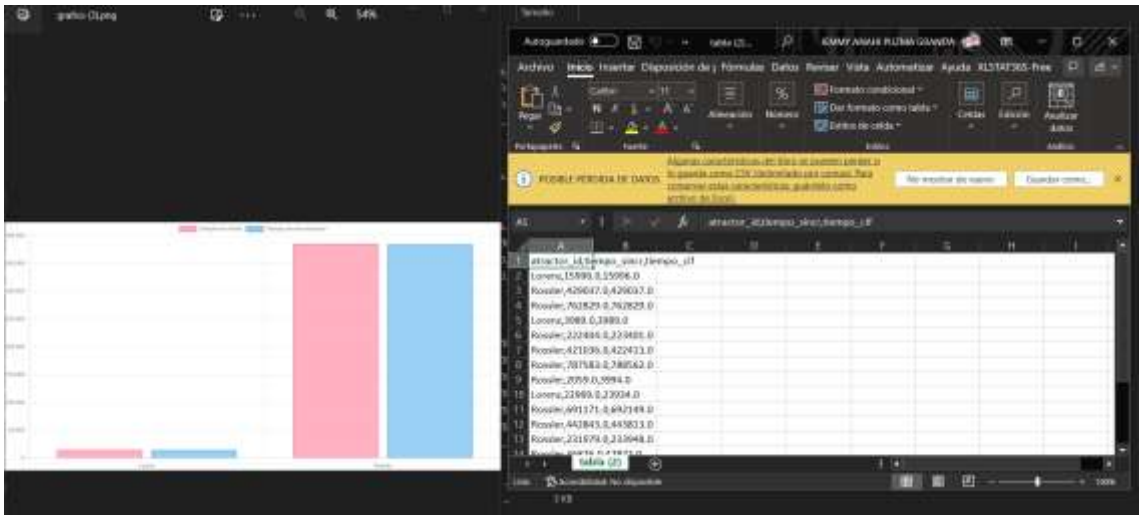
Observar los usuarios registrados.

Se puede visualizar los inicios de sesión con su ubicación.

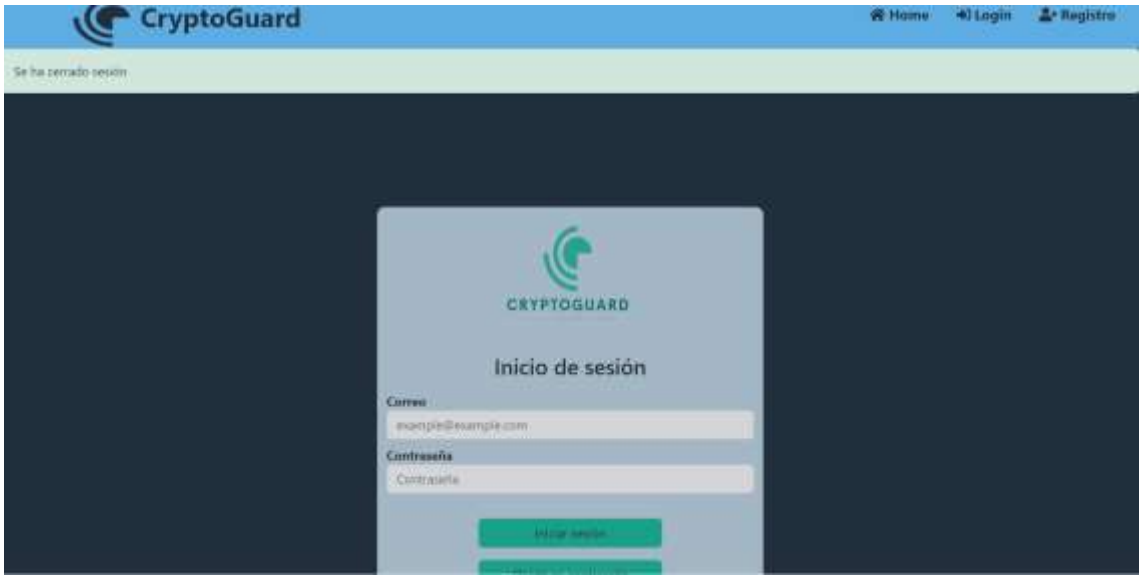
En los reportes se muestra las gráficas con los tiempos de sincronización, cifrado y descifrado.

22. Se puede descargar las tablas en formato CSV y las imágenes de las gráficas





23. Tanto el usuario como administrador puede cerrar sesión cuando ya no requiera seguir utilizando la aplicación web.



Anexo G: Texto plano

El texto que se utilizó para el cifrado y descifrado es:

“A medida que la crisis climática se intensifica, los incendios forestales han aumentado en frecuencia y severidad, devastando grandes áreas de tierra en todo el mundo. En particular, California ha sufrido enormemente. Los incendios forestales del estado, alimentados por el cambio climático y las prácticas de gestión de la tierra, han tenido un impacto sin precedentes en la biodiversidad de la región.

Los efectos directos de los incendios forestales son obvios: destrucción de hábitats, pérdida de vidas silvestres y humanas, y devastación de las comunidades. Sin embargo, los efectos a largo plazo pueden ser incluso más perjudiciales para la biodiversidad del estado.

La biodiversidad de California es impresionante, con más de 30,000 especies de plantas y animales, muchas de las cuales no se encuentran en ningún otro lugar del mundo. Sin embargo, los incendios forestales están amenazando este delicado equilibrio ecológico.

Las especies que dependen de los bosques y los hábitats de matorrales están en grave peligro debido a los incendios frecuentes. Los incendios pueden cambiar las composiciones de las especies en un ecosistema, favoreciendo a las especies que son resistentes al fuego y reduciendo la diversidad general de especies. Los incendios también pueden amenazar a las especies que ya están en peligro de extinción.

Los efectos de los incendios forestales también se extienden más allá de los bordes del fuego. La degradación del hábitat puede llevar a la fragmentación de la población, lo que puede disminuir la diversidad genética y aumentar la vulnerabilidad de las especies a las enfermedades y otros factores de estrés. Además, los animales que logran sobrevivir a los incendios a menudo enfrentan la escasez de alimentos y refugio en el período posterior al incendio.

Además, los incendios forestales pueden tener impactos significativos en los ecosistemas acuáticos. El calor extremo puede matar a los peces y otros organismos acuáticos, y las cenizas y los escombros del incendio pueden contaminar las fuentes de agua. Además, los incendios pueden cambiar los patrones de escorrentía, lo que puede llevar a inundaciones y erosión del suelo en las áreas quemadas, dañando aún más los ecosistemas acuáticos.

A pesar de estos impactos devastadores, hay motivos para el optimismo. Muchas especies tienen una capacidad sorprendente para recuperarse después de los incendios, y algunas incluso dependen de los incendios para su ciclo de vida. Por ejemplo, varias especies de plantas en California tienen semillas que solo germinan después de un incendio.

Además, los esfuerzos de conservación pueden ayudar a mitigar los impactos de los incendios forestales en la biodiversidad. Esto incluye la gestión del fuego para reducir el riesgo de incendios severos, la protección de los hábitats críticos y las especies en peligro de extinción, y la restauración de los ecosistemas después de los incendios.

Sin embargo, es claro que, para proteger verdaderamente la biodiversidad de California, debemos abordar la raíz del problema: el cambio climático. La lucha contra el cambio climático requiere un esfuerzo global para reducir las emisiones de gases de efecto invernadero y pasar a una economía baja en carbono. Solo a través de estos esfuerzos podremos prevenir los incendios forestales cada vez más severos y proteger la rica biodiversidad de California.

Los incendios forestales en California son un recordatorio de lo que está en juego en nuestra lucha contra el cambio climático. Estas devastadoras manifestaciones de un planeta en calentamiento no solo afectan a los humanos, sino a todas las formas de vida en nuestro planeta. La protección de la biodiversidad no es solo una cuestión de conservación, sino también de supervivencia: nuestra supervivencia".

El fragmento utilizado para la evaluación de la confidencialidad es:

“Los incendios forestales han aumentado en frecuencia y severidad, devastando grandes áreas de tierra en todo el mundo”.

Anexo H: Tabla de resultados completos del cifrado y descifrado

Resultados del cifrado

Nro	**Atractor**	**Tiempo sincronización µs**	**Tiempo cifrado µs**
1	Rossler	3660490	1496170
2	Rossler	2240740	1894170
3	Rossler	3454760	3427860
4	Rossler	3091610	3828160
5	Rossler	4460910	5678820
6	Rossler	3329640	4832020
7	Rossler	600390	662820
8	Rossler	179980	816290
9	Rossler	2203360	3018520
10	Rossler	1682690	2500580
11	Rossler	3119970	3291650
12	Rossler	2776990	5196160
13	Rossler	7791330	5739050
14	Rossler	239720	577280
15	Rossler	7790710	6743990
16	Rossler	6797270	7000370
17	Rossler	2577760	2582350
18	Rossler	319920	348840
19	Rossler	2128670	1813430
20	Rossler	1633080	2044580
21	Rossler	2137050	3456750
22	Rossler	7149650	6362450
23	Rossler	2206760	2399720
24	Rossler	3849310	5101210
25	Rossler	3211220	6615990
26	Lorenz	319870	155220
27	Lorenz	320140	653240

28	Lorenz	525320	139230
29	Lorenz	385500	615780
30	Lorenz	269630	514880
31	Lorenz	399800	140410
32	Lorenz	399780	163310
33	Lorenz	339890	6140
34	Lorenz	481050	988060
35	Lorenz	240230	53320
36	Lorenz	239870	323420
37	Lorenz	313570	531950
38	Lorenz	257260	130800
39	Lorenz	291840	624470
40	Lorenz	350350	253770
41	Lorenz	385350	412820
42	Lorenz	313570	252330
43	Lorenz	399730	1442190
44	Lorenz	247540	16970
45	Lorenz	481100	871760
46	Lorenz	419520	1212770
47	Lorenz	229750	438960
48	Lorenz	356030	247580
49	Lorenz	400670	1197450
50	Lorenz	295380	185050
51	Chen	399750	1138520
52	Chen	456450	626760
53	Chen	959680	303410
54	Chen	1121770	1083410
55	Chen	872140	860250
56	Chen	1563360	200190
57	Chen	1211560	921990
58	Chen	400500	902010
59	Chen	399760	198450
60	Chen	399720	610630
61	Chen	8875890	9645150
62	Chen	2935470	2144260

63	Chen	959410	9862490
64	Chen	799480	178340
65	Chen	2807550	2727660
66	Chen	719540	683130
67	Chen	1039620	289130
68	Chen	1528120	220910
69	Chen	816240	1057700
70	Chen	322160	131260
71	Chen	6301810	6725630
72	Chen	241730	400170
73	Chen	799810	1100360
74	Chen	8305320	7910920
75	Chen	9120270	248140
76	Sprott	504170	300970
77	Sprott	9741480	899750
78	Sprott	333180	17490
79	Sprott	310350	7360
80	Sprott	363940	282170
81	Sprott	327840	1133350
82	Sprott	319970	56610
83	Sprott	381320	69390
84	Sprott	251640	1224810
85	Sprott	399890	8969960
86	Sprott	399810	29880
87	Sprott	639650	201740
88	Sprott	276970	373150
89	Sprott	639950	343210
90	Sprott	248140	130510
91	Sprott	479730	695610
92	Sprott	319820	177520
93	Sprott	319840	142350
94	Sprott	412120	513530
95	Sprott	399750	673750
96	Sprott	319620	637060
97	Sprott	320090	11850

98	Sprott	361660	687510
99	Sprott	244760	324260
100	Sprott	319710	813030

Resultados del descifrado

Nro	**Atractor**	**Tiempo descifrado µs**
1	Rossler	5529110
2	Rossler	2807210
3	Rossler	4746240
4	Rossler	3820010
5	Rossler	3070580
6	Rossler	4906160
7	Rossler	2126780
8	Rossler	2618070
9	Rossler	2776890
10	Rossler	3198720
11	Rossler	3710240
12	Rossler	4237580
13	Rossler	4058760
14	Rossler	2365830
15	Rossler	5390830
16	Rossler	3197300
17	Rossler	2963230
18	Rossler	1782130
19	Rossler	4519650
20	Rossler	3916780
21	Rossler	4327550
22	Rossler	4383640
23	Rossler	2657930
24	Rossler	5006570
25	Rossler	6879140
26	Lorenz	1846800
27	Lorenz	2382140
28	Lorenz	2480070
29	Lorenz	2177980

30	Lorenz	8129190
31	Lorenz	1903490
32	Lorenz	1740100
33	Lorenz	1899270
34	Lorenz	1765100
35	Lorenz	1698570
36	Lorenz	1698490
37	Lorenz	1814860
38	Lorenz	2045600
39	Lorenz	1690010
40	Lorenz	2430620
41	Lorenz	7513990
42	Lorenz	1727630
43	Lorenz	7657560
44	Lorenz	1856510
45	Lorenz	2267540
46	Lorenz	8133810
47	Lorenz	1646120
48	Lorenz	1779330
49	Lorenz	1861930
50	Lorenz	1803150
51	Chen	1882040
52	Chen	7367780
53	Chen	2811240
54	Chen	6788470
55	Chen	2843170
56	Chen	2865340
57	Chen	6769860
58	Chen	2363050
59	Chen	2200710
60	Chen	2129330
61	Chen	7528830
62	Chen	4604470
63	Chen	2099710
64	Chen	7419640

65	Chen	4973340
66	Chen	1967780
67	Chen	2100740
68	Chen	6273500
69	Chen	2351180
70	Chen	1903110
71	Chen	4174940
72	Chen	2372750
73	Chen	1953830
74	Chen	6124360
75	Chen	2953410
76	Sprott	1986910
77	Sprott	1863990
78	Sprott	2230620
79	Sprott	2569460
80	Sprott	7677520
81	Sprott	1803730
82	Sprott	1894520
83	Sprott	2530600
84	Sprott	7988750
85	Sprott	2608590
86	Sprott	2258940
87	Sprott	2310050
88	Sprott	2208250
89	Sprott	7711140
90	Sprott	2362910
91	Sprott	1788720
92	Sprott	2180550
93	Sprott	1886380
94	Sprott	1916770
95	Sprott	1969910
96	Sprott	2479950
97	Sprott	1940000
98	Sprott	1792230
99	Sprott	2232190

100	Sprott	7148250

Anexo I: Tabla de resultados de los caracteres del texto plano, cifrado y descifrado

Rossler

Información del texto plano, cifrado y descifrado.

Nro	Texto plano	Texto cifrado	Texto descifrado
1	76	7,86743801104064	75,99
2	111	7,92394819142514	111,0015
3	115	7,85707143834833	115,005
4	32	7,44724231823095	32,0025
5	105	7,64749863941912	105,009
6	110	7,57938144914527	110,007
7	99	7,44683501303916	98,991
8	101	7,36380677647765	101,0055
9	110	7,30664730720773	110,007
10	100	7,17351021883958	100,011
11	105	7,09775207498257	105,009
12	111	7,02453227398611	111,0015
13	115	6,94221291444625	115,005
14	32	6,51745864184454	32,0025
15	102	6,69153647689665	102
16	111	6,62531562639889	111,0015
17	114	6,53456727757006	114,0105
18	101	6,38006437708824	101,0055
19	115	6,33058139621558	115,005
20	116	6,22929408358353	115,9995
21	97	6,04887920737430	97,002
22	108	5,98541428877764	107,9925
23	101	5,85087732872304	101,0055
24	115	5,79814652998303	115,005
25	32	5,36460001681238	32,0025
26	104	5,53851555432845	103,989

27	97	5,40247026984906	97,002
28	110	5,34464037838607	110,007
29	32	4,92980091444535	32,0025
30	97	5,07572547220771	97,002
31	117	5,04518595606290	116,994
32	109	4,90505234334088	109,0125
33	101	4,76499246093450	101,0055
34	110	4,69187177733828	110,007
35	116	4,60725321144143	115,9995
36	97	4,42499695921460	97,002
37	100	4,32946033922114	100,011
38	111	4,26569765766922	111,0015
39	32	3,84956009350496	32,0025
40	101	4,01439560383130	101,0055
41	110	3,94454884972707	110,007
42	32	3,53416114233765	32,0025
43	102	3,70487040891669	102
44	114	3,64891117831855	114,0105
45	101	3,49561458527707	101,0055
46	99	3,38620839265832	98,991
47	117	3,35611703074482	116,994
48	101	3,19356165249756	101,0055
49	110	3,12986020364979	110,007
50	99	2,98852750641321	98,991
51	105	2,91487535552312	105,009
52	97	2,78711262531256	97,002
53	32	2,43674538648724	32,0025
54	121	2,69117703127003	120,9975
55	32	2,24850840559683	32,0025
56	115	2,48123794707134	115,005
57	101	2,33446182742494	101,0055
58	118	2,31007409827626	117,9885
59	101	2,15336683904300	101,0055
60	114	2,11513030592365	114,0105
61	105	1,99145308093766	105,009

62	100	1,88432222008805	100,011
63	97	1,78582339978878	97,002
64	100	1,71174106077940	100,011
65	44	1,40695854883012	43,9875
66	32	1,27565825162086	32,0025
67	100	1,45882173125641	100,011
68	101	1,37992985195697	101,0055
69	118	1,36446290253669	117,9885
70	97	1,20080071335372	97,002
71	115	1,19072276748172	115,005
72	116	1,11460830591517	115,9995
73	97	0,96073642667911	97,002
74	110	0,93298617776724	110,007
75	100	0,81563664388138	100,011
76	111	0,78116702698939	111,0015
77	32	0,39435672075858	32,0025
78	103	0,59628537895675	102,9945
79	114	0,56353297794405	114,0105
80	97	0,42137987340570	97,002
81	110	0,39740685149855	110,007
82	100	0,28369517460378	100,011
83	101	0,21352662189384	101,0055
84	115	0,19478352493440	115,005
85	32	-0,20395120144803	32,0025
86	225	0,48010596720462	225,012
87	114	-0,02766081290176	114,0105
88	101	-0,15076673570709	101,0055
89	97	-0,23822633095530	97,002
90	115	-0,23905345337314	115,005
91	32	-0,63566127512828	32,0025
92	100	-0,43976228132951	100,011
93	101	-0,50636826833695	101,0055
94	32	-0,84719034465644	32,0025
95	116	-0,58773893419914	115,9995
96	105	-0,70052378169500	105,009

97	101	-0,78565396005696	101,0055
98	114	-0,80383787950133	114,0105
99	114	-0,87278329823846	114,0105
100	97	-1,00819733455715	97,002
101	32	-1,33158648013534	32,0025
102	101	-1,12925661441869	101,0055
103	110	-1,16201301991831	110,007
104	32	-1,53576039828749	32,0025
105	116	-1,27400288704695	115,9995
106	111	-1,36104407683630	111,0015
107	100	-1,47138702907869	100,011
108	111	-1,49533429395365	111,0015
109	32	-1,87198792858132	32,0025
110	101	-1,66804951532940	101,0055
111	108	-1,70712018016141	107,9925
112	32	-2,07140061095233	32,0025
113	109	-1,83549107570457	109,0125
114	117	-1,87009144060383	116,994
115	110	-1,96320118786075	110,007
116	100	-2,06791943329026	100,011
117	111	-2,09014494358597	111,0015
118	46	-2,41017615325253	46,002

Lorenz

Información del texto plano, cifrado y descifrado.

Nro	Texto plano	Texto cifrado	Texto descifrado
1	76	-6,93800314509052	75,99
2	111	-6,81436187645274	111,0015
3	115	-6,82350279035299	115,005
4	32	-7,18481470158141	32,0025
5	105	-6,94502658767896	105,009
6	110	-6,98230772045485	110,007
7	99	-7,09236677486122	98,991
8	101	-7,16085000967341	101,0055
9	110	-7,21093865477001	110,007

10	100	-7,34394568115708	100,011
11	105	-7,42591217249746	105,009
12	111	-7,51100356058409	111,0015
13	115	-7,61010603112878	115,005
14	32	-8,05572344888340	32,0025
15	102	-7,90567519009758	102
16	111	-7,99809530238161	111,0015
17	114	-8,11613343305820	114,0105
18	101	-8,29785797218262	101,0055
19	115	-8,37326184025137	115,005
20	116	-8,49787130783185	115,9995
21	97	-8,69765816013343	97,002
22	108	-8,77515541045230	107,9925
23	101	-8,91697662123428	101,0055
24	115	-8,96883871210402	115,005
25	32	-9,39198792638720	32,0025
26	104	-9,19682840154580	103,989
27	97	-9,29955255905827	97,002
28	110	-9,31087231383277	110,007
29	32	-9,66504992285252	32,0025
30	97	-9,44352716837212	97,002
31	117	-9,38295152137337	116,994
32	109	-9,41609796998067	109,0125
33	101	-9,43318533153729	101,0055
34	110	-9,36748609326210	110,007
35	116	-9,29782913219333	115,9995
36	97	-9,31099502870104	97,002
37	100	-9,22350408042022	100,011
38	111	-9,09139751245257	111,0015
39	32	-9,30011273265205	32,0025
40	101	-8,91775376929017	101,0055
41	110	-8,76155823120125	110,007
42	32	-8,93906223584342	32,0025
43	102	-8,53036475691441	102
44	114	-8,34499275801790	114,0105

45	101	-8,25536831778354	101,0055
46	99	-8,12197873521972	98,991
47	117	-7,91105035451813	116,994
48	101	-7,83592658813390	101,0055
49	110	-7,66675036520704	110,007
50	99	-7,58135100467835	98,991
51	105	-7,43563531945247	105,009
52	97	-7,35248260558757	97,002
53	32	-7,50134306040686	32,0025
54	121	-7,05563910386549	120,9975
55	32	-7,31796904423620	32,0025
56	115	-6,91641252646121	115,005
57	101	-6,90633722296197	101,0055
58	118	-6,78620626592910	117,9885
59	101	-6,81098597127364	101,0055
60	114	-6,73005346247497	114,0105
61	105	-6,74740386346145	105,009
62	100	-6,76105679038109	100,011
63	97	-6,77886193061195	97,002
64	100	-6,78490355244703	100,011
65	44	-7,03410384013283	43,9875
66	32	-7,12202499650435	32,0025
67	100	-6,90737009995527	100,011
68	101	-6,96628274482928	101,0055
69	118	-6,97284553560632	117,9885
70	97	-7,13817754660738	97,002
71	115	-7,15993090137048	115,005
72	116	-7,25708667012837	115,9995
73	97	-7,44065033031255	97,002
74	110	-7,50594708352974	110,007
75	100	-7,66781737208895	100,011
76	111	-7,75281298710844	111,0015
77	32	-8,19509420569720	32,0025
78	103	-8,05242843280042	102,9945
79	114	-8,14699084906471	114,0105

80	97	-8,35216757363691	97,002
81	110	-8,43896183367502	110,007
82	100	-8,61380358395914	100,011
83	101	-8,74186293445770	101,0055
84	115	-8,81366761677319	115,005
85	32	-9,25902455053602	32,0025
86	225	-8,61354536035275	225,012
87	114	-9,15027544996873	114,0105
88	101	-9,29122597537702	101,0055
89	97	-9,38400779054197	97,002
90	115	-9,37636619054957	115,005
91	32	-9,74961507242752	32,0025
92	100	-9,51456899879611	100,011
93	101	-9,52557160600694	101,0055
94	32	-9,79391886206859	32,0025
95	116	-9,44497585647318	115,9995
96	105	-9,45138608849171	105,009
97	101	-9,41367259498717	101,0055
98	114	-9,29323069488208	114,0105
99	114	-9,20871258886671	114,0105
100	97	-9,17700449998671	97,002
101	32	-9,32099743505273	32,0025
102	101	-8,92855295615509	101,0055
103	110	-8,76216555358501	110,007
104	32	-8,92952329581218	32,0025
105	116	-8,45596840084006	115,9995
106	111	-8,32765923920528	111,0015
107	100	-8,22093506331881	100,011
108	111	-8,02788448681921	111,0015
109	32	-8,18931843849200	32,0025
110	101	-7,77354801369018	101,0055
111	108	-7,60566736355607	107,9925
112	32	-7,76924151471477	32,0025
113	109	-7,34009880959440	109,0125
114	117	-7,19002750463898	116,994

115	110	-7,10797596018651	110,007
116	100	-7,04785579785035	100,011
117	111	-6,91624738264460	111,0015
118	46	-7,09400700035627	46,002

Chen
Información de texto plano, cifrado y descifrado.

Nro	Texto plano	Texto cifrado	Texto descifrado
1	76	-8,36718919160779	75,99
2	111	-7,91027340445434	111,0015
3	115	-7,37307853206051	115,005
4	32	-7,01140739370766	32,0025
5	105	-5,91152492509744	105,009
6	110	-4,99154893536060	110,007
7	99	-4,08492330403017	98,991
8	101	-3,11066810324026	101,0055
9	110	-2,11954316746969	110,007
10	100	-1,23398202760202	100,011
11	105	-0,33470826681954	105,009
12	111	0,51533721385190	111,0015
13	115	1,30155289672409	115,005
14	32	1,69179239519970	32,0025
15	102	2,63167225170632	102
16	111	3,28865745442470	111,0015
17	114	3,88656819992857	114,0105
18	101	4,39501895967025	101,0055
19	115	4,99187855361461	115,005
20	116	5,52922607180263	115,9995
21	97	5,98806987998390	97,002
22	108	6,57189362707675	107,9925
23	101	7,09879288201237	101,0055
24	115	7,72606843548136	115,005
25	32	7,99334811517105	32,0025
26	104	8,88841996461280	103,989
27	97	9,48997857260750	97,002
28	110	10,17821643156760	110,007

29	32	10,50513590417400	32,0025
30	97	11,37041399455790	97,002
31	117	12,01321417248430	116,994
32	109	12,47168869792180	109,0125
33	101	12,82292041281060	101,0055
34	110	13,09957668098600	110,007
35	116	13,19066144475420	115,9995
36	97	12,98306250470490	97,002
37	100	12,64377010807590	100,011
38	111	12,11331885137190	111,0015
39	32	11,01751617267590	32,0025
40	101	10,31363072652700	101,0055
41	110	9,22124676560106	110,007
42	32	7,67684715252763	32,0025
43	102	6,64664783415895	102
44	114	5,36515041309938	114,0105
45	101	3,99813930677652	101,0055
46	99	2,71536785473491	98,991
47	117	1,57211258040478	116,994
48	101	0,36812903301391	101,0055
49	110	-0,66095847587770	110,007
50	99	-1,69308733413455	98,991
51	105	-2,58858350137160	105,009
52	97	-3,47756378541836	97,002
53	32	-4,53820465132242	32,0025
54	121	-4,95300298983843	120,9975
55	32	-6,03301285552783	32,0025
56	115	-6,41332199783935	115,005
57	101	-7,15412872494267	101,0055
58	118	-7,75588968566501	117,9885
59	101	-8,47213023269290	101,0055
60	114	-9,04683955733813	114,0105
61	105	-9,67431051071977	105,009
62	100	-10,23842405817890	100,011
63	97	-10,72871107353830	97,002

64	100	-11,10753439301400	100,011
65	44	-11,60610264485790	43,9875
66	32	-11,79633820834140	32,0025
67	100	-11,51597319549010	100,011
68	101	-11,32566510356150	101,0055
69	118	-10,89206431407280	117,9885
70	97	-10,42870210957310	97,002
71	115	-9,64605630987855	115,005
72	116	-8,78549299616550	115,9995
73	97	-7,88780825979612	97,002
74	110	-6,78249022668844	110,007
75	100	-5,71958595677874	100,011
76	111	-4,55884742814626	111,0015
77	32	-3,76327605866947	32,0025
78	103	-2,41366301161136	102,9945
79	114	-1,34881324967106	114,0105
80	97	-0,45249665809530	97,002
81	110	0,49949617467911	110,007
82	100	1,30061623763290	100,011
83	101	2,08921929597849	101,0055
84	115	2,88095704260621	115,005
85	32	3,25396833242247	32,0025
86	225	4,68159733697179	225,012
87	114	4,90013225166714	114,0105
88	101	5,49673598294507	101,0055
89	97	6,13232660580998	97,002
90	115	6,86655803588963	115,005
91	32	7,22384909324586	32,0025
92	100	8,19681237372019	100,011
93	101	8,93144554029268	101,0055
94	32	9,41277144588712	32,0025
95	116	10,50665631320380	115,9995
96	105	11,22550343153420	105,009
97	101	11,94671566162570	101,0055
98	114	12,67923394080470	114,0105

99	114	13,26756003041030	114,0105
100	97	13,65250109662880	97,002
101	32	13,66675247278340	32,0025
102	101	13,98089952804360	101,0055
103	110	13,79978469631450	110,007
104	32	12,99790264556210	32,0025
105	116	12,55133142688230	115,9995
106	111	11,49605209818760	111,0015
107	100	10,19652292039630	100,011
108	111	8,81491039600431	111,0015
109	32	6,97108255620209	32,0025
110	101	5,65665147269313	101,0055
111	108	4,09981998110601	107,9925
112	32	2,25995469448324	32,0025
113	109	1,09230838629058	109,0125
114	117	-0,25529440424944	116,994
115	110	-1,56202495077839	110,007
116	100	-2,77958495314635	100,011
117	111	-3,81748869669625	111,0015
118	46	-5,06240305395864	46,002

Sprott

Información del texto plano, cifrado y descifrado.

Nro	Texto plano	Texto cifrado	Texto descifrado
1	76	2,28980446586058	75,99
2	111	2,42607552251276	111,0015
3	115	2,43997690986897	115,005
4	32	2,11190252578857	32,0025
5	105	2,39484776474017	105,009
6	110	2,41030955580947	110,007
7	99	2,36218639430670	98,991
8	101	2,36437836666128	101,0055
9	110	2,39318716834120	110,007
10	100	2,34671611458726	100,011
11	105	2,35827014380894	105,009

12	111	2,37295581354681	111,0015
13	115	2,37908128896692	115,005
14	32	2,04325632391348	32,0025
15	102	2,30669223460743	102
16	111	2,33020186613883	111,0015
17	114	2,32949955196017	114,0105
18	101	2,26530106664415	101,0055
19	115	2,30632357222362	115,005
20	116	2,29568555848090	115,9995
21	97	2,20600677760027	97,002
22	108	2,23330817363777	107,9925
23	101	2,18951180729892	101,0055
24	115	2,22744077654471	115,005
25	32	1,88441913357097	32,0025
26	104	2,14867179872444	103,989
27	97	2,10272447193108	97,002
28	110	2,13470354221855	110,007
29	32	1,80933599591481	32,0025
30	97	2,04434932409942	97,002
31	117	2,10247142987303	116,994
32	109	2,05053053599443	109,0125
33	101	1,99815509341376	101,0055
34	110	2,01217369120496	110,007
35	116	2,01411496837218	115,9995
36	97	1,91780752797211	97,002
37	100	1,90757985395977	100,011
38	111	1,92846023112777	111,0015
39	32	1,59627666847090	32,0025
40	101	1,84435682626769	101,0055
41	110	1,85702794713045	110,007
42	32	1,52841679123508	32,0025
43	102	1,78014957590152	102
44	114	1,80445191965685	114,0105
45	101	1,73064879087487	101,0055
46	99	1,69996446104948	98,991

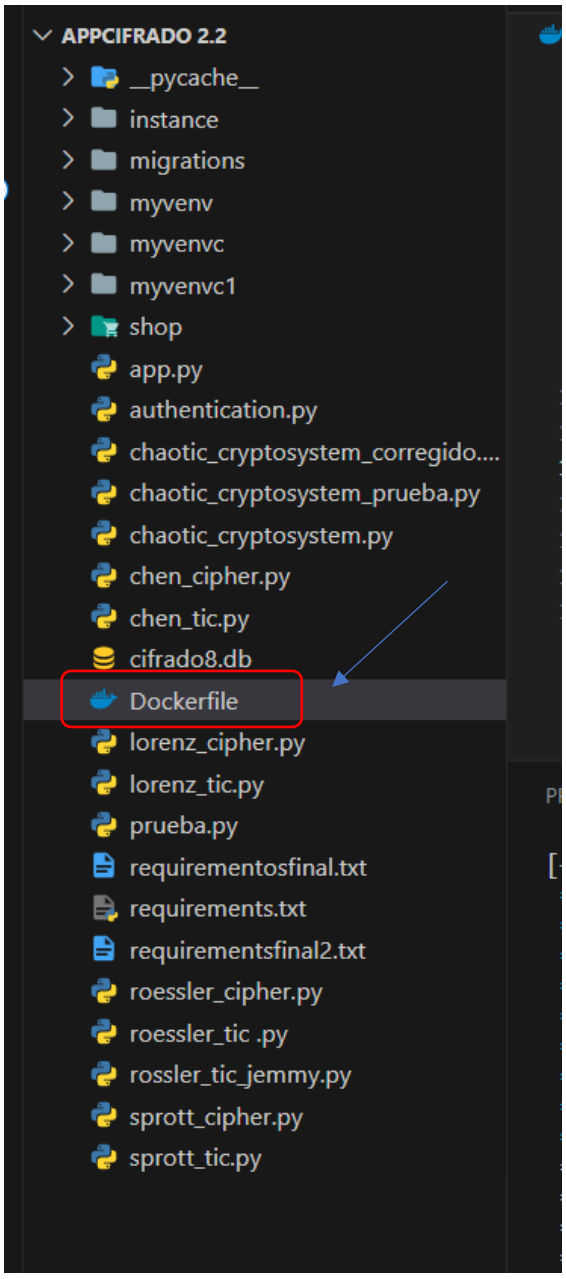
47	117	1,74782246272438	116,994
48	101	1,66244555206906	101,0055
49	110	1,67515567606047	110,007
50	99	1,60947394420172	98,991
51	105	1,61072060468365	105,009
52	97	1,55711502487191	97,002
53	32	1,28017567598197	32,0025
54	121	1,60732012178653	120,9975
55	32	1,23666501118438	32,0025
56	115	1,54072607444728	115,005
57	101	1,46461812295055	101,0055
58	118	1,51025505218543	117,9885
59	101	1,42294984784490	101,0055
60	114	1,45351459477094	114,0105
61	105	1,39806048854931	105,009
62	100	1,35859784953718	100,011
63	97	1,32723613911076	97,002
64	100	1,31978397792255	100,011
65	44	1,08114916596157	43,9875
66	32	1,01553870421563	32,0025
67	100	1,26395881774012	100,011
68	101	1,24991497994512	101,0055
69	118	1,29891193792001	117,9885
70	97	1,19935373862286	97,002
71	115	1,25304375577072	115,005
72	116	1,24038471727536	115,9995
73	97	1,14967873307854	97,002
74	110	1,18482732324995	110,007
75	100	1,13013144622030	100,011
76	111	1,15809152703112	111,0015
77	32	0,83350748549241	32,0025
78	103	1,09747876414773	102,9945
79	114	1,12660435595575	114,0105
80	97	1,04618283160515	97,002
81	110	1,08381236638867	110,007

82	100	1,03159076656962	100,011
83	101	1,02281549518201	101,0055
84	115	1,06538369721270	115,005
85	32	0,72789222412064	32,0025
86	225	1,47313765765525	225,012
87	114	1,02651633294166	114,0105
88	101	0,96452436080655	101,0055
89	97	0,93815764932366	97,002
90	115	0,99841192456302	115,005
91	32	0,66288275053263	32,0025
92	100	0,91986554830552	100,011
93	101	0,91435561432907	101,0055
94	32	0,63464813791723	32,0025
95	116	0,95523821792922	115,9995
96	105	0,90362087864156	105,009
97	101	0,87969108482274	101,0055
98	114	0,92274375602236	114,0105
99	114	0,91507378008854	114,0105
100	97	0,84097602592943	97,002
101	32	0,57894535553611	32,0025
102	101	0,84267663528569	101,0055
103	110	0,87136474654467	110,007
104	32	0,55910459559330	32,0025
105	116	0,88239112289309	115,9995
106	111	0,85691931171964	111,0015
107	100	0,80818419618397	100,011
108	111	0,84588086866562	111,0015
109	32	0,53090448668116	32,0025
110	101	0,79655027921177	101,0055
111	108	0,81921355251379	107,9925
112	32	0,51668969543572	32,0025
113	109	0,81437418426532	109,0125
114	117	0,84156258713007	116,994
115	110	0,81025056797392	110,007
116	100	0,76733389013292	100,011

117	111	0,80690841953203	111,0015
118	46	0,54867012752472	46,002

Anexo J: Despliegue de la aplicación

Primero se debe crear un archivo sin extensión en la raíz donde se encuentra la app.py



Después dentro del archivo se debe colocar la siguiente configuración

```dockerfile
# Usar una imagen base de Python
FROM python:3.8

# Establecer el directorio de trabajo en el contenedor
WORKDIR /usr/src/app

# Copiar requirements.txt y instalar las dependencias
COPY requirementsfinal2.txt .
RUN pip install --no-cache-dir -r requirementsfinal2.txt

# Copiar el resto del código fuente
COPY . .

# Comando para ejecutar al iniciar el contenedor
CMD [ "python", "app.py" ]
```

Se configura en el archivo app.py para que inicie con cualquier puerto

```python
from shop import app

# if __name__ =="__main__":
#     app.run(debug=True)

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)  # El puerto 5000 es el predeterminado para Flask

```

Después se ingresa el siguiente comando para crear la imagen Docker

```
(myvenvc1) PS D:\appcifrado 2.2> docker build -t cryptoguard:latest .
>>
```

Por último, se ejecuta la imagen Docker

```
(myvenvc1) PS D:\appcifrado 2.2> docker run -p 5000:5000 -it cryptoguard
>>
```

En la aplicación de Imagen Docker de Windows se puede observar que se ha creado la imagen

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 10/01/2024

INFORMACIÓN DE LA AUTORA
Nombres – Apellidos: Jemmy Anahí Puzma Granda
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Software
Título a optar: Ingeniera de Software
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.

UNIDAD DE PROCESOS TÉCNICOS DBRA ESPOCH