UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO ENSENADA

CIFRADO CAÓTICO DE SEÑALES ELECTROFISIOLÓGICAS BASADO EN MAPA DE USHIO PARA TELEMETRÍA SEGURA

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de

INGENIERO EN ELECTRÓNICA

presenta:

JOSÉ ALFONSO QUINTANA IBARRA

ENSENADA, BAJA CALIFORNIA, MÉXICO, FEBRERO 2018.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO ENSENADA

CIFRADO CAÓTICO DE SEÑALES ELECTROFISIOLÓGICAS BASADO EN MAPA DE USHIO PARA TELEMETRÍA SEGURA

TESIS

Que para obtener el grado de Ingeniero en Electrónica presenta:

JOSÉ ALFONSO QUINTANA IBARRA

Aprobada por el siguiente comité:

Dr. Miguel Ángel Murillo Escobar
Director del comité

Dra. Rosa Martha López Gutiérrez
Miembro del comité

Dr. César Cruz Hernández
Miembro del comité

Dra. Liliana Cardoza Avendaño
Miembro del comité

M.C. José Antonio Michel Macarty
Miembro del comité

ENSENADA, BAJA CALIFORNIA, MÉXICO. FEBRERO 2018.

RESUMEN de la tesis de **JOSÉ ALFONSO QUINTANA IBARRA**, presentada como requerimiento parcial para obtener el grado de Ingeniero en Electrónica, del programa de licenciatura de la Universidad Autónoma de Baja California. Ensenada, Baja California, México. Febrero 2018.

CIFRADO CAÓTICO DE SEÑALES ELECTROFISIOLÓGICAS BASADO EN MAPA DE USHIO PARA TELEMETRÍA SEGURA

Resumen aprobado por:

Dr. Miguel Ángel Murillo Escobar
Director

En este trabajo de tesis de licenciatura, se diseña e implementa un algoritmo de cifrado caótico para encriptar señales electrofisiológicas como: electrocardiograma (ECG), electroencefalograma (EEG) y presión de la sangre (BP), para brindar confidencialidad a la información en aplicaciones de telemedicina.

Primeramente, se estudian cinco sistemas caóticos de tiempo discreto y se determina utilizar el mapa 2D de Ushio, ya que presenta resultados excelentes en la pruebas de tiempo de cálculos, aleatoriedad y uniformidad. Posteriormente, se diseña e implementa a nivel MatLab el algoritmo criptográfico basado en caos y en la arquitectura de confusión y difusión. Las señales electrofisiológicas son adquiridas de una base de datos de internet.

Finalmente, la información cifrada es sometida a un análisis de seguridad estadístico y diferencial como: correlación, autocorrelación, entropía, frecuencia flotante, histogramas y prueba de NPCR-UACI. Los resultados muestran una alta resistencia del algoritmo criptográfico ante este tipo de ataques y su potencial uso en aplicaciones de telemedicina, particularmente en telemetría.

Palabras clave: cifrado caótico, mapa de Ushio, análisis de seguridad, telemetría.

Abstract of the thesis presented by **JOSÉ ALFONSO QUINTANA IBARRA**, as a partial requirement to obtain the bachelor degree in Electronics Engineering, of the program of Bachelor's of the Autonomous University of Baja California. Ensenada, Baja California, México. February 2018.

CHAOTIC CIPHER OF ELECTROPHYSIOLOGICAL SIGNALS BASED ON USHIO MAP FOR SECURE TELEMETRY

Abstract approved by:

Dr. Miguel Ángel Murillo Escobar
Director

In this thesis work, a cryptographic algorithm based on chaos is designed and implemented to encrypt electrophysiological signals such as electrocardiogram (ECG), electroencephalogram (EEG) and blood pressure (BP), to provide confidentiality at the information in telemedicine applications.

Firstly, we study five chaotic systems of discrete time and the Ushio map 2D is selected, because it offers excellent results in time processing, randomness, and uniformity. Then, the cryptographic algorithm is implemented at MatLab based on confusion and diffusion architecture. The electrophysiological signals are acquired from a database on internet.

Finally, the encrypted information is tested with several statistical and differentials security analysis such as: correlation, autocorrelation, entropy, floating frequency, histograms, and NPCR-UACI. The results show high resistance of the cryptographic algorithm against this kinds of attacks and its potential use in applications of telemedicine, particularly at telemetry.

Keywords: cryptographic algorithm, Ushio map, confusion, diffusion, security analysis.

A mis padres Isela Ibarra Mendoza y Héctor Pascual Quintana González.

A mis hermanos Héctor Alejandro y Leonardo Gabriel Quintana Ibarra.

Agradecimientos

A mi familia, en especial a mi abuelita **María** por su apoyo y enseñanzas.

A la memoria de mis abuelos **Victoria González, Alfonso Quintana y José Ibarra**.

A la **Dra. Rosa Martha López Gutiérrez,** por su invitación a la realización de este trabajo, su amabilidad, sus consejos, su interés en mi formación y su ayuda durante toda la carrera.

Al **Dr. Miguel Ángel Murillo Escobar,** por sus comentarios, enseñanzas, su atención, sus consejos y su guía durante este trabajo. Fue un honor trabajar con usted. ¡Muchas gracias!

Al **Dr. César Cruz Hernández,** por su guía durante la realización de este trabajo, sus consejos y por ayudar al fortalecimiento de mi aprendizaje.

A mi comité de evaluación, **Dra. Rosa Martha López Gutiérrez, Dra. Liliana Cardoza Avendaño, Dr. César Cruz Hernández, M.C. José Antonio Michel Macarty** por sus consejos y comentarios, permitiendo la mejora de este trabajo y de mi aprendizaje.

A la **UABC**, por ser mi segunda casa durante estos cuatro años de aprendizaje, a los **Profesores** por ser parte de ello y por ser el lugar donde conocí excelentes personas.

A mis amigos, **Gerardo A., Víctor, Daniel, Óscar, Esgar, Gerardo, Jesús, Carlos, Aldo, Héctor, Eduardo A., Luis G., Miguel Á., Antonio V., Eduardo, York, Ricardo, Rene, Ulises, Antonio, Luis M., Rigoberto, Hugo, Michael, Carolina, Patricia, Juan, David, Roberto, Alan, Ramón, Elizvan y Francisco,** por su amistad, su ayuda en los momentos que los necesite y por todo lo que aprendí y espero seguir aprendiendo de cada uno de ustedes.

Al **Consejo Nacional de Ciencia y Tecnología (CONACyT),** por el apoyo económico que me fue otorgado para el desarrollo de mi trabajo, a través del Proyecto de Grupos de Investigación en Ciencia Básica, Referencia 166654.

A todos aquellos que de alguna manera fueron parte de la culminación de una etapa más en mi vida y que permitieron que este trabajo fuese lo más ordenado, claro y coherente a pesar de ser de auténtico caos. ¡Gracias!

Ensenada, B.C., México.
Febrero de 2018.

José Alfonso Quintana Ibarra.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Capítulo 1

Introducción

Actualmente, las diversas plataformas de comunicación (como correo electrónico, internet, etc.) son empleadas por millones de usuarios para transmitir y recibir infinidad de información digital multimedia (como imágenes, video, texto, audio, etc.). Estos tipos de sistemas de comunicación utilizan canales inseguros que ponen en riesgo la información de las personas, la cual, puede caer en manos equivocadas para implementar fraudes, robo de identidad, actividades ilegales, etc. Además, las personas tienden a compartir cada vez más información personal y basta solo con revisar en las plataformas sociales y así de fácil obtener información muy valiosa, por ejemplo en la figura 1.1 y la figura 1.2 se muestra que usuarios comparten información de tarjetas de crédito a través de canales inseguros, como internet.

Esto se debe principalmente en que cuándo se elabora un nuevo software o sistema, primero se desarrolla el producto y por último se le añaden métodos de seguridad de la información, es decir, en muchas ocasiones no se trabaja en conjunto. Es por ello que cuándo se detecta una falla, se busca la manera de solucionarlo y posteriormente entran en cuestión las nuevas actualizaciones de sistema, dónde se incluye la última versión del sistema ya con la falla contrarrestada. Otro factor a tomar en cuenta, es que usualmente la protección de la información se basa en un nombre de usuario y de contraseña como método de autenticación, lo cual, por más complejas que estas sean, pueden ser robadas desde un correo falso (haciendo creer que el correo es de alguna de tus compañías de preferencia) o mediante herramientas con algo más de complejidad, por ejemplo un ataque dirigido mediante software malicioso (virus). Por lo tanto, el empleo de usuario y contraseña no es conveniente para el envío de información privada.

Además, los metadatos que se generan en la información que compartimos pueden poner en riesgo nuestra seguridad. Al emplear las diversas herramientas digitales que nos facilitan la vida hoy en día (software para desarrollo de documentos, las cámaras de nuestros dispositivos móviles, etc.), se generan metadatos como: título, categoría, autor, lenguaje, palabras claves y datos relevantes de contacto [1], mientras que para imágenes o videos se incluye una descripción basada en información geográfica y geométrica [2]. En la actualidad, la comunidad científica está buscando el camino para automatizar el análisis y reconocimiento de documentos por al menos dos razones: el número

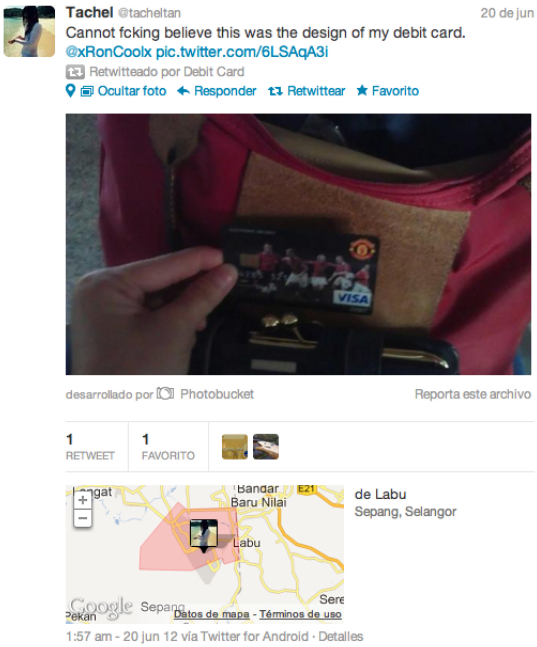

Figura 1.1: Usuario de Twitter compartiendo una imagen de su tarjeta de crédito además de incluir su ubicación.

Figura 1.2: Usuario de Twitter inconforme debido a nombre erróneo en su tarjeta de crédito.

de documentos es muy extenso y diverso (realizar esta tarea manualmente requiere de mucho tiempo y dinero) y la segunda es por la riqueza del contenido en términos de conocimiento [3].

Existen áreas en desarrollo en las que es de suma importancia contar con estructuras que briden seguridad a los usuarios debido al manejo de información sumamente confidencial o privada. Un ejemplo de ellas es en telemedicina que literalmente significa medicina a distancia, la cual, se define como el uso de las tecnologías de la telecomunicación para proveer de información y servicios médicos de forma remota, empleando procesos de comunicación electrónicos, visuales y auditivos, por medio de diagnósticos y procedimientos de consulta, tales como exámenes clínicos y transferencia de imágenes médicas. Por ejemplo, el uso de este tipo de tecnologías permite a los doctores ayudar a aquellos pacientes imposibilitados físicamente para visitar un hospital, especialmente en áreas rurales donde los médicos especialistas no siempre están disponibles [4]. Sin embargo, la telemedicina implica transmitir información confidencial de forma remota a través de canales inseguros. Por lo tanto, un sistema de telemedicina debe asegurar que la información que se transmite sea conocida únicamente por el emisor y el receptor, es decir, entre paciente y médico.

La telemetría permite realizar mediciones y obtener información en lugares distantes, principalmente enfocada a actividades de monitoreo, su definición literalmente es mediciones a distancia, por lo tanto, se relaciona con muchas áreas, y en este caso, con telemedicina.

Una opción favorable como método de protección de información es el cifrado donde el objetivo es generar un texto cifrado (irreconocible) a partir de la señal (clara) mediante un algoritmo simétrico (con clave secreta) o asimétrico (con dos claves secretas). Actualmente, se tiene la criptografía moderna 3DES (Tryple Data Encryption Standard) y AES (Advanced Encryption Standard) para cifrado simétrico de información y ambos son aceptados como estándar en Estados Unidos. AES tiene como ventajas velocidad, bajo espacio de memoria, implementación sencilla y arquitectura de confusión-difusión. RSA (Rivest, Shamir y Adleman) es un algoritmo asimétrico con ventajas de seguridad pero lento comparado con algunos del tipo simétrico [5]. La metodología de los algoritmos criptográficos modernos (criptografía convencional) se basa en propiedades algebraicas y numéricas, como estructura de Feistel del TDES y la arquitectura confusión-difusión del AES.

Por otra parte, se tiene la criptografía no convencional basada en herramientas matemáticas en estado de investigación como la criptografía cuántica, criptografía con ADN y la criptografía caótica.

Este trabajo de tesis se basa en la criptografía no convencional, concretamente en la criptografía caótica donde el caos en matemáticas y otras ciencias, es adjudicado a los fenómenos que presentan sistemas dinámicos discretos y continuos no lineales, con comportamiento "pseudoaleatorio"determinístico y que poseen muchas propiedades

criptográficas como alta sensibilidad a condiciones iniciales y a parámetros de control, mezcla de datos, entre otros, lo que hace que sea muy interesante y efectivo para el cifrado de información [6, 7].

En contraparte, se encuentra el criptoanálisis, que es la ciencia que se ocupa de corromper un sistema criptográfico y determinar el mensaje original a partir del mensaje cifrado o de secuencias de clave secreta. Emplea análisis matemáticos y estadísticos conocidos como ataques criptoanalíticos, los cuales, varían dependiendo el método criptográfico implementado. Por lo tanto, un sistema criptográfico debe resistir los distintos tipos de ataques criptoanalíticos conocidos en la actualidad para ser considerado seguro. Otro factor importante es la eficiencia para cifrar información a alta velocidad con características similares de seguridad.

1.1. Motivación

Debido al avance de la tecnología y en sistemas de telecomunicaciones, es que hoy contamos con formas más rápidas y sencillas de comunicarnos a lugares que antes eran prácticamente imposibles de contactar. Sin embargo, estos avances traen consigo desventajas que preocupan en muchas áreas, entre ellas la telemedicina, ya que la seguridad de la información transmitida puede verse vulnerada de no contar con una protección, dejando al descubierto información sensible o privada.

Los sistemas caóticos son cada vez más utilizados en el diseño de sistemas de comunicaciones seguras principalmente por sus características similar al ruido, alta sensibilidad a condiciones iniciales y parámetros de control, no linealidad, transitividad topológica y ergodicidad, lo que permite ser aplicado en criptosistemas [8, 9].

Con el amplio interés de la comunidad científica en el cifrado no convencional, particularmente criptografía caótica, existen dos variantes de cifrado: analógico y digital. La versión analógica se implementa mediante circuitos eléctricos y técnicas de sincronización. En la versión digital, no se requieren de componentes analógicos ni sincronización, por lo que la dinámica caótica es fácil de controlar mediante software y lo hace un excelente candidato para trabajar en un sistema de cifrado con ventajas de seguridad y flexibilidad. Una de las áreas de aplicación de los criptosistemas, es en la telemedicina para almacenar, acceder y transmitir información médica de pacientes de forma segura y prevenir robo de datos en sus sistemas.

La información médica que se maneja en telemedicina y particularmente en telemetría, es generalmente confidencial y por lo tanto, requiere ser resguardada de intrusos que puedan afectar el derecho a la privacidad de los pacientes, mediante el conocimiento de su estado de salud con fines de fraudes robo de identidad, diagnóstico incorrecto, etc [10]. El adecuado resguardo de la información brinda al paciente seguridad hacia su integridad. El electrocardiograma (ECG) es el primer examen que se hace para detec-

tar daños al corazón (cardiopatía) y además tiene la característica de ser diferente para cada persona, es decir, puede ser utilizado para identificar individuos [11]. Por su parte, el electroencefalograma (EEG) se utiliza para diagnosticar traumatismos craneales, tumores, enfermedades como Alzheimer, nula actividad cerebral en caso de un coma y determina si una persona presenta muerte cerebral [12]. La presión arterial (BP) se utiliza para diagnosticar la hipertensión (presión alta de la sangre), la cual puede provocar daños como derrame cerebral, ataque al corazón e insuficiencia renal. Para detectar el problema de salud que está ocasionando la hipertensión, es necesario la realización de exámenes adicionales de sangre, orina, rayos X, ECG y en condiciones especiales ecografía, ecocardiograma y ECG de esfuerzo [13].

La telemedicina puede ser utilizada para el cuidado en casa, mecanismos de referencia y contrarreferencia, emergencias, catástrofes, línea abierta de información en salud, servicios de segunda opinión, asesoría de especialistas y educación continua, pero políticas y leyes en cada uno de los países podrían influenciar favorablemente o impedir la aplicación de la tecnología de las comunicaciones en el área de la salud. Existen muchas discusiones en países desarrollados pero con pocas conclusiones al respecto. Por otro lado, la falta de reglamentos es un factor de preocupación para el desarrollo de la telemedicina. El mayor desarrollo en la telemedicina es por parte de grupos independientes y universidades, los cuales utilizan principios bioéticos básicos para proteger la privacidad e integridad del paciente, pero sin coordinación para protocolizarlos ante la falta de reglamentación [14].

En el caso de México, el 21 de Diciembre de 2015 se presentó en el Diario Oficial de la Federación el "Proyecto de Norma Oficial Mexicana PROY-NOM-036-SSA3-2015, Para la regulación de la atención médica a distancia". Con el objetivo de establecer los procedimientos del personal prestador de los servicios de atención médica a distancia, características mínimas de infraestructura y equipamiento de los establecimientos.

Destacando el inciso 7.3.3, el cual hace referencia a la protección de datos del paciente en caso del empleó de los sistemas para visualización física del paciente y el inciso 7.4.2, en el que se indica que los establecimientos de salud que presten servicios de atención médica a distancia deberán adoptar las medidas necesarias para garantizar la confidencialidad, seguridad, integridad y disponibilidad de la información derivada de dicho proceso. Debiendo cumplir con los requisitos de la "NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de la información de la salud". Enfatizando la sección 6.6.5, para fines de intercambios de información entre prestadores de servicios de salud los Sistemas de Información de Registro Electrónico para la Salud (SIRES) deben implementar mecanismos de autenticación, cifrado y firma digital avanzada [15, 16].

Pero al ser un proyecto no puede ser utilizado ya que podría modificarse, por lo que a falta de normas que regulen los diferentes aspectos de la medicina a distancia, es necesaria la adaptación de los criterios existentes para el intercambio de información de la salud, resaltando el cifrado caótico.

Además, surgen cada vez más sistemas caóticos, tanto de tiempo discreto como continuo, donde cada uno presenta diferentes propiedades dinámicas, lo que hace necesario su estudio desde un punto de vista estadístico para determinar los sistemas que tengan mejores propiedades criptográficas y así aplicarlas a un sistema que permita mantener segura la información médica.

1.2. Objetivos

Debido a la necesidad de mantener segura la información en aplicaciones de telemedicina, en particular en telemetría, es que surge la realización de esta tesis de licenciatura, en la que se plantea alcanzar el siguiente *objetivo general*:

Diseñar e implementar un algoritmo de cifrado caótico digital para su aplicación en señales electrofisiológicas.

Con el propósito de cumplir con el objetivo general, se plantean los siguientes *objetivos específicos*:

1. Determinar el mapa caótico a utilizar en función de sus características como tiempo de ejecución y uniformidad de datos caóticos.
2. Diseñar y ajustar el algoritmo de cifrado caótico con la arquitectura de confusión-difusión y dinámicas caóticas.
3. Implementar el algoritmo criptográfico en MatLab y cifrar señales electrofisiológicas adquiridas de una base de datos.
4. Analizar la seguridad del algoritmo contra ataques estadísticos, diferenciales y evaluar el desempeño.

1.3. Organización del manuscrito

- **Capítulo 1:** Se presenta la introducción de este trabajo, la motivación y los objetivos generales y específicos.
- **Capítulo 2:** En este capítulo, se adentra al área de la telemedicina.
- **Capítulo 3:** Se presentan los diferentes sistemas caóticos y se determina el sistema caótico en base a análisis estadístico en MatLab.
- **Capítulo 4:** Este capítulo se enfoca en los aspectos más relevantes de la criptografía.
- **Capítulo 5:** Se presenta el algoritmo de cifrado caótico y su análisis de seguridad.
- **Capítulo 6:** Se mencionan las conclusiones generales de este trabajo y el trabajo a futuro.

Capítulo 2

Telemedicina

En este capítulo, se presentan los aspectos históricos que permitieron el desarrollo de la telemedicina, su clasificación y algunos aspectos que hacen necesaria la seguridad de un sistema enfocado a esta interesante área.

2.1. Introducción

Uno de los primeros registros del uso de las Tecnologías de la Información y la Comunicación (ICT, por sus siglas en inglés) en telemedicina fue cuándo Einthoven en Febrero de 1906 (figura 2.1), transmitió trazos de electrocardiograma (ECG) por medio de líneas telefónicas [17].

Figura 2.1: Willem Einthoven (1860-1927) descubridor del mecanismo del ECG [18, 19].

Se menciona que la telemedicina se remonta a la aparición del telégrafo y posteriormente comenzó a efectuarse por radio: su empleo en alta mar comenzó en los años 1920, cuando varios países ofrecieron asesoramiento médico desde hospitales a sus flotas de

buques mercantes y para entonces se utilizó el código Morse. Para los años 50, se difundió mediante circuitos cerrados de televisión en los congresos de medicina. En los 60, la NASA desarrolló un sistema de asistencia médica que incluía diagnóstico y tratamiento de urgencias durante las misiones espaciales. En 1965, fue efectuada una demostración durante una cirugía a corazón abierto con la ayuda de un sistema de telemedicina entre el Methodist Hospital en Estados Unidos y el Hospital Cantonal de Genéve en Suiza, la transmisión fue realizada por medio del primer satélite de interconexión continental creado por Comsat llamado "*Early* Bird". Casi ningún sistema de entre los años 60 a los 80, logró mantenerse por sí solo al terminar el capital. La década de los 80 fue de gran actividad, dando lugar a muchos proyectos. En Estados Unidos se dio un estancamiento que duró casi hasta los años 90, a partir de esta década se dio el resurgimiento denominado "la segunda era de la telemedicina", dando lugar a nuevas propuestas con objetivos de continuidad y rentabilidad.

La telemedicina es la práctica de la medicina y de sus actividades relacionadas, como la educación y la planeación de sistemas de salud, a distancia por medio de sistemas de comunicación. Su característica principal es la separación geográfica entre dos o más agentes implicados: ya sea un médico y un paciente, un médico y otro médico, o un médico y/o un paciente y/o la información o datos relacionados con ambos. Debido a la gran variedad de especialidades existentes en la medicina y las diferentes maneras de adaptar la tecnología para realizar telemedicina, es que existen distintas clasificaciones: en el tiempo, en especialidades y en tipo de aplicación médica. En la clasificación en tiempo, se toma en cuenta el momento en que se realiza la intervención médica a distancia y la comunicación entre el proveedor y el cliente: tiempo diferido y tiempo real. En la clasificación por tiempo de servicio tenemos: Teleconsulta, Telediagnóstico, Telecuidado (Teleatención), Telemetría, Teleeduación, Teleadministración, Teleterapia (Telepsiquiatría, Telefisioterapia, Teleoncología, Teleprescripción) y Telefarmacia, entre otras. En la clasificación por especialidades tenemos: Telerradiología, Telepatología, Telecardiología, TeleORL, Teleendoscopia, Teledermatología, Teleoftalmología y Telecirugía [14].

La telemedicina es comparada con un paraguas, ya que abarca cualquier actividad médica involucrando el elemento de la distancia. Como se mencionó en el capítulo anterior es de gran utilidad para áreas rurales donde no siempre hay médicos disponibles, ya que el cliente se encuentra separado del experto, es muy adecuada para el monitoreo, y los sistemas tienen un impacto directo en aspectos fundamentales en la gestión de pacientes. Su principal objetivo es el intercambio de información para diagnósticos, tratamientos y prevención de enfermedades, así como para la investigación y evaluación, en orden de mejorar la salud de las personas y de las comunidades donde habitan [20]. La telemedicina se practica a nivel rural o a nivel urbano. En el primer caso, se refiere con frecuencia a comunicaciones para la salud y suelen ser simples: canales de comunicación de bajo ancho de banda, equipos básicos y aplicaciones simples. En el segundo caso, se aplica en telemedicina hospitalaria, la cual, emplea canales de gran ancho de banda y sistemas de información muy complejos y costosos.

Telemedicina tiene beneficios como la disminución de los tiempos de atención, diagnósticos y tratamientos oportunos, mejora en la calidad del servicio, reducción de costes de trasporte, atención continua, tratamientos apropiados, disminución de riegos profesionales, posibilidad de interconsulta, mayor cobertura, así como campañas oportunas de prevención, entre otras tantas.

A continuación se presentan las características esenciales de un sistema de telemedicina:

1. Separación geográfica entre proveedor y cliente durante un encuentro clínico (Telediagnóstico) o entre dos o más proveedores (Teleconsulta).
2. El empleó de las tecnologías informáticas y de comunicaciones necesarias para la interacción.
3. Equipo de gestión del sistema.
4. Infraestructura organizacional.
5. Desarrollo de protocolos clínicos para orientación de los pacientes hacia diagnósticos y fuentes de tratamiento apropiados.
6. Creación de normas de comportamiento para el remplazamiento de las normas del comportamiento cara-a-cara tradicionales.

2.2. Historia de la telemedicina

En [14] se presentan algunas de las actividades que permitieron el crecimiento de la telemedicina, las cuales se mencionan cronológicamente a continuación:

1957: El Dr. Cecil Wittson creó un sistema de telemedicina e interacción entre médico y paciente como parte de un programa de enseñanza médica y de telepsiquiatría en Omaha, Nebraska. Este fue el establecimiento del primer enlace de vídeo interactivo entre el Nebraska Psychiatric Institute en Ohama y el Norfolk State Hospital, separados por 180 kilómetros de distancia.

1965: Se demostró una operación a corazón abierto (remplazo de válvula aórtica), en el que se empleó el sistema de telemedicina "*Early Bird*", entre el Methodist Hospital en Estados Unidos y el Hospital Cantonal de Genéve en Suiza.

1967: En Boston se instaló un sistema de telemedicina, el cual generó una interacción entre médicos y pacientes. Un radiólogo del Massachusetts General Hospital (MGH) abrió un centro de diagnóstico en el servicio médico del aeropuerto Logan. De esta manera, médicos presentaron sus estudios (radiografías e historiales), estás fueron exploradas por una cámara de televisión y transferidas al MGH a través de una línea telefónica común.

1971: Fueron seleccionados 26 lugares en Alaska para comprobar si las comunicaciones podrían mejorar la salud de los pueblos. Se utilizó el satélite ATS-1 (Applied Technology Satellite I de la Nasa) lanzado en 1966 y la transmisión de televisión en blanco y negro. Al final se determinó que el uso de vídeo a distancia aportaba beneficios en algunos casos de no urgencia (ya que en casos de urgencia no se puede esperar a la agenda de consultas planificadas de acuerdo a la disponibilidad del satélite).

1972-1975: Space Technology Applied to Rural Papago advanced Health Care (STARPAHC), fue una de las primeras aventuras de la telemedicina. Sus objetivos fueron brindar asistencia médica a los astronautas en el espacio y a nativos americanos de la reserva de Papago. Empleaba una furgoneta, la cual contenía el equipo médico y un par de enlaces de microondas para la transmisión de las señales y el sonido hasta el hospital donde se encontraban los especialistas.

1976: El lanzamiento del satélite Hermes en Enero, diseñado para cubrir las necesidades de comunicaciones de zonas remotas en Canadá. En Junio, el Ministerio de Sanidad de Ontario, lo utilizó junto con ondas métricas para examinar la posibilidad de vigilar parámetros vitales, tales como ritmo cardíaco, respiración, temperatura y presión arterial, cuando pacientes eran evacuados de una comunidad remota al norte de Ontario. En Octubre, la Universidad de Western Ontario estableció enlaces entre el Hospital Universitario de London (Ontario), el Moose Factory General Hospital y la Kashechewan Nursing Station de James Bay, por un período de 5 meses, con la finalidad de realizar consultas médicas, transmisión de datos (ECG, radiografías, soplos cardíacos, etc.) y para la formación permanente. El último proyecto por parte de la Memorial University de St. John's (Terranova), permitió al personal médico difundir imágenes de televisión desde St. John's a los hospitales de Stephenville, St. Anthony, Labrador City y Goose Bay.

1986: La clínica Mayo instaló un sistema dedicado basado en satélite con la finalidad de unir las clínicas de Rochester, Jacksonville y Scottsdale. El sistema permite una comunicación de video con una tasa completa de imágenes (30fps), permitido para varias disciplinas.

1988: Un gran terremoto asoló la República Soviética en Armenia; durante la catástrofe se efectuaron consultas desde EE.UU. mediante un sistema unidireccional de vídeo, voz y fax entre un centro médico ubicado en Yerevan y 4 centros de EE.UU. Posteriormente se extendió a Rusia tras un accidente ferroviario.

1993: Primer Symposium de Telemedicina. 13,000 kilómetros no fueron obstáculo para el Ejército estadounidense, mediante la operación *"Restore Hope"* brindaron servicio médico a sus tropas durante la crisis de Somalia en Mogadiscio. Se utilizó el sistema INMARSAT con el uso de sistemas portátiles y baratos. En 1995 también brindaron servicio de telemedicina a tropas en Bosnia.

1994: La clínica Mayo usa los satélites ACTS (Advanced Communications Techno-

logy Satellite) de la NASA para la realización de varias demostraciones de telemedicina. La escuela de medicina de la universidad de Carolina del Este creó la primera instalación dedicada al uso de la telemedicina que consiste en 4 salas de teleconsulta específicamente diseñadas. Durante las olimpiadas de invierno en Lillehammer, Noruega estableció un enlace para comunicar a especialistas con las pequeñas poblaciones donde son efectuadas las pruebas consideradas de alto riesgo. Son atendidos 271 pacientes en sólo 2 meses, empleando el servicio de telemedicina de la prisión federal de la University of Texas Medical Branch at Galveston, la razón del éxito de dicho programa es que son atendidas las necesidades de una población de 140,000 reclusos. Reduciendo en gran medida los costos requeridos en dichos centros debido a los costos de desplazamientos, escoltas, etc.

1997: El proyecto ACTS de la NASA pasa a segunda fase permitiendo transferencias a alta velocidad. Consiguiendo con esto la transmisión de secuencias de angiografías, ecocardiografías y radiografías a una velocidad de 40 Mbps utilizando ATM (Modo de transferencia asíncrona).

1998: Es realizada en España la primera experiencia de telecirugía con robots. Los cirujanos estaban operando en un barco a un paciente situado a cientos de kilómetros.

2.3. Clasificación de los servicios de telemedicina

Como se planteó anteriormente existen muchas clasificaciones, a continuación nos adentraremos más en dichas clasificaciones [14]:

Tiempo

Tiempo diferido: Es cuándo el cliente y el proveedor no se encuentran en comunicación directa, a esta modalidad se le denomina store-and-forward o *"almacenamiento y envío"*, esto se debe a que la información llega al especialista y se almacena para que él pueda revisarla y posteriormente enviar su punto de vista, un ejemplo sería en radiología ya que se reciben varias radiografías para que el médico las analice.

Tiempo real: Es cuándo cliente y proveedor se encuentran en comunicación directa a través de un medio de comunicación. Son requeridos anchos de banda superiores y por lo tanto su costo de implementación es mayor, además de disponibilidad de ambas partes.

Existen dos divisiones de la medicina en tiempo real:

1. **Videoconferencia**: Emplea cámaras de vídeo para la realización de la comunicación.

2. **Aplicación interactiva**: Emplea programas de software que permite a los implicados sincronizar dos aplicaciones remotas para compartir información, por

ejemplo un microscopio robotizado que puede ser manipulado a distancia.

Tipo de servicio

Teleconsulta

1. **Consulta general**: Se efectúa por medio de videoconferencia con un médico general.
2. **Consulta de especialista**: De igual manera que el anterior pero ya con un médico especialista.

Telediagnóstico: en este caso el diagnóstico se realiza después de una consulta rutinaria o como una segunda opinión.

Telecuidado: En este caso, pacientes son asistidos por enfermeras remotas, la cuales dan indicaciones a partir de las líneas telefónicas. Se utiliza como método de prevención y educativo.

Telemetría: Es utilizado para el monitoreo de signos vitales: ECG, EEG, EMG, Presión Arterial, Temperatura, Pulso, Oximetría, Espirometría y exámenes de laboratorio mediante punción digital para enfermedades metabólicas que requieren llevar un control.

Teleeducación: Permite la capacitación a distancia, educación continua, apoyo a estudiantes en prácticas, campañas de prevención, enseñanza de procedimientos mediante técnicas interactivas o módulos de realidad virtual y evaluación así como retroalimentación entre docentes y alumnos.

Teleadministración: Tiene la finalidad de controlar de mejor manera procesos como citas, remisiones, referencias, facturación, control de cartillas, inventarios, planeación estratégica y orientación a brindar servicios de mejor calidad.

Teleterapia: Se emplean sistemas de videoconferencia para realizar tratamientos y consultas a pacientes de telepsiquiatría, telefisioterapia, teleoncología y teleprescripción.

Telefarmacia: Para realizar prescripciones, dispensación de medicamentos, facturación y seguimiento a fórmulas.

Telecirugía: Cirugía asistida por sistemas robotizados, por ejemplo para corregir la miopía, o también durante confrontaciones bélicas.

Especialidad médica

Telerradiología: Muy usada ya que el radiólogo no tiene contacto directo con el paciente y en algunos casos se cuenta con modalidades digitales, se destacan la radiología convencional (RX), escanografía, resonancia magnética (MR), medicina nuclear (NM) y ultrasonido (US).

Telepatología: Emplea imágenes o videos obtenidas del microscopio y son de dos casos: Anatómico (especímenes de cirugía, biopsias, autopsias, etc.) historial del paciente como (banco de sangre, microbiología, análisis de orina, etc.)

Telecardiología: ECG, ecocardiograma (2D, 3D, fijas, dinámicas), sonidos cardíacos, etc.

TeleORL-Teleendoscopía: En otorrinolaringología (ORL) se realizan exámenes mediante sistemas de endoscopia de fibra óptica conectados a un sistema de videoconferencia o de digitalización.

Teledermatología: Consiste en consultas a distancia mediante videoconferencia o mediante el envío de fotografías.

Teleoftanmología: Muy útil en la prevención y seguimiento de enfermedades metabólicas, mediante la conexión de sistemas oftalmoscopios conectados a sistemas de videoconferencia o mediante digitalización de imágenes.

2.4. Seguridad

La información que se maneja en telemedicina, debe ser confidencial, por lo cuál debe ser resguardada de ataques y amenazas que atenten contra la privacidad y la protección de datos del paciente. Las redes de datos son vulnerables a ataques que buscan el colapso de los sistemas para sustraer datos privados mediante técnicas de hurto de información como spyware (espías), virus, troyanos, el acceso no autorizado, la alteración o deterioro total o parcial de la información. En el caso particular de los sistemas de telemedicina, se puede atacar aprovechando sus vulnerabilidades entre las que se destacan: falta de sistemas de seguridad informática, sistemas inestables de autenticación, errores en los procesos de transmisión y almacenamiento de la información y por un manejo inadecuado de la información por parte del personal.

En Junio del 2011 en Birmingham, Estados Unidos, una mujer fue acusada de robar la identidad de más de 4,000 pacientes del Hospital de Birmingham, la implicada accedió a los recursos de la base de datos de dicha institución. La información fue empleada para robar correos y pretendía realizar fraudes bancarios mediante el número de seguro social de los pacientes. En otro caso, un empleado del Midstate Medical Center transfirió información confidencial de más de 93,500 pacientes del hospital a un sitio externo, esto con la finalidad de trabajar desde casa, dejando vulnerable la información que con-

tenía nombres, direcciones, fechas de nacimiento e información médica confidencial [10].

Las vulnerabilidades en telemedicina hacen que su seguridad sea débil, lo que aumenta las posibilidades de ataques. Por lo que se requiere fortalecer tres aspectos importantes: aplicaciones, servicios y la infraestructura. En el primer caso, se habla de cuentas e-mail, servicios web y registros de información clínica. En el segundo, se centra en los servicios prestados al usuario final. Finalmente, se habla de sistemas como routers, switch (interruptores), servidores, computadoras y enlaces de redes.

2.5. Conclusiones

En este capítulo, se presentó una introducción a la telemedicina, así como su uso a lo largo de la historia con grandes avances en las áreas de investigación y militar. Además, se mencionan las diversas ramas así como la información que puede ser transmitida a través de estos sistemas. Un factor importante a tomar en cuenta es la seguridad de la información de dichos sistemas, por lo que es necesaria la implementación de estrategias que ofrezcan un mayor grado de seguridad de la información para brindar confidencialidad a los usuarios.

Capítulo 3

Caos

Este capítulo presenta una introducción al caos y su definición, desde un punto de vista físico-matemático y se presentan las propiedades que permiten su identificación. Se proponen algunos mapas caóticos y se analizan para su elección y aplicación en el cifrado propuesto en este trabajo de tesis y de qué manera mejorar las dinámicas caóticas que el mapa presenta.

3.1. Introducción

El caos es el término que se le asigna a distintos fenómenos (tanto físicos como naturales) no lineales que ocurren en sistemas dinámicos de tiempo discreto y continuo [21]. Las ideas básicas del caos han sido descubiertas en los trabajos realizados por Henri Poincaré, John Littlewood, Mary Cartwright y Edward Lorenz, siendo este último considerado padre del caos.

Johannes Kepler publicó *"The Three Laws of Planetary Motion (las tres leyes del movimiento planetario)"* en sus dos libros en 1609 y 1618 respectivamente. En 1687, Isaac Newton consolida el principio de causalidad derivado de la filosofía de René Descartes en su *"Third Meditation"* de 1641, el cuál dice que cada efecto tiene un antecedente y causa inmediata. Dicha consolidación se debe a la reafirmación de dos conceptos: condiciones iniciales y ley del movimiento. Para calcular las trayectorias de los planetas, Newton simplificó el modelo y asumió que cada planeta estaba únicamente relacionado con el sol, sus cálculos fueron concordantes con las leyes de Kepler.

Pierre-Simon Laplace fue quién más claramente expuso el concepto de determinismo universal en 1778: cada evento es físicamente determinado por una cadena inquebrantable de acontecimientos previos. Demostró que la totalidad de los movimientos de los cuerpos celestes pueden ser explicados por la ley de Newton, lo que reduce el estudio de los planetas a series de ecuaciones diferenciales.

Urbain Jean Joseph Le Verrier descubrió el planeta Venus en 1848 a través de

cálculos sin observaciones astronómicas. Adicionalmente, desarrollo métodos de Laplace (para aproximaciones de soluciones a ecuaciones de séptimo grado).

Para estudiar la evolución de un sistema físico a través del tiempo, Henri Poincaré dijo que es necesario construir un modelo basado en la elección de leyes físicas y enumerar los parámetros necesarios y suficientes que caracterizan el sistema (ecuaciones diferenciales). Poincaré también descubrió el fenómeno de sensibilidad a condiciones iniciales en su estudió *n-body problem*. Un siglo después de Laplace, el mismo Poincaré indicó que la aleatoriedad y el determinismo se vuelven algo compatibles debido a la imprevisibilidad a largo plazo [22].

Si conocemos exactamente las leyes de la naturaleza y el estado del universo en el momento inicial, podemos predecir exactamente el estado del mismo universo en un momento posterior. Sin embargo aunque conozcamos todo sobre las leyes de la naturaleza, solo podríamos conocer un estado aproximado. Si esto permite predecir el siguiente estado con la misma aproximación, es todo lo que se requiere, por lo tanto se dice que el fenómeno ha sido predicho, por lo que está gobernado por leyes. Pero no siempre es así, pequeñas diferencias en las condiciones iniciales pueden generar grandes diferencias en el fenómeno final. Un pequeño error en el primero conducirá a un gran error en el último. Haciendo la predicción imposible, teniendo como resultado un fenómeno aleatorio.

Henri Poincaré.

En 1860, James Clerk Maxwell estudió el movimiento de las moléculas de gas. En el experimento se colisionaron dos partículas de gas encerrados en una caja y el resultado no presentó movimientos del tipo A o B (estable u oscilatorio), se trató de un comportamiento impredecible. Además, se percató que cambios muy pequeños en el movimiento inicial de las partículas, generaba un inmenso cambio en las trayectorias de las moléculas, es decir sensibilidad a condiciones iniciales.

Esto es lo que se denominó el *"Nacimiento del Caos"*. Posteriormente, ya con sistemas que permitían la realización de operaciones con mayor precisión como la Royal McBee LGP-30 empleada por Edward Lorenz, es que se pudo constatar el caos mediante las pequeñas variaciones a las condiciones iniciales. Esto dio lugar en 1963 al trabajo que fue conocido por ser el parteaguas del caos [23], donde fueron diseñados algunos sistemas finitos de ecuaciones diferenciales ordinarias, para representar que los sistemas hidrodinámicos poseen soluciones analíticas periódicas, cuando la fuerza es estrictamente constante. Con la finalidad de verificar la existencia del flujo determinístico no-periódico, se obtuvieron soluciones numéricas de un sistema mediante tres ecuaciones diferenciales ordinarias diseñadas para representar un proceso convectivo. Las ecuaciones poseen tres soluciones de estado estable e innumerables soluciones periódicas. Los resultados sobre la inestabilidad del flujo no-periódico son aplicados a la atmósfera, la cual aparentemente es no-periódica. Los resultados indicaron que la predicción a futuro suficientemente distante es imposible por cualquier método, a menos que las presentes

condiciones se conozcan exactamente.

En vista de la inestable imprecisión y el estado incompleto de las observaciones del clima, el rango de predicciones muy precisas parecía ser inexistentes. Lo que generó una pregunta, ¿Los resultados son realmente aplicables a la atmósfera? El punto crucial es entonces si estados análogos han ocurrido desde la primera observación de esta. Por analogías se refiere a dos o más estados de la atmósfera, junto con su entorno, que son tan estrechamente parecidos que las diferencias puedan ser atribuidas a errores en las observaciones. En caso de que las similitudes no ocurran durante este periodo, puede existir un esquema preciso de predicción de muy largo alcance al utilizar observaciones disponibles actualmente. Pero, si no existe, la atmósfera adquirirá un comportamiento cuasi-periódico, nunca perdido, una vez que la analogía ocurre. Este comportamiento cuasi-periódico no necesita ser establecido, aunque es factible realizar pronósticos a muy largo alcance, si la variedad de estados atmosféricos posibles son tan inmensos que las analogías no necesitan ocurrir.

Cabe señalar que estas conclusiones no dependen de si la atmósfera es o no determinista. Otra pregunta muy importante es la siguiente, ¿Cuánto es de muy largo alcance? Los resultados no dieron respuestas para la atmósfera; concebiblemente pueden ser pocos días o pocos siglos. En un sistema idealizado, ya sea un modelo simple, o un sistema especialmente diseñado para parecerse lo más posible a la atmósfera, la respuesta puede ser obtenida comparando pares de soluciones numéricas con condiciones iniciales casi idénticas.

3.2. Sistemas caóticos y sus propiedades

Durante generaciones se destacó la existencia de dos tipos de movimientos, el tipo A ofrece un estado estable debido a la pérdida de energía por la fricción y el de tipo B oscilatorio, periódico o cuasiperiódico, similar al giro de las manecillas del reloj presente en el movimiento de la Luna y los demás planetas. En 1975, después de tres siglos de estudios, científicos alrededor del mundo repentinamente empiezan a ser conscientes de la existencia de un tercero, el movimiento tipo C, actualmente conocido como caos.

El caos puede ser identificado cuándo el sistema cuenta con las siguientes propiedades [6, 21]:

- *Determinismo:* Conocimiento del estado presente a partir del estado pasado.
- *Ergodicidad:* Para cualquier condición inicial o parámetro de control, la trayectoria caótica se mantiene confinada en un espacio conocido como atractor extraño.
- *Fractales:* Término acuñado en 1960 por B. Mandelbrot, matemático de IBM, y que generalmente cuentan con algunas o todas estas propiedades: estructura complicada con un amplio rango de escalas largas, repetición de estructuras en

diferentes escalas de longitud (similitud propia) y una *"dimensión fractal"* no entera.

- *Sensibilidad a condiciones iniciales y parámetros de control:* La dinámica o trayectoria caótica se verá altamente modificada con una pequeña variación de estos.
- *Mezcla de datos:* Un rango pequeño de condiciones iniciales o parámetro de control cubre la mayor parte del espectro caótico.
- *No linealidad:* No cumple con el principio de superposición, es decir un sistema complejo no puede ser descompuesto en un conjunto de sistemas simples.
- *Exponente de Lyapunov positivo:* Un sistema de N dimensiones posee N exponentes de Lyapunov; si uno es positivo, se determina que el sistema es caótico; en caso de que dos o más sean positivos, el sistema es hipercaótico.

Los sistemas dinámicos con los que se trabajará en este trabajo de tesis son de tiempo discreto, ya que para su cálculo no se requiere de métodos de aproximaciones numéricos como lo es RK4 o Euler. Para conocer qué sistema será elegido en esta tesis, hay que tomar en cuenta que estos sistemas pueden presentar baja uniformidad, lo cual, perjudica la seguridad al momento de diseñar un algoritmo de cifrado, debido a que en los procesos de confusión (permutación) y difusión, los elementos cifrados no serían modificados en gran proporción en comparación con la señal original, lo que genera criptogramas con propiedades criptográficas ineficientes, y lo hace susceptible ante ataques de criptoanálisis [6]. Por tanto, es necesario la implementación de un mejoramiento a la secuencia caótica desde el punto de vista pseudoaleatorio.

3.3. Máximo exponente de Lyapunov

El número de Lyapunov es el promedio de la tasa de divergencia por paso de los puntos cercanos a lo largo de la órbita y el exponente de Lyapunov es el logaritmo natural del número de Lyapunov. El caos es definido por un exponente de Lyapunov mayor a cero [21].

El exponente de Lyapunov provee una medición de como dos órbitas que inician con condiciones iniciales diferentes, pero muy similares difieren en el tiempo. Dos órbitas inicialmente cercanas en un sistema con un exponente de Lyapunov positivo se separarán muy rápidamente [24]. El exponente de Lyapunov se determina mediante la siguiente expresión:

$$\lambda = \frac{1}{T}\ ln\ |\frac{f^n(x_n - \delta_0) - f^n(x_n)}{\delta_0}|, \tag{3.1}$$

donde λ es el exponente de Lyapunov, x_n es la condición inicial, δ_0 es al pequeña diferencia que se le añadirá a la condición inicial, n es la iteración y T es el número total de iteraciones.

La implementación de los mapas caóticos se realiza en el software de MatLab V7.8 (R2009a) en una laptop con procesador Intel Core 2.9 GHz, 8 GB de RAM y sistema operativo Windows 10 64 bits. Se utiliza representación aritmética (estándar IEEE 754) tipo double (64) bits que permite una precisión de 10^{-15} decimales.

3.4. Mapa Logístico

En 1976, Robert May estudió un modelo matemático no lineal en tiempo discreto, para explicar la dinámica poblacional de especies animales [25]. Es el sistema no lineal más simple que existe y se encuentra descrito por la siguiente ecuación:

$$x_{n+1} = ax_n(x_n - 1), \tag{3.2}$$

donde $x \in (0, 1)$ es el estado del mapa discreto, n son las iteraciones, x_0 es la condición inicial con valores entre $0 < x_0 < 1$ y a es el parámetro de control entre $3.57 < a < 4$ para que el mapa genere secuencias caóticas. En la figura 3.1, se observa el comportamiento del estado del mapa logístico x, con $a = 3.990000000000000$, $y_0 = 0.800000000000000$ y $n = 50$.

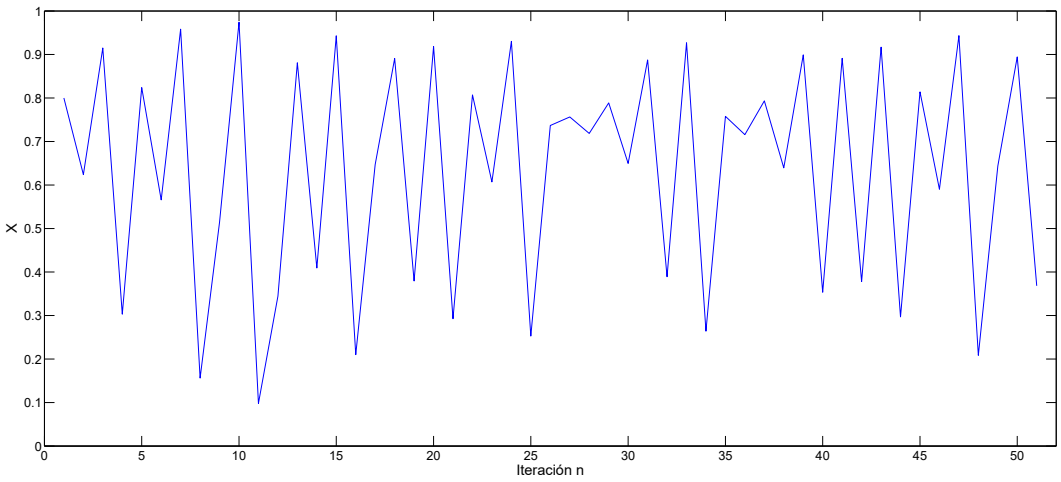

Figura 3.1: Gráfica temporal del mapa logístico.

Para el cálculo del máximo exponente de Lyapunov, se utiliza como condición inicial $x_0 = 0.800000000000000$, perturbación $\delta_0 = 1 \times 10^{-6}$, número de iteraciones $T = 1,000$ y parámetro de control $a = 3.990000000000000$. Los valores obtenidos fueron $\lambda_1 = 0.496607301217345$, por lo que, se comprueba la presencia de caos en el mapa logístico.

3.5. Mapa de Hénon

En 1969, Michel Hénon demostró que los sistemas dinámicos definidos por ecuaciones diferenciales presentan las mismas características [26], por lo que propone el famoso mapa de dos dimensiones, presentando un enfoque reducido del estudio realizado por Lorenz [27] y se encuentra descrito por las siguientes ecuaciones:

$$x_{n+1} = y_n + 1 - ax_n^2, \tag{3.3}$$

$$y_{n+1} = bx_n, \tag{3.4}$$

donde x y y representan los estados del sistema discreto, las condiciones iniciales no son mencionadas y los parámetros de control para generar caos son $a = 1.400000000000000$, $b = 0.300000000000000$ y n son las iteraciones. En la figura 3.2, se muestra el atractor extraño generado de este mapa caótico con condiciones iniciales $x_0 = 0.600000000000000$, $y_0 = 0.50000000000000$ y $n = 10,000$.

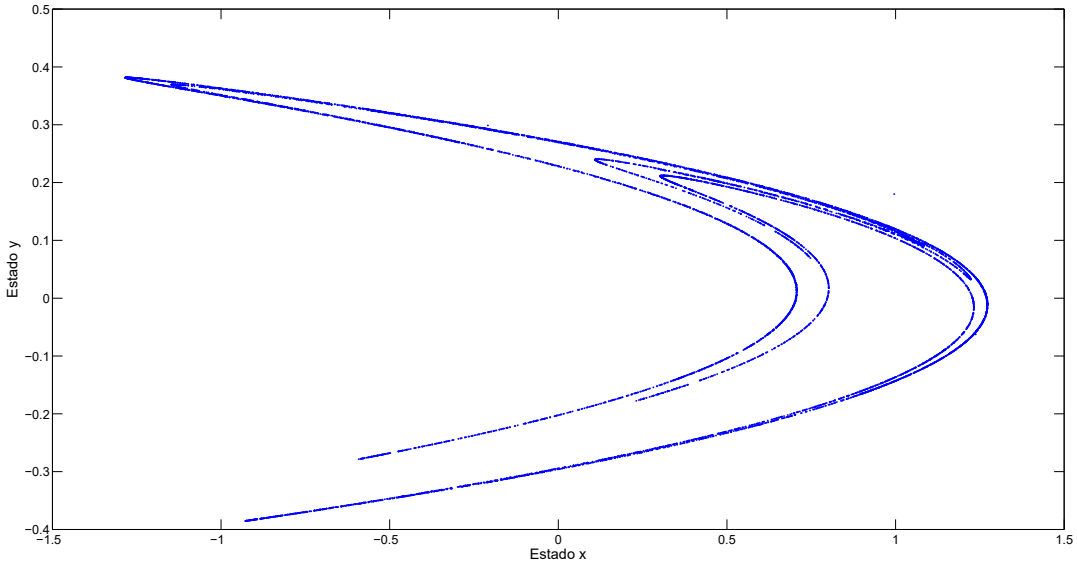

Figura 3.2: Atractor extraño del mapa de Hénon.

Para el cálculo del exponente de Lyapunov del Mapa de Hénon, se utilizaron como condiciones iniciales $x_0 = 0.600000000000000$ y $y_0 = 0.50000000000000$, la perturbación $\delta_0 = 1 \times 10^{-6}$, el número de iteraciones $T = 1,000$ y parámetros de control $a = 1.400000000000000$ y $b = 0.300000000000000$. Los valores obtenidos fueron $\lambda_1 = 0.065133088617776$ y $\lambda_2 = -1.203972804342254$, al tener un exponente de Lyapunov positivo, se comprueba que el mapa presenta un comportamiento caótico.

3.6. Mapa Ikeda

Es uno de los mapas caóticos que modela el movimiento de la luz alrededor de resonadores ópticos no-lineales, frecuentemente este mapa es modificado del original, el cual está representado por la siguiente ecuación [28]:

$$z_{n+1} = A + Bz_n e^{iK/(|z_n|^2+1)^{+C}}, \tag{3.5}$$

donde, z_n es el campo eléctrico en el interior del resonador, A y C son luces de láser aplicadas desde el exterior y B es la pérdida del resonador.

Escrito en dos dimensiones (2D) se tiene

$$x_{n+1} = 1 + u(x_n cos\ t_n - y_n sin\ t_n), \tag{3.6}$$

$$y_{n+1} = u(x_n sin\ t_n - y_n cos\ t_n), \tag{3.7}$$

donde x y y son los estados, $u \geq 0.6$ es el parámetro de control, n las iteraciones y

$$t_n = 0.4 - \frac{6}{1 + x_n^2 + y_n^2} \tag{3.8}$$

con condiciones iniciales $x_0 = 0.300000000000000$, $y_0 = 0.300000000000000$, parámetro de control $u = 0.918000000000000$ y $n = 10,000$. En la figura 3.3, se presenta el atractor extraño de dicho mapa. En este trabajo, la ecuación (3.6) fue modificada cambiando el signo a positivo para generar mejores resultados.

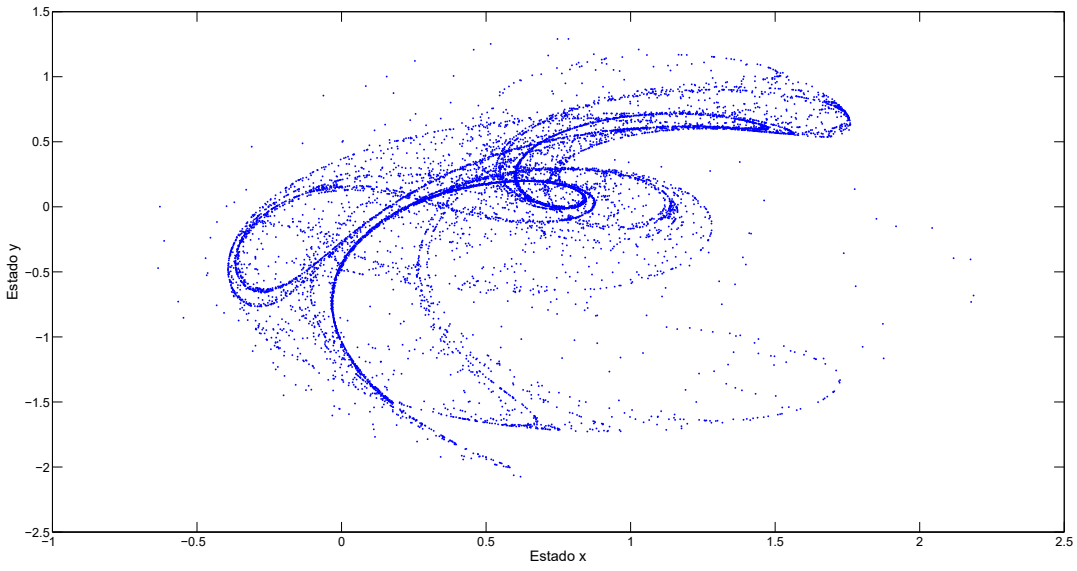

Figura 3.3: Atractor extraño del mapa Ikeda.

Para el cálculo del exponente de Lyapunov del mapa de Ikeda, se utilizaron como condiciones iniciales $x_0 = 0.300000000000000$ y $y_0 = 0.300000000000000$, la perturbación $\delta_0 = 1 \times 10^{-6}$, el número de iteraciones $T = 1,000$ y parámetro de control $u = 0.918000000000000$. Los valores obtenidos fueron $\lambda_1 = -1.351808994818498$ y $\lambda_2 = 0.193090153550621$. Al tener un exponente de Lyapunov positivo, se comprueba que el mapa Ikeda presenta caos.

3.7. Mapa Tinkerbell

Es un mapa caótico utilizado para describir resonadores ópticos, se encuentra descrito por las siguientes ecuaciones en diferencia [29]:

$$y_{n+1} = y_n^2 - \theta_n^2 + \alpha y_n + \beta \theta_n, \tag{3.9}$$

$$\theta_{n+1} = 2y_n\theta_n + \gamma y_n + \delta \theta_n, \tag{3.10}$$

donde y y θ son variables de estado y $\alpha = 0.9$, $\beta = -0.6013$, $\gamma = 2$ y $\delta = 0.50$ o $\alpha = 0.3$, $\beta = 0.6000$, $\gamma = 2$ y $\delta = 0.27$ son los parámetros de control para la generación de secuencias caóticas y n es el número de iteraciones. En la figura 3.4, se observa su atractor extraño, con condiciones iniciales $y_0 = -0.720000000000000$ y $\theta_0 = -0.640000000000000$ y parámetros de control $\alpha = 0.900000000000000$, $\beta = -0.601300000000000$, $\gamma = 2.000000000000000$, $\delta = 0.500000000000000$ y $n = 10,000$.

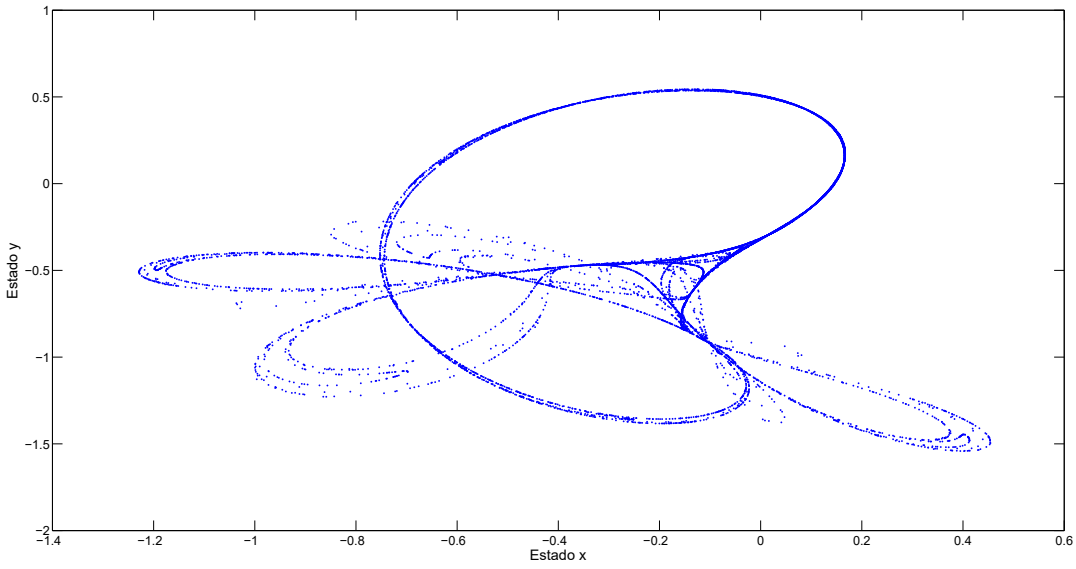

Figura 3.4: Atractor extraño del mapa Tinkerbell.

Para el cálculo del exponente de Lyapunov del Mapa de Tinkerbell, se utilizaron como condiciones iniciales $y_0 = -0.720000000000000$ y $\theta_0 = -0.640000000000000$, la

perturbación $\delta_0 = 1 \times 10^{-6}$, el número de iteraciones $T = 1,000$ y parámetros de control $a = 0.900000000000000$, $\beta = -0.601300000000000$, $\gamma = 2.000000000000000$ y $\delta = 0.500000000000000$. Los valores obtenidos fueron, $\lambda_1 = -0.261121001055689$ y $\lambda_2 = 0.132749855337637$. Al tener un exponente de Lyapunov positivo, se comprueba la presencia de caos en el mapa Tinkerbell.

3.8. Mapa de Ushio

Este mapa fue reportado en [30], en dicho trabajo el sistema es utilizado para comprobar un método de sincronización denominado anti-fase (la más familiar es la conocida como en-fase o simplemente sincronización). Posteriormente, el sistema ha sido empleado en otros trabajos, en los cuales se busca un método para el control del caos en sistemas caóticos de tiempo discreto [31, 32]. Las ecuaciones representativas del sistema son:

$$x_{n+1} = px_n - x_n^3 + y_n, \tag{3.11}$$

$$y_{n+1} = \frac{1}{2}x_n, \tag{3.12}$$

donde x y y son los estados, $p \geq 0.5$ es el parámetro de control para que presente comportamiento caótico y n son las iteraciones. En la figura 3.5, se muestra su atractor extraño, con condiciones iniciales $x_0 = 0.500000000000000$, $y_0 = 0.500000000000000$, parámetro de control $p = 1.900000000000000$ y $n = 10,000$.

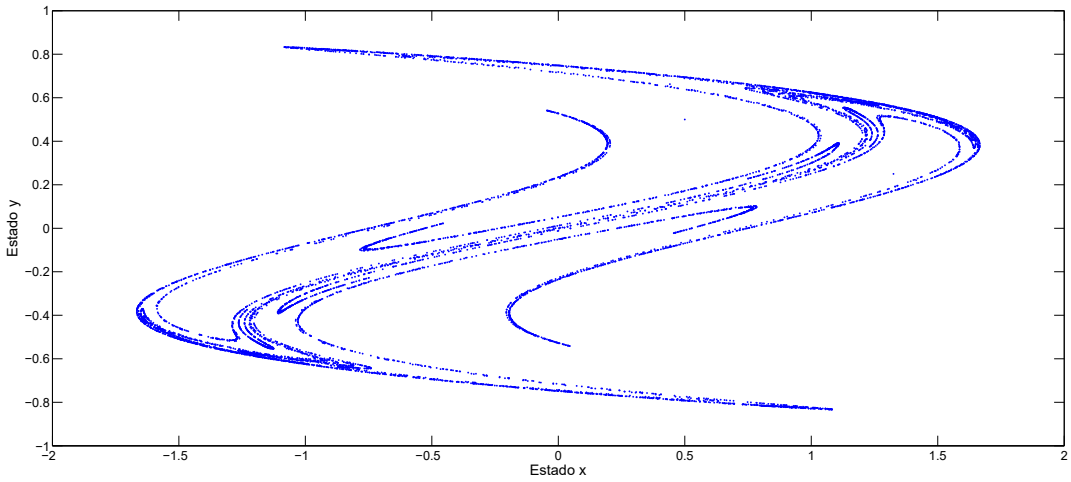

Figura 3.5: Atractor extraño del mapa de Ushio.

Para el cálculo del exponente de Lyapunov, se utilizó como condiciones iniciales $x_0 = 0.500000000000000$ y $y_0 = 0.500000000000000$, la perturbación $\delta_0 = 1 \times 10^{-6}$, el número de iteraciones $T = 1,000$ y parámetro de control $p = 1.9$. Los valores obtenidos fueron $\lambda_1 = 0.330753934238647$ y $\lambda_2 = -0.693147180592924$. Al tener un exponente de

Lyapunov positivo, se comprueba que el sistema presenta dinámicas caóticas.

3.9. Selección de mapa caótico y mejoramiento de dinámicas caóticas

La prueba numérica del máximo exponente de Lyapunov verifica la presencia de dinámica caótica en los cinco sistemas, lo que indica que son aptos para el cifrado de información. Sin embargo, las secuencias caóticas deben ser uniformes para producir eficientes criptogramas. Por lo tanto, en este trabajo de tesis se estudian y analizan distintas operaciones matemáticas, por ejemplo, funciones trigonométricas y exponenciales para realizar la prueba de frecuencia (monobit) con el objetivo de uniformizar los datos caóticos. El propósito de esta prueba es determinar si el número de ceros y unos en una secuencia binaria son aproximadamente iguales, tal como se prevé para una secuencia aleatoria. La prueba consta de los siguientes pasos [33]:

1. Convertir la secuencia caótica decimal $x^U \in (0,1)$ a binaria mediante la siguiente condición propuesta:
$$x_k^B = \begin{cases} 1 & Si\ x_k^U \geq 0.5 \\ 0 & Otro\ caso \end{cases} \tag{3.13}$$
donde x^U representa el valor del mapa de Ushio, x^B representa la secuencia binaria y $k = 1, 2, 3, \ldots, I$.

2. Posteriormente, se genera la secuencia de bits mediante funciones como: Generador de números aleatorio (RNG, por sus siglas en inglés) o Generador de números pseudoaleatorio (PRNG, por sus siglas en inglés). Esto existe como una estructura global en el tiempo de la función llamada $\varepsilon = \varepsilon_1, \varepsilon_2, ..., \varepsilon_n$.

3. Conversión a ± 1: los ceros y unos de la secuencia de entrada ε son convertidos a valores de -1 y $+1$ y son sumados para producir $S_n = X_1 + X_2 + ... + X_n$, donde $X_i = 2\varepsilon - 1$. Es decir, si el valor en X_i de la secuencia binaria es un uno en la secuencia S se suma un 1 en caso contrario un -1.

4. Se calcula $S_{abs} = \dfrac{|S_n|}{\sqrt{n}}$, donde n es la longitud de la secuencia.

5. Se calcula el $P\_value = erfc(\dfrac{S_{abs}}{\sqrt{2}})$, donde el *erfc* es la función de error complementario.

Si $P\_value < 0.01$, se concluye que la secuencia no es aleatoria. En caso contrario, la prueba indica que la secuencia es aleatoria. Idealmente un $P\_value = 1$ indica que

hay el mismo número de ceros y de unos en la secuencia. Se recomienda que la longitud de la secuencia sea $n \geq 100$. Los resultados de los cinco mapas caóticos con dinámicas procesadas con distintas operaciones matemáticas se muestran en la tabla 3.1.

Primeramente, se analiza el mapa logístico por ser un sistema unidimensional. El sistema es iterado 10,000 veces con parámetro de control $a = 3.900000000000000$ y condición inicial $x_0 = 0.800000000000000$. En la figura 3.6(a), se observa el histograma generado a partir de los datos del mapa logístico. En la figura 3.6(b), se aprecia el histograma del mapa logístico con la función tangente con resultados más uniformes y mejor distribuidos (ver tabla 3.1).

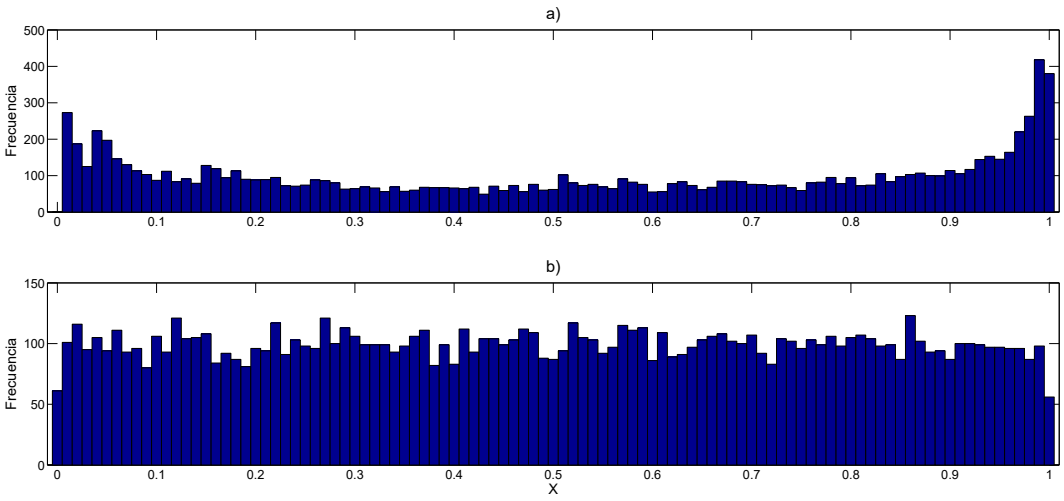

Figura 3.6: Histograma: **a)** mapa logístico y **b)** mapa logístico con implementación de operación tangente.

Con esto se comprueba que las funciones están mejorando la secuencia caótica, con excepción de la función exponente la cual arroja una no aleatoriedad. A continuación, se realiza la prueba a los mapas caóticos restantes y los resultados se presentan en la tabla 3.1.

La figura 3.7, muestra los resultados de la prueba monobit para cada uno de los mapas caóticos. Las figuras 3.8 y 3.9, muestran la cantidad de ceros y unos que presenta cada mapa caótico en su respectivo estado. La figura 3.10, muestra el gráfico de duración de la prueba monobit, el cual sirve como referencia para los tiempos de cifrado y descifrado.

El mapa de Ushio obtuvo un excelente *P_value* para el estado x, lo cual nos indica una alta aleatoriedad al emplear las distintas operaciones de mejora de las dinámicas caóticas y el tiempo de procesamiento para la prueba monobit es el menor, por lo tanto, es el sistema seleccionado para este trabajo de tesis.

	Mapa logístico	Mapa Hénon	Mapa Ikeda	Mapa Tinkerbell	Mapa de Ushio
# Mapa	1	2	3	4	5
Estados	x	x, y	x, y	x, y	x, y
Lambda	$\lambda_x = 0.49$	$\lambda_x = 0.06$	$\lambda_x = -1.35$	$\lambda_x = -0.26$	$\lambda_x = 0.33$
		$\lambda_y = -1.2$	$\lambda_y = 0.193$	$\lambda_y = 0.13$	$\lambda_y = -0.69$
P_value	$E_x = 0$	$E_x = 0$	$E_x = 0$	$E_x = 0$	$\mathbf{E_x = 0.568697}$
	$E_y = 0$	$E_y = 0$	$E_y = 0$	$E_y = 0$	$\mathbf{E_y = 0.555210}$
Aleatorio	No	No	No	No	**Si**
P_value	$E_x = 0.322198$	-	-	-	-
Raíz(Estado)	-	-	-	-	-
P_value	$E_x = 0.568697$	$E_x = 0.582338$	$E_x = 0.056146$	$E_x = 0.477726$	$E_x = 0.880771$
Seno(Estado)	-	$E_y = 0.103119$	$E_y = 0.197073$	$E_y = 0.141582$	$E_y = 0.073468$
P_value	$E_x = 0.218720$	$E_x = 0.802597$	$E_x = 0.515713$	$E_x = 0.818101$	$E_x = 0.204107$
Coseno(Estado)	-	$\mathbf{E_y = 0.960124}$	$E_y = 0.696551$	$E_y = 0.190218$	$E_y = 0.016854$
P_value	$\mathbf{E_x = 0.912414}$	$\mathbf{E_x = 0.896572}$	$E_x = 0.312519$	$E_x = 0.441323$	$E_x = 0.384324$
Tangente(Estado)	-	$E_y = 0.596130$	$E_y = 0.515713$	$E_y = 0.141582$	$\mathbf{E_y = 0.928291}$
P_value	$E_x = 0.000051$	$E_x = 0.332071$	$E_x = 0.541882$	$E_x = 0.429551$	$\mathbf{E_x = 0.976068}$
$e^{Estado} * 100$	-	$E_y = 0.064327$	$E_y = 0.218720$	$E_y = 0.849317$	$E_y = 0.342136$
Tiempo	$t_1 = 96.907$	$t_1 = 144.653$	$t_1 = 205.698$	$t_1 = 181.941$	$\mathbf{t_1 = 144.140}$
de cálculo (ms)	-	$t_2 = 149.611$	$t_2 = 208.408$	$t_2 = 182.150$	$t_2 = 144.491$
para exponencial					
Ceros	$E_x = 5203$	$E_x = 4908$	$E_x = 4970$	$E_x = 5040$	$E_x = 4999$
	-	$E_y = 5049$	$E_y = 5062$	$E_y = 5010$	$E_y = 4953$
Unos	$E_x = 4798$	$E_x = 5093$	$E_x = 5031$	$E_x = 4961$	$E_x = 5002$
	-	$E_y = 4952$	$E_y = 4939$	$E_y = 4991$	$E_y = 5048$
Diferencia	$E_x = 405$	$E_x = 185$	$E_x = 61$	$E_x = 79$	$E_x = 3$
	-	$E_y = 97$	$E_y = 123$	$E_y = 19$	$E_y = 95$

Tabla 3.1: Resultados de aleatoriedad al aplicar funciones trigonométricas y exponenciales en cada mapa caótico, durante cada operación se utilizó la función módulo 1 y el tiempo de cálculo se refiere a la demora en obtener el *P_value* para $n = 10,000$ (longitud de secuencias).

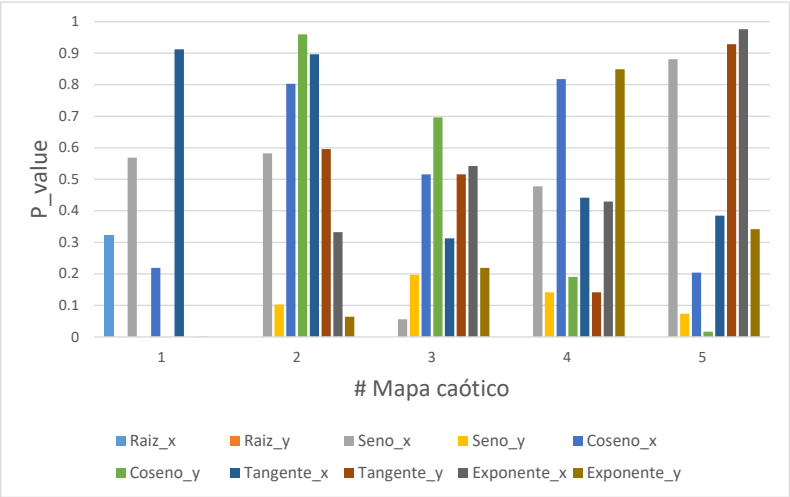

Figura 3.7: Gráfica del *P_value* obtenido en la prueba monobit para cada una de las funciones trigonométricas y exponencial.

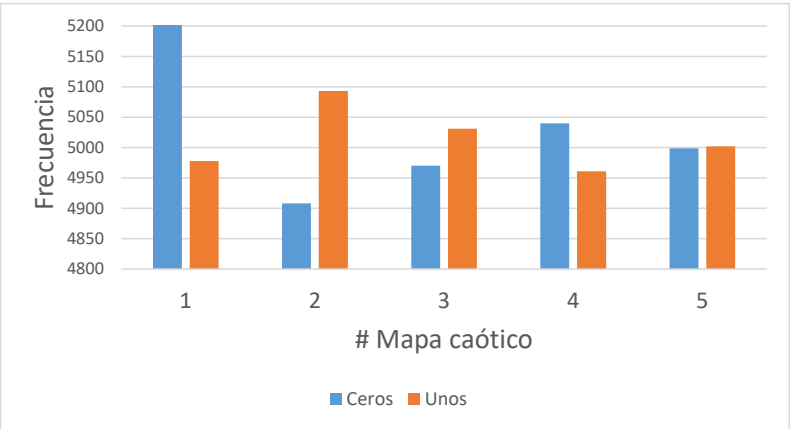

Figura 3.8: Frecuencia de ceros y unos del estado x para cada mapa caótico.

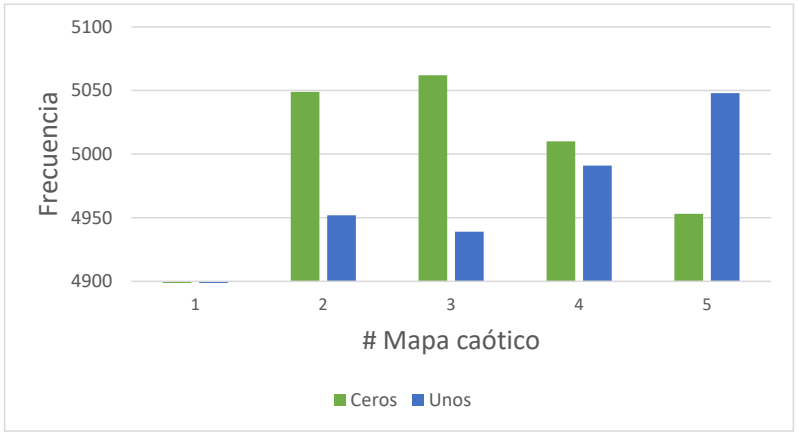

Figura 3.9: Frecuencia de ceros y unos del estado y para cada mapa caótico (excepto para mapa logístico).

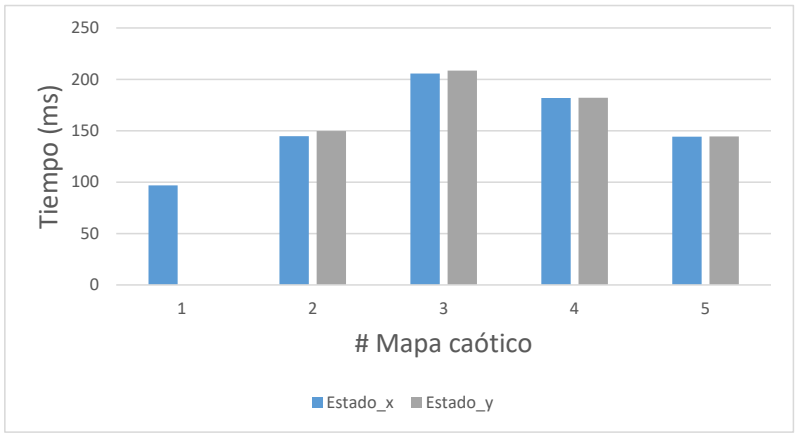

Figura 3.10: Tiempo de cálculo para la prueba monobit.

3.10. Conclusiones

Se presentaron los antecedentes del caos, así como sus principales precursores y sus características más representativas como la sensibilidad a condiciones iniciales y parámetros de control.

Con la prueba numérica del máximo exponente de Lyapunov, es posible determinar si el sistema presenta dinámicas caóticas. Con base a las pruebas de monobit (P_value) y tiempo de cómputo, se determinó el sistema caótico y la operación matemática a utilizar para uniformizar las secuencias caóticas, siendo, el mapa de Ushio y la función exponencial los que obtuvieron excelentes resultados, de esta manera el sistema tendrá una excelente aleatoriedad, una distribución más uniforme de los datos y un tiempo de procesamiento aceptable.

Capítulo 4

Criptografía

En este capítulo se destacan aspectos que permitieron el desarrollo de la criptografía durante su historia. También, se muestran algunos ataques, existentes que pueden ser utilizados para quebrantar el sistema criptográfico, así como los diferentes análisis que se pueden realizar para aportar robustez al sistema.

Finalmente, se muestran las tres categorías que están tomando más importancia en el campo de la criptografía no convencional, subrayando aspectos referentes al caos y sus atributos criptográficos en caos analógico y caos digital.

4.1. Introducción

Debido a los diferentes sucesos bélicos a lo largo de la historia, nace la necesidad de desarrollar estrategias de alta confidencialidad con la finalidad de conseguir la victoria. En ocasiones, estas órdenes estratégicas llegan desde sitios remotos y durante su transmisión puede ocasionar una intercepción del mensaje por los adversarios, significando una posible pérdida en combate. Con la finalidad de evitar estos problemas, surge la necesidad de resguardar la información por medio de sistemas criptográficos.

Se tiene constancia de una serie de jeroglíficos "no estándar" de más de 4,500 años de antigüedad, aunque no se sabe con certeza si obedecían a un intento serio por ocultar la información o si más bien corresponden a algún tipo de ritual. Mayor certeza se tiene con una tablilla babilónica fechada en el 2,500 A.C. En ella aparecen términos a los que se les ha retirado la primera consonante o emplea caracteres en variantes poco habituales. Investigaciones posteriores han revelado que su contenido se refiere a la descripción de un método para elaborar cerámica vidriada [34].

La criptografía es el arte de escribir en clave secreta o de un modo enigmático y es dividida en dos categorías: la clásica y la moderna. En la primera tenemos como ejemplo, la escítala que fue de los primeros elementos utilizados para transmitir un mensaje, su uso se remonta al siglo V A.C. por parte de los griegos, la cual, consistía en una tira

de cuero, tela o papiro con el mensaje grabado, enrollado en un cilindro de madera y utilizaba la técnica de cambio de posición (confusión o permutación). En el siglo I A.C., aparece el procedimiento conocido como cifrado de César, llamado así debido a que era implementado por el militar y político romano Julio César. Su funcionamiento consistía en sustituir cada carácter del mensaje original por otro situado tres posiciones después. En 1790, Thomas Jefferson creó un cilindro formado por varios discos coaxiales, cada uno de ellos con un alfabeto en la parte exterior [34, 35].

En 1920, se desarrollan dispositivos mecánicos de cifrado, dando lugar al nacimiento de la criptografía moderna, la cual, emplea rotores mecánicos principalmente. Se toma una clave sustituta y entonces se gira, esta idea ya había sido utilizada anteriormente en un número de claves de manera manual, pero al utilizar máquinas esto se realiza de manera más eficiente. Los rotores pueden ser implementados con cables y el cifrado puede ser aplicado mecánicamente con un circuito eléctrico. El más famoso de estos dispositivos fue la máquina Enigma, usada por los alemanes durante la Segunda Guerra Mundial.

En la figura 4.1, se muestra el esquema simplificado de la máquina Enigma. Para trazar las líneas rojas, se miran los carácter del texto claro A cifrado con un carácter del texto clave D. Nótese que cifrado y descifrado puede ser realizado por la máquina al comenzar en la misma posición. Asumiendo que el rotor uno se mueve un paso, así que, A corresponde a D, según el rotor uno, B a C, C a C y D a B [36]. Más máquinas como Enigma fueron desarrolladas, todas prácticamente con fines militares.

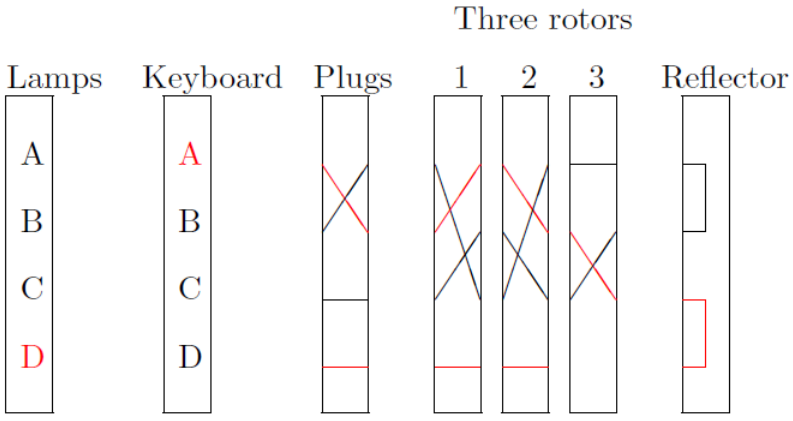

Figura 4.1: Esquema simplificado de la máquina Enigma [36].

En [37], Claude Shannon establece importantes fundamentos matemáticos para la teoría de la información y la comunicación, dando hincapié a las bases teóricas para los sistemas confidenciales establecidas en [38], lo que permitió a la criptografía dejar de ser tomada como un arte y ser reconocida como una ciencia [6]. En la figura 4.2, se presenta un diagrama esquemático general de un sistema confidencial.

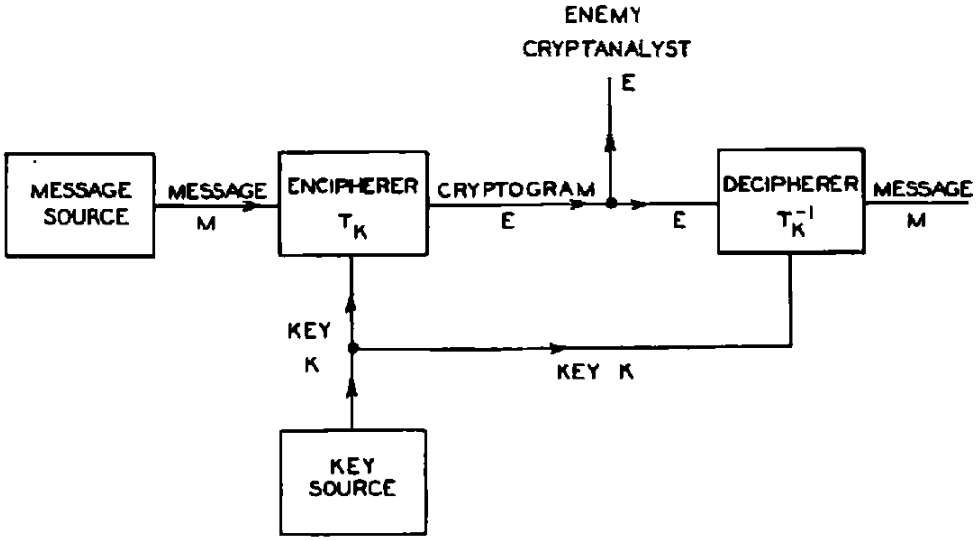

Figura 4.2: Esquema general de un sistema confidencial, representado por $E = f(M, K)$, donde M es el mensaje, K es la clave, y E el mensaje cifrado o criptograma (imagen extraída de [38]).

También se destacan cinco criterios para obtener un buen sistema confidencial:

- **Cantidad de confidencialidad:** Interceptar alguna cantidad del mensaje no debe presentar alguna ventaja para el adversario, es decir, que mediante dicha intercepción se logre obtener la solución única del criptograma. Por lo tanto, los sistemas de solución única presentan grandes variaciones entre la cantidad de material que debe ser interceptado y la cantidad de trabajo requerido para hacer que la solución sea única.

- **Tamaño de la clave:** La clave debe ser transmitida por medios no interceptables hasta el receptor autorizado, por lo tanto, es necesario tener la clave lo más pequeña posible.

- **Complejidad de las operaciones de cifrado y descifrado:** El cifrado y descifrado deben ser lo más simple posibles. Si se realizan manualmente, la complejidad ocasiona pérdida de tiempo, errores, etc. Si se hace mecánicamente, la complejidad conduce a usar máquinas grandes y costosas.

- **Propagación de errores:** En cierto tipo de claves, un error de una letra en el cifrado o transmisión ocasiona un largo número de errores en el texto descifrado.

- **Expansión del mensaje:** En algunos tipos de sistemas confidenciales, el tamaño del mensaje es incrementado por el proceso de cifrado. Este efecto indeseable puede observarse en sistemas en los que se intenta anular estadísticas del mensaje mediante la adición de muchos valores nulos o al utilizar varios sustitutos.

Como se puede hacer notar algunos de estos criterios han sufrido cambios en la actualidad debido a la aparición de las computadoras y a su desarrollo. Esto ha generado que los nuevos algoritmos de cifrado sean cada día más complejos, como el DES (Data Encryption Standard), primer algoritmo de cifrado estándar en los años 70's, AES (Advanced Encryption Standard), RSA (Rivest, Shamir y Adleman), entre otros.

La criptografía es uno de los ámbitos de las matemáticas aplicadas donde se hace más evidente la enormidad de las consecuencias humanas de su puesta en práctica. El destino de naciones enteras depende del éxito o el fracaso de mantener seguras las comunicaciones [34].

Como se mencionó al inicio de este capítulo, el surgimiento y desarrollo de la criptografía se debe en gran parte a los diversos sucesos bélicos a lo largo de la historia. Uno de los sucesos más destacables del uso de la criptografía se dio hace más de un siglo, el caso es conocido como "el telegrama Zimmermann".

El 7 de mayo de 1915, con media Europa sumida en un sangriento conflicto, un submarino alemán (U-Boat) lanzó un torpedo al barco de pasajeros Lusitania, el cual navegaba cerca de Irlanda. El resultado fue una masacre: 1,198 civiles, de los cuales, 124 eran de nacionalidad estadounidense y perdieron la vida ese día. Este suceso enfureció al gobierno del presidente Woodrow Wilson, advirtiendo a los alemanes que cualquier acto similar repercutiría en la inmediata entrada del gobierno norteamericano en la guerra.

Arthur Zimmermann fue nombrado por parte de Alemania ministro de Exteriores en noviembre de 1916, tal noticia fue bien recibida por la prensa norteamericana y calificó el nombramiento como el surgimiento de las relaciones entre Alemania y Estados Unidos.

En enero de 1917, el embajador alemán en Washington, Johann von Bernstorff, recibió por parte de Zimmermann un telegrama codificado, con la finalidad de que este último lo hiciera llegar a su homólogo en México, Heinrich von Eckardt. En el telegrama, propone inicialmente comenzar la guerra submarina. En caso de fallar, propone a México una alianza, en la que aparte de la contribución económica, se subraya, la posibilidad de reconquistar el territorio perdido en Nuevo México, Texas y Arizona. Además propone a México convencer a Japón de unirse a esta alianza y ser mediador entre los dos países.

Los alemanes no contaban con que al poco tiempo de iniciado el conflicto, el gobierno británico había bloqueado los cables telegráficos, por lo tanto, interceptó el mensaje remitiéndolo de forma inmediata a su departamento de criptoanálisis, conocido como Habitación 40.

Los alemanes emplearon para el cifrado su algoritmo convencional del ministerio de Exteriores y usaron una clave denominada 0075, la cual, ya había sido descifrada parcialmente por los expertos de la Habitación 40. De esta manera, el telegrama fue descifrado rápidamente.

Sin embargo, dicha información no fue mostrada a los Estados Unidos de manera inmediata, ya que el canal de comunicación había sido otorgado por los Estados Unidos para los mensajes diplomáticos alemanes (debido a la mejora en las relaciones, desde el nombramiento de Zimmermann) y a que el gobierno alemán cambiaría inmediatamente sus códigos al ver vulnerables sus sistemas de cifrado. De manera que tiempo después hicieron creer que el mensaje había sido interceptado en México ya descifrado y a finales de febrero fue filtrado el contenido del mensaje por parte del gobierno estadounidense, parte de la prensa se mostró escéptica, hasta que a mediados de marzo Zimmermann reconoció ser autor de dicho telegrama y el 6 de abril de 1917, el Congreso de Estados Unidos declaró la guerra a Alemania.

La criptología se divide en las siguientes ramas [39]:

- **Criptografía:** ciencia que estudia las técnicas y métodos para transformar la información (texto claro) de manera que no sea entendible (texto cifrado) por personas que no cuenten con autorización, este servicio de la criptografía se denomina confidencialidad. Otros servicios son:
  - Integridad: la información no se altera durante su transmisión o almacenamiento.
  - Autentificación: verifica la identidad de quien envió la información.
  - Vinculación: garantiza que el emisor envió la información.
- **Criptoanálisis:** ciencia que se ocupa de analizar el algoritmo y texto cifrado, para encontrar el texto claro o la clave secreta; de manera que criptoanálisis y criptografía son ciencias complementarias pero contrarias.
- **Esteganografía:** ciencia que estudia los métodos y técnicas que permitan ocultar mensajes dentro de otros, conocidos como portadores, de tal manera que no se perciba su existencia y pase inadvertido.

4.2. Claves

En criptografía, el término codificar se refiere a un método de escritura en clave que consiste en sustituir unas palabras por otras. La alternativa a este método es el cifrado, el cual sustituye letras o caracteres. Este último ha prevalecido convirtiéndose en sinónimo de escribir en clave. El término correcto para este último es cifrar (descifrar para el proceso inverso).

Por lo que, para transmitir de manera segura un mensaje “x”, puede hacerse de dos maneras: mediante la sustitución de la palabra (codificación) o sustituyendo alguna o la totalidad de las letras que la componen (cifrado). Una manera sencilla de codificar un mensaje es traducirlo a un idioma que los posibles “espías” desconozcan, mientras que para cifrarlo bastaría, por ejemplo, con sustituir cada letra por otra situada más

adelante en el alfabeto. Para ambos casos es necesario que el receptor conozca la regla empleada para cifrar el mensaje, de esta manera, solo tendría que traducirla de idioma o sustituir cada letra las posiciones acordadas.

Así, el espía podría saber que la regla de cifrado es sustituir cada letra por la correspondiente a "y" posiciones más adelante del alfabeto, pero al desconocer "y" deberá probar todas las combinaciones posibles. Debido a que el alfabeto cuenta con 27 letras, agotar todas las posibilidades mediante un descifrado por fuerza bruta no resulta extremadamente laborioso. Sin embargo, al emplear técnicas más complejas incrementa en espacio de claves y hace a este ataque ineficiente, además, hay que tener en cuenta otro parámetro muy importante, el tiempo: ya que la información debe ser obtenida con suficiente margen para poder actuar.

A la regla de cifrado se le denomina frecuentemente algoritmo de cifrado, mientras que al parámetro empleado para cifrar o codificar el mensaje (idioma o posiciones, para los ejemplos vistos anteriormente) se le denomina clave.

Dado un mismo algoritmo de cifrado, el número de claves puede ser muy grande, generalizando, para n usuarios son necesarias tantas claves como combinaciones de n usuarios escogidos de dos en dos, es decir:

$$n_2 = \frac{n(n-1)}{2} \tag{4.1}$$

De esta forma, para una población mundial de 7,000 millones de individuos, serían requeridas unas 2.45×10^{19} claves.

Conocer el algoritmo de cifrado resulta inútil a menos que conozca la clave utilizada en el proceso de cifrado, esto hace constar la importancia de las claves, además de que estas son más sencillas de modificar en caso de algún problema de seguridad, por lo tanto es lógico que sean concentrados los esfuerzos en proteger un sistema de cifrado que mantenga de manera secreta las claves. Este principio se debe al lingüista neerlandés Auguste Kerckhoffs von Nieuwenhof, denominado como "principio de Kerckhoffs".

El principio de Kerckhoffs determina a la clave como elemento fundamental en la seguridad de un sistema criptográfico. Todavía hace poco tiempo, las claves entre emisor y receptor de un sistema criptográfico tenían que ser iguales o simétricas, es decir, la misma clave se empleaba para cifrar y descifrar. Lo cual hace a la clave vulnerable, al ser compartida por dos usuarios. La criptografía dependiente de una misma clave compartida entre emisor y receptor se denomina clásica o de clave privada.

Parece ilógico, emplear una clave para cifrar y otra totalmente distinta para descifrar, de manera que el mensaje recuperado sea el mismo, durante mucho tiempo esta idea parecía absurda.

En la actualidad, algunos algoritmos de cifrado utilizan dos claves: una privada

(tradicional) y una pública conocida por todo el mundo. De manera que, el emisor se hace de la clave pública del receptor y la emplea para cifrar la información. Por su parte, el receptor utiliza su clave privada para descifrar el mensaje. Esto presenta una gran ventaja de seguridad al no compartir claves privadas. Este tipo de cifrado se conoce como clave asimétrica.

4.3. Seguridad de un sistema criptográfico

La comunidad criptográfica acordó que la protección de la clave es lo más importante para garantizar la seguridad del criptosistema, ya que el algoritmo criptográfico se considera de dominio público.

Las formas de vulnerar un sistema criptográfico son [40]:

- **Ataques teóricos (lógicos)**: Mediante la aplicación de la teoría de la información y criptoanálisis, con la finalidad de quebrantar el algoritmo. La seguridad es evaluada mediante análisis basados en métodos matemáticos.
- **Ataques físicos**: En este caso se aprovechan las posibles vulnerabilidades del sistema criptográfico, por ejemplo, la información de tiempo, el consumo de energía, fugas electromagnéticas o incluso sonido, pueden llegar a ser fuentes adicionales de información útiles para quebrantar el sistema criptográfico.
- **Ataque humanos**: Básicamente consta del uso de sobornos o ataques dirigidos a personas que poseen información privilegiada.

En la categoría de ataques físicos tenemos:

- Ataques de sincronización: Se basan medir el tiempo que lleva ejecutar los cálculos.
- Ataques de monitoreo de energía: Se emplean diferentes consumos de energía en el hardware durante un cálculo.
- Ataques electromagnéticos: Basados en la radiación electromagnética que puede proporcionar directamente textos claros y otra información. Un análisis de potencia puede determinar la clave.
- Análisis de sonido: Aprovechan el sonido producido durante algún cálculo.
- Remanencia de datos: Datos sensibles que se suponía habían sido borrados.

La categoría de ataques de tipo teórico, presenta:

- Ataque de fuerza bruta: Se prueban todas las posibles claves.
- Sólo texto cifrado: El criptoanalista conoce el algoritmo y el texto cifrado, utilizando dicha información con la finalidad de encontrar la clave. Para su seguridad, el espacio de claves debe ser suficientemente grande.

- Texto claro conocido: Ataque diferencial en el que el criptoanalista conoce el texto claro de un texto cifrado, de manera que utiliza esta información para descifrar otros criptogramas.
- Texto claro elegido: Ataque diferencial donde el criptoanalista selecciona su propio texto claro para cifrar, posteriormente hace una pequeña modificación (un bit o dato) al texto claro y vuelve a cifrar para determinar una relación entre la entrada y la salida para determinar la clave secreta.

4.4. Criptografía no convencional

Como se mencionó anteriormente, la criptografía convencional emplea propiedades algebraicas y numéricas, mientras que, la no convencional se basa en herramientas matemáticas en estado de investigación, tales como [6]:

- **Criptografía cuántica:** Basado en el principio de incertidumbre de Heisenberg, es decir, al observar un sistema cuántico éste se perturba a sí mismo, impidiendo que el observador conozca su estado exacto antes de la observación. De manera que al utilizar un sistema cuántico para transferir información, un espía e incluso el propio receptor se verían impedidos de obtener toda la información. Este tipo de criptografía hace uso de dos canales de comunicación, un canal cuántico distribuido en una sola dirección, generalmente una fibra óptica y un canal convencional, público y bidireccional para la transmisión de información, datos binarios (unos y ceros) son codificados mediante fotones (partícula portadora de todas las formas de radiación electromagnética).
- **Criptografía ADN:** El ADN tiene propiedades que pueden ser útiles en un sistema de criptografía, tales como: capacidad de almacenar mucha información, paralelismo (fenómeno evolutivo, que produce un cambio equivalente en dos ramas de una agrupación contenida en un antepasado común) y poco consumo de potencia. En la actualidad operaciones de ADN basadas en suma, complemento, eliminación e inserción, son utilizadas para el cifrado de información.
- **Criptografía caótica:** Basada en ecuaciones diferenciales no lineales que presentan alta sensibilidad a condiciones iniciales y parámetros de control, las cuales, producen dinámicas caóticas tipo "aleatorias"pero deterministas. No existe una fórmula simple que defina a un sistema caótico en cualquier punto dado, lo cual, es una ventaja de seguridad para su implementación en criptografía al proporcionar complejidad al sistema.

El caos tiene propiedades como transitividad topológica, ergodicidad, y sensibilidad a condiciones iniciales, lo que hace del caos adecuado para criptosistemas. Por ejemplo, la transitividad topológica permite utilizar la difusión (cambiar el valor de un dato) durante el cifrado y las condiciones iniciales son usadas como claves. La sensibilidad a condiciones iniciales dificulta los ataques de fuerza bruta [9]. Por lo tanto, en este trabajo de tesis se utiliza criptografía caótica.

4.5. Requerimientos para un cifrado caótico digital

En criptografía basada en caos analógico, requiere la construcción de circuitos analógicos. Además deben construirse dos circuitos o sistemas (uno para el receptor y otro para el transmisor), los cuáles, deben estar sincronizados. En tal sistema, una variable es suficiente para esclavizar al conjunto de ecuaciones diferenciales [7]. Sin embargo, este tipo de sistemas presentan problemas como baja sensibilidad a la clave secreta, espacio de claves reducido, fácil estimación de parámetros, extracción del texto claro de forma directa mediante filtrado, análisis de potencia, análisis de periodo corto, entre otros. De manera que se consideran poco seguros criptográficamente [41].

La criptografía caótica digital no requiere de técnicas de sincronización y su implementación se realiza en sistemas como computadoras, microcontroladores, etc. Con las condiciones iniciales y parámetros de control como clave secreta. Por lo tanto, criptografía caótica digital se empleará en este trabajo de tesis.

En [40], Alvarez y Li presentaron una serie de reglas que un sistema criptográfico basado en caos digital debe considerar:

- El sistema caótico utilizado debe ser descrito.
- La degradación digital debe ser evaluada, en caso de discretizar un sistema continuo.
- Fácil implementación, en base a costos aceptables y buena velocidad de cifrado.
- La clave secreta debe ser claramente definida.
- El espacio de claves debe ser especificada sólo para generar secuencias caóticas.
- El efecto avalancha debe producirse para cualquier clave secreta, es decir, alta sensibilidad a la clave secreta.
- Información parcial de la clave secreta no debe revelar información parcial del texto claro y tampoco parte de la clave secreta.
- El proceso para generar secuencias caóticas a partir de la clave secreta debe estar claramente definido.
- El cifrado debe tener alta sensibilidad al texto claro.
- El cifrado debe generar un texto cifrado con distribución de probabilidad uniforme.

Por último, para que un sistema criptográfico sea eficiente debe resistir los siguientes ataques criptográficos analíticos (de tipo lógico), en donde lo único no conocido debe ser la clave secreta:

- Ataques diferenciales. Ataques de tipo solo texto claro elegido conocido, de manera que el sistema criptográfico debe mostrar alta sensibilidad a la clave secreta y al texto claro, para que pueda resistirlos.
- Ataques estadísticos. Ataques de histogramas y correlación, donde se muestra la uniformidad del texto cifrado, de manera que pueda resistir estos ataques.
- Ataques exhaustivos. Ataque en el que se prueba todas las posibles combinaciones de claves, por lo tanto, esta debe de contener más de 2^{100} opciones [40].

4.6. Conclusiones

Se conocieron algunos aspectos importantes de la criptografía, así como, el entendimiento de que principalmente los sucesos bélicos son los que han permitido su desarrollo, por lo que, la mejor manera de evolucionar a la criptografía es enfocarla en aspectos que beneficien a la sociedad en general, tal es el caso de este trabajo, el cual está dirigido a fortalecer la seguridad de la telemedicina, particularmente en telemetría.

Además, se mostraron características primordiales de la criptografía como: los diversos criterios para obtener un buen sistema confidencial (criptográfico), las ramas en las que se divide, aspectos importantes de la clave y los diferentes ataques que puede sufrir el sistema.

Finalmente, se determinaron los aspectos que permitieron que la criptografía caótica fuese la principal base de este trabajo, resaltando su aspecto más relevante como lo es la sensibilidad a condiciones iniciales y complejidad del sistema, aspecto fundamental para dificultar los ataques de fuerza bruta y por último se conocieron los requerimientos básicos para su implementación de manera digital.

Capítulo 5

Algoritmo de cifrado caótico propuesto

5.1. Introducción

La telemetría es una técnica de las comunicaciones que permite realizar mediciones y obtención de información en lugares distantes. Regularmente utiliza transmisión inalámbrica y permite llevar a cabo actividades de monitoreo. Tal es el caso del área de la medicina donde se utiliza para el monitoreo de signos vitales (ver Sección 2.3).

Al estar relacionada con mediciones, la telemetría permite abarcar diversas áreas. En México se encuentra más orientada a la agricultura para conocer el estado de equipos, procesos, sistemas y controlar remotamente funcionamientos [42].

En el área médica, las señales de ECG cambian de persona a persona. Comparado con un sistema biométrico común, las características biométricas del ECG son extremadamente difíciles de duplicar. Por lo tanto, un ECG puede ser usado como una herramienta biométrica para la identificación de individuos [43]. Cambios en el ECG puede indicar problemas cardíacos como fibrilación auricular, insuficiencia cardíaca, taquicardia auricular multifocal, taquicardia paroxística supraventricular, síndrome del seno enfermo y síndrome de Wolff-Parkinson-White. La presión arterial (BP) va acompañada de exámenes adicionales entre ellos el ECG [11, 13].

La señales biomédicas de EEG han sido usadas desde 1950 para monitorear o diagnosticar a pacientes con coma, demencia, tumores, problemas de memoria a largo plazo, Alzheimer, traumatismos craneales, infecciones, cambios anormales en la química corporal que afectan al cerebro, convulsiones y epilepsia. También se usa en evaluaciones de muerte cerebral para probar legalmente que el paciente con equipo de soporte vital no se recuperará. De manera que, esto hace que ECG, EEG y BP sean información importante en telemetría. Sin embargo, transmiten rutinariamente esta información privada a través de un canal inseguro para su diagnóstico. Cuando los datos son obtenidos para propósitos de telemedicina, se convierte en información biomédica obligada a ser protegida para evitar accesos no autorizados [12, 44].

En un mundo en el que la tecnología avanza día con día es importante brindar la protección necesaria a la información sensible de los pacientes, de manera que se brinde la mayor tranquilidad posible de que sus datos médicos solo serán vistos por el personal autorizado. De manera que la opción viable es cifrar la información, mediante un algoritmo de cifrado caótico.

Recientemente, se han propuesto algoritmos de cifrado basados en caos para telemedicina, con la utilización de señales ECG y EEG. En 2016, Raeiatibanadkooki *et al.* [45] presentaron un moderno esquema de compresión y cifrado de ECG usando ondícula (transformada matemática) y el código Huffman, con el objetivo de comprimir la señal sin que haya pérdida de información esencial y también cifrar la información para que sea confidencial excepto para médicos. Se implementó en un procesador móvil y la señal cifrada de ECG se envió a un centro de telemedicina mediante el protocolo TCP/IP (hace posible servicios como E-mail, Telnet Y FTP entre ordenadores no pertenecientes a la misma red). Sin embargo, no se presentó ningún análisis de seguridad.

En el mismo año, Lin propuso un criptosistema visual caótico usando un algoritmo de descomposición y dos mapas logísticos para EEG. Se realizaron las pruebas de error cuadrático medio (MSE, mean square error) y correlación entre la señal original y la señal cifrada, arrojando excelentes resultados [46].

En 2014, Kenfack y Tiedeu proponen en [47] un cifrador de ECG basado en caos y resultados experimentales con osciladores Colpitts (circuito basado en un oscilador LC) caóticos. El sistema fue implementado y probado mediante un circuito electrónico con buenos resultados, pero ningún análisis de seguridad fue efectuado.

En [48] se propuso un esquema de cifrado caótico para EEG basado en el mapa logístico pero ningún análisis de seguridad fue presentado.

En [43], Chen *et al.* presentaron un esquema de cifrado personalizado para ECG, el mapa logístico se implementó para el cifrado de texto y el mapa Hénon para el de imagen. Contó con los análisis de histogramas y espacio de clave.

Por lo tanto, es importante el diseño de sistemas criptográficos basados en caos, pero más importante es mostrar que son seguros y eficientes.

El algoritmo propuesto en este trabajo de tesis se basa en las siguientes características criptográficas [49]:

- Cifrado simétrico. Es empleada la misma clave secreta para cifrar y descifrar.
- Arquitectura de confusión y difusión. El algoritmo emplea procesos para cambiar de posición y de valor a cada elemento claro (señal original) en una sola operación.

- Cifrado a flujo. Cada elemento del texto claro es cifrado uno por uno. Los elementos utilizados se representan por 8 bits (1 byte).
- Cifrado no convencional. El mapa caótico de Ushio es empleado para generar las dinámicas caóticas, que son determinadas por la clave secreta para generar secuencias pseudoaleatorias para efectuar el proceso de confusión y difusión.

En la figura 5.1, se muestra el diagrama a bloques del proceso de cifrado propuesto basado en [6], donde, el mapa de Ushio número 2 se itera en base a la clave secreta, después se obtiene el valor de Z relacionado con la señal clara y las secuencias caóticas del mapa de Ushio 2, posteriormente, el mapa de Ushio número 1 es iterado con base en la clave secreta y el valor de Z con la finalidad de llevar a cabo los procesos de confusión y difusión sobre la señal clara, finalmente, el valor de Z es añadido al criptograma para que el usuario autorizado pueda descifrar adecuadamente.

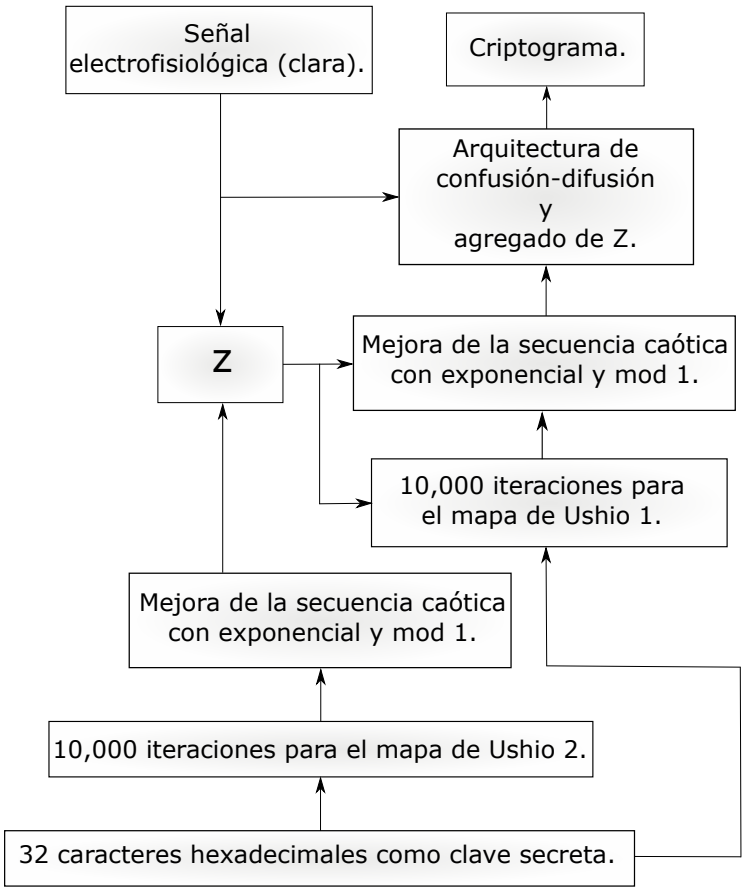

Figura 5.1: Diagrama a bloques del proceso de cifrado.

Para el descifrado, cuyo diagrama se muestra en la figura 5.2, primero se extrae el valor de Z de una parte del criptograma (el valor no es calculable del criptograma), posteriormente 10,000 datos son calculados del mapa de Ushio 1 con la ayuda de la clave secreta y el valor de Z, finalmente, se efectúan los procesos inversos de confusión y difusión para recuperar la señal clara.

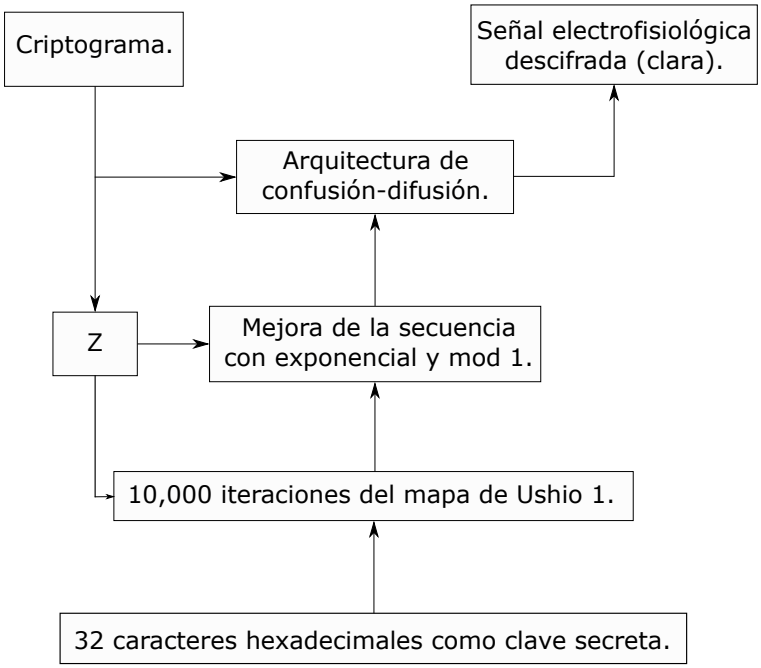

Figura 5.2: Diagrama a bloques del proceso de descifrado.

5.2. Clave secreta

La clave utilizada es de 128 bits representada por 32 caracteres hexadecimales. La cual es dividida en cuatro secciones y cuatro números son calculados (A, B, C y D), los cuales son empleados para determinar las condiciones iniciales y el parámetro de control

de los dos mapas de Ushio utilizados en este trabajo. En la tabla 5.1, se muestran los cálculos utilizados:

Clave secreta	Parámetro de control				Condición inicial	
32 dígitos Hex	$H_1, H_2, \ldots, H_{32}$ donde $H \in [0-9, A-F]$					
Cálculos	$A = \frac{(H_1, H_2, \ldots, H_8)_{10}}{2^{32}+1}$	$B = \frac{(H_9, H_{10}, \ldots, H_{16})_{10}}{2^{32}+1}$	$C = \frac{(H_{17}, H_{18}, \ldots, H_{24})_{10}}{2^{32}+1}$	$D = \frac{(H_{25}, H_{26}, \ldots, H_{32})_{10}}{2^{32}+1}$		
Ushio 1	$p_1 = 1.900 + [((A+B+Z) mod 1) * 0.001]$				$x_{1_0} = y_{1_0} = 0.5 + [((C+D+Z) mod 1) * 0.1]$	
Ushio 2	$p_2 = 1.900 + [((A+B) mod 1) * 0.001]$				$x_{2_0} = y_{2_0} = 0.5 + [((C+D) mod 1) * 0.1]$	

Tabla 5.1: Cálculo de parámetro de control y condiciones iniciales mediante la clave secreta.

5.3. Cálculo de Z

Con este valor se incrementa la sensibilidad a pequeños cambios de la señal clara P y la clave secreta a nivel de bit, además hace que el cifrado sea robusto ante ataques diferenciales (ataques de texto claro y de texto elegido). El valor de Z se obtiene al sumar todos los valores de la señal clara P con la secuencia de datos caóticos del segundo mapa de Ushio. El mapa es iterado I_2 veces con el parámetro de control p_2 y las condiciones iniciales x_{2_0} y y_{2_0}, obtenidos mediante la tabla 5.1 generando una secuencia caótica de datos $x^{U2} = x_1^{U2}, x_2^{U2}, x_3^{U2}, \ldots, x_{I_2}^{U2}$ con $x^{U2} \in (0, 1)$. A continuación la secuencia caótica es mejorada con la siguiente expresión:

$$x_i^{U2} = \left((e^{x_i^{U2}}) * 100\right) \quad (\text{mód } 1), \quad para\ i = 1, 2, 3, \ldots, I_2, \tag{5.1}$$

donde I_2 es el número de iteraciones para el mapa de Ushio 2, que depende de la señal electrofisiológica y *mod 1* es la operación módulo. Posteriormente, todos los elementos de la señal clara se suman con x^{U2}, de la siguiente manera:

$$Z = \left\{Z + [P_i * x_{I_2+1-i}^{U2}] + x_{I_2+1-i}^{U2}\right\} \quad (\text{mód } 1), \quad para\ i = 1, 2, 3, \ldots, I_2, \tag{5.2}$$

donde P_i representa el elemento i de la señal clara, Z es una variable inicializada en cero y x^{U2} corresponde a la secuencia caótica del mapa Ushio 2.

5.4. Cifrado

El mapa de Ushio 1 es iterado $I_1 = 10,000$ veces (para la señal EEG aumenta a más de 20,000) con los valores p_1 y las condiciones iniciales x_{1_0} y y_{1_0} obtenidos de la tabla 5.1, de esta manera, se genera la segunda secuencia de datos caóticos $x^{U1} = x_1^{U1}, x_2^{U1}, x_3^{U1}, \ldots, x_{I_1}^{U1}$ con $x^{U1} \in (0, 1)$. Las dinámicas caóticas de la secuencia x^{U1} es mejorada mediante la siguiente expresión:

$$x_i^{U1} = \left((e^{x_i^{U1}}) * 100\right) \quad (\text{mód } 1), \quad para\ i = 1, 2, 3, \ldots, I_1 \tag{5.3}$$

En la figura 5.3, se muestra la distribución caótica de Ushio y con mejoramiento, lo que resulta en una distribución más uniforme.

La secuencia caótica x^{U1} determina subsecuencias para los procesos de confusión y difusión. Para el proceso de confusión, la subsecuencia se calcula con la siguiente expresión:

$$CF_i = \ round\left[x^{U1}_{I_1-\ell+i} * (\ell - 1)\right] + 1, \quad para\ i = 1, 2, 3, \ldots, \ell \tag{5.4}$$

donde ℓ representa la longitud requerida y $CF \in [1, \ell]$ es el vector pseudoaleatorio para el proceso de confusión. Durante un proceso de confusión eficiente, todos los elementos de la señal clara son permutados (cambió de posición) entre sí mismos, sin embargo, la Ec. (5.4) genera valores para reposicionamiento repetidos. Por lo que, los valores repetidos de CF se cambian mediante programación con ayuda de la siguiente expresión:

$$G_h = [K_h], \quad con\ h \ll \ell \tag{5.5}$$

donde K_h es un valor en orden ascendente que no se encuentra presente en el vector CF. El vector de valores repetidos G es dividido en dos secciones, cada valor se asigna a CF de manera alternada cada vez que aparece un valor repetido. Al finalizar este proceso, se cuenta con un vector para confusión con todas las posibles posiciones (confusión optimizada).

La subsecuencia para difusión se determina con x^{U1} con la misma longitud ℓ. Aunque el mapa de Ushio presenta una mejor distribución de los datos, aún hay tendencias marcadas hacia ciertos valores, lo cual puede llevar a un proceso de difusión ineficiente. La solución al problema es eliminar los primeros tres decimales de la secuencia caótica (Eq.5.3) y sólo para una determinada longitud de ℓ. La subsecuencia se obtiene como se muestra a continuación:

$$DF_i = \left(x^{U1}_{I_1-\ell+i} + Z\right) \pmod 1, \quad para\ i = 1, 2, 3, \ldots, \ell \tag{5.6}$$

donde $DF_i \in (0, 1)$ es el vector pseudoaleatorio para el proceso de difusión con longitud ℓ (por seguridad solo son tomados los últimos datos de la secuencia x^{U1}). Dependiendo la aplicación, el vector para difusión es determinado mediante DF.

El proceso de cifrado se calcula mediante la expresión:

$$E_i = P(CF_i) + DF_i, \quad para\ i = 1, 2, 3, \ldots, \ell \tag{5.7}$$

donde P es la señal clara y E el criptograma (señal encriptada).

El valor de Z debe ser incluido en el criptograma, para que el usuario autorizado pueda recuperar la información correctamente, debido a que no se puede calcular directamente del criptograma E, de esta manera, dicho valor es añadido al final del proceso.

5.5. Descifrado

Este proceso consiste en invertir cada uno de los pasos desarrollados en el cifrado y con exactamente la misma clave de 128 bits, en caso contrario, un solo bit de diferencia

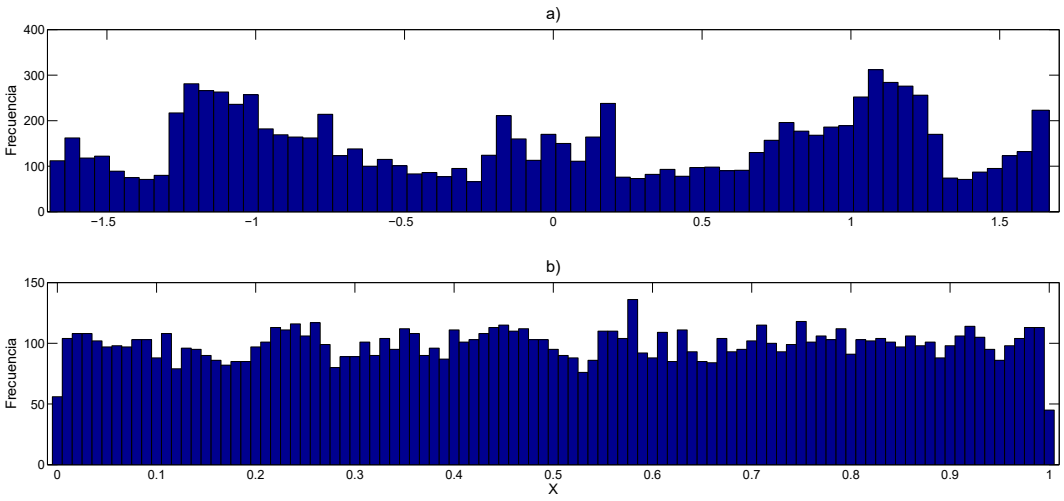

Figura 5.3: Histogramas **a)** mapa de Ushio y **b)** mapa de Ushio con implementación de la mejora.

en la clave secreta no permite la recuperación de la señal clara.

Lo primero es recuperar el valor de Z. Posteriormente, el mapa de Ushio 1 es iterado 10,000 veces (EEG, el número aumenta) con la clave secreta y el valor de Z. A continuación, se calculan las subsecuencias CF y DF (confusión y difusión). Por último, el descifrado se realiza con la siguiente expresión:

$$D_i(CF_i) = E_i - DF_i, \quad para\ i = 1, 2, 3, \ldots, \ell \tag{5.8}$$

donde E es el criptograma y D es la señal recuperada.

5.6. Espacio de clave secreta

Un algoritmo de cifrado debe resistir un ataque exhaustivo, donde todas las posibles claves son probadas en el criptograma. De manera que un aspecto importante a tomar en cuenta es que el espacio de clave secreta, sea suficiente considerando el poder actual de computación. Alvarez y Li recomiendan que el espacio de clave secreta debe ser mayor a 2^{100} [40]. El algoritmo de este trabajo presenta un clave secreta de 128 bits, por lo tanto, el espacio de claves es de 2^{128}.

5.7. Funcionamiento del algoritmo propuesto

Para comprobar el correcto funcionamiento del algoritmo criptográfico caótico, se obtuvieron señales clínicas (ver figura 5.4) de la base de datos en internet PhysioBank ATM desde el sitio *www.physionet.org*, las cuales se usaron para conocer la respuesta del algoritmo criptográfico (figura 5.5) mediante el empleo de la clave secreta

$E3F48B2326D641B57B0CF3EEC509D780$. En el caso de la señal de EEG el número de iteraciones aumenta a más de 20,000 debido a que la señal contiene más información, haciendo que el criptograma abarque mayor área (figura 5.5(b)).

En la tabla 5.2, se muestran los resultados de tiempo de ejecución del algoritmo de cifrado para cada una de las señales electrofisiológicas. A continuación se muestran las características de cada una de las señales utilizadas:

- **Electrocardiograma (ECG):** Señal obtenida del monitoreo de la apnea del sueño, se descargó de la fuente *"apnea-ecg/a01val"*. La señal tiene una duración de 10 segundos, una amplitud en milivolts, ganancia de 200 y frecuencia de muestreo Fs= 100 Hz.
- **Electroencefalograma (EEG):** Monitoreo de una prueba de presentación visual serial rápida (RSVP, por sus siglas en inglés), obtenida de la fuente "$ltrsvp/10-Hz/rsvp_10Hz_02a.edf''$. Cuenta con una duración de 10 segundos, la amplitud en microvolts, ganancia de 31.99 y Fs= 2.048 KHz.
- **Presión de la sangre (BP):** Prueba de presión de la sangre debido a la sensibilidad a la sal, en ratas. La señal se extrajo de la fuente "$bpssrat/ssbn13hs01val''$. Consta de una duración de 10 segundos, amplitud en miligramos de mercurio (mmHg), ganancia de 100 y Fs= 100 Hz.

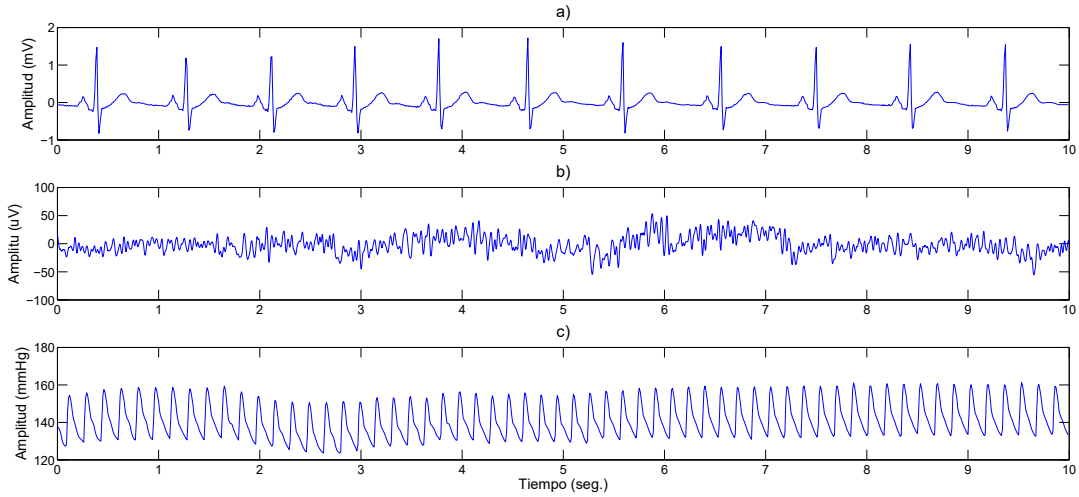

Figura 5.4: Señales electrofisiológicas obtenidas de PhysioBank: **a)** EGC, **b)** EEG y **c)** BP.

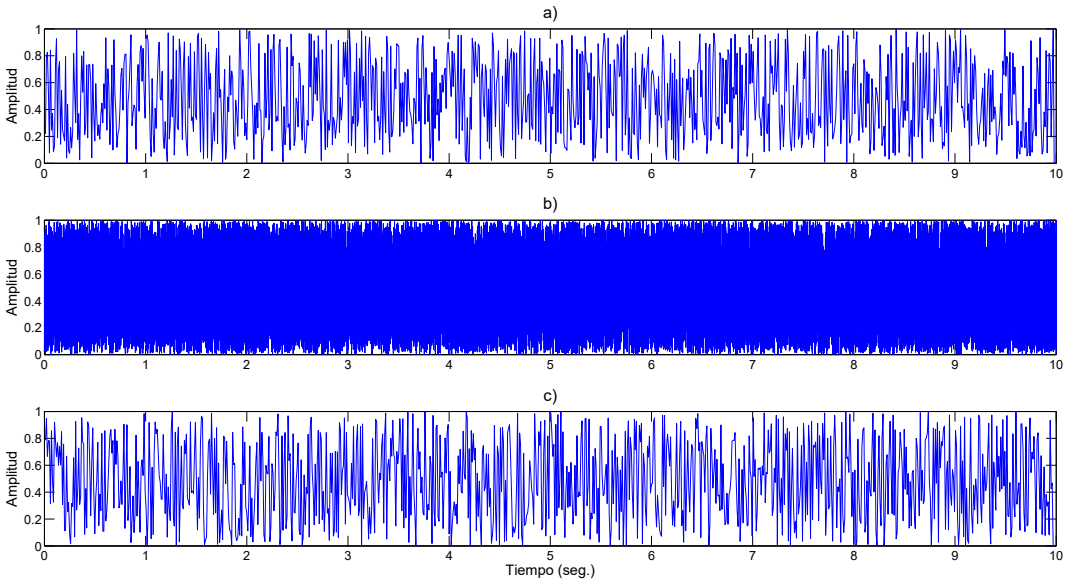

Figura 5.5: Criptogramas: **a)** EGC, **b)** EEG y **c)** BP.

Señal	Longitud	Tiempo de cifrado	Tiempo de descifrado
ECG	$10\ seg \times 100$ Hz$= 10,000$	83.954 ms	57.352 ms
EEG	$10\ seg \times 2,048$ Hz$= 20,480$	8.22 s	7.46 s
BP	$10\ seg \times 100$ Hz$= 10,000$	98.464 ms	63.167 ms

Tabla 5.2: Tiempo de cómputo para el cifrado y descifrado de las señales de 10 segundos.

5.8. Análisis de seguridad estadísticos

5.8.1. Coeficiente de correlación

El coeficiente de correlación determina si la señal clara y la cifrada están desvinculadas. El coeficiente de correlación es $Cr \in (-1, 1)$, donde 0 representa una correlación nula. A continuación se muestra la ecuación para determinar Cr [6, 20]:

$$Cr = \frac{N \times \sum_{i=0}^{N}(x_i \times y_i) - \sum_{i=0}^{N} x_i \times \sum_{i=0}^{N} y_i}{\sqrt{\left(N \times \sum_{i=0}^{N}(x_i)^2 - \left(\sum_{i=0}^{n} x_i\right)^2\right) \times \left(N \times \sum_{i=0}^{N}(y_i)^2 - \left(\sum_{i=0}^{n} y_i\right)^2\right)}}, \tag{5.9}$$

donde x y y son los valores de cada señal a comparar y N es el tamaño de la señal clara. La prueba consiste en calcular el coeficiente de correlación entre la señal clara y 1,000 criptogramas para cada señal, generados mediante 1,000 claves seleccionadas aleatoriamente. El promedio de correlación es $-4.36145265731 \times 10^{-4}$ para ECG, $1.419282475011 \times 10^{-3}$ para BP y $-2.13408713388 \times 10^{-4}$ para EEG. Los resultados muestran una alta eficiencia del algoritmo caótico de cifrado al generar criptogramas altamente desvinculados a partir de señal clara correspondiente.

5.8.2. Autocorrelación

Se define como la correlación de una señal consigo misma pero desplazada k posiciones. Este análisis puede brindar información sobre las características en la señal clara y cifrada, tales como: periodicidad, dependencia y repetición de patrones.

La autocorrelación es calculada a nivel de bit para ambos casos: señal clara y señal cifrada. Se utilizó 52-bits de acuerdo a IEEE 754, los datos son definidos del tipo doble punto flotante (double floating-point) todos ellos entre (0,1). En esta prueba se utiliza $k = 25,000$. Los resultados de la prueba se muestran en la figura 5.6, se aprecia que la señal clara presenta patrones repetitivos debido a los altos valores positivos de autocorrelación (ACr), mientras el ACr de la señal cifrada es cercana a cero. Por lo que, se concluye que la señal cifrada no presenta periodicidad o patrones repetitivos, haciendo al algoritmo robusto para producir criptogramas sin dependencia o periodicidad.

5.8.3. Frecuencia flotante

Esta prueba verifica la distribución uniforme de la información cifrada mediante ventanas de 1,000 elementos. Un electrocardiograma (ECG) de 60 segundos con frecuencia de muestreo Fs=100 Hz es cifrado y ambas señales son analizadas. Los 6,000 valores de la señal clara y de la cifrada son concatenados entre (0,1) con incrementos de 0.001. La frecuencia flotante de la señal cifrada debe ser uniforme y puede tener todos los 1,000 elementos posibles, idealmente. El proceso de la prueba se muestra a continuación:

- Se selecciona una ventana de los primeros 1,000 elementos y se determina cuantos elementos de los 1,000 posibles son diferentes.

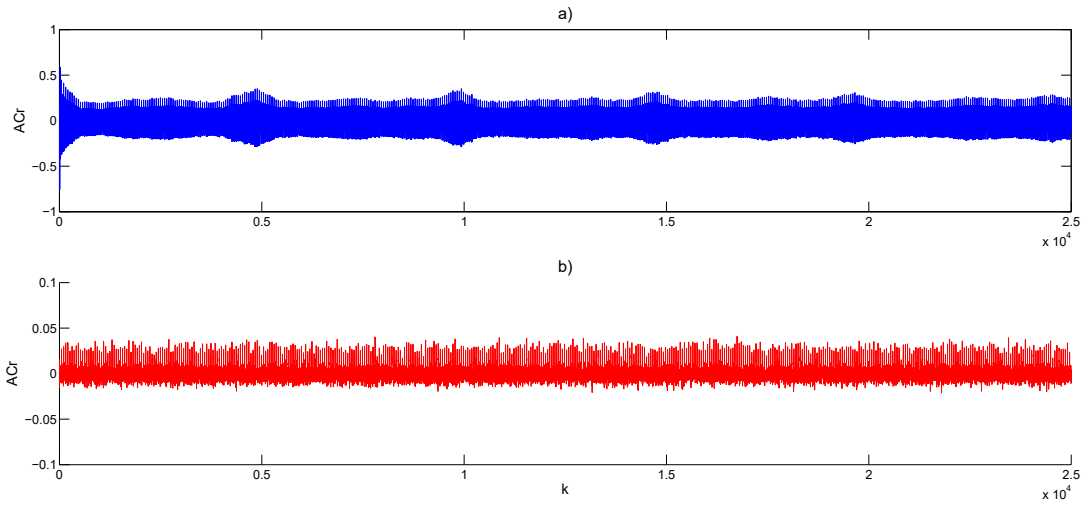

Figura 5.6: Análisis de autocorrelación de un electrocardiograma (ECG): **a)** señal clara y **b)** señal cifrada.

- La ventana es desplazada una posición a la derecha con rotación circular hasta el elemento 5,001 y se obtiene la frecuencia flotante para cada ventana.

En la figura 5.7, se muestran los resultados obtenidos en la prueba, para la señal ECG. El promedio de elementos diferentes en la señal clara es 19.3 %, mientras que para la señal cifrada es 82.4 %. La figura 5.7(b), muestra que el criptograma no presenta secciones débiles estadísticamente, por lo tanto, cada ventana de prueba presenta valores uniformes de frecuencia flotante. Estos resultados validan la prueba de autocorrelación, por lo tanto, el criptograma presenta altas capacidades de uniformidad. La frecuencia flotante es muy utilizada para determinar la eficiencia del algoritmo de cifrado, una alta frecuencia flotante significa alta seguridad en el algoritmo de cifrado.

5.8.4. Histogramas

Este análisis muestra de manera gráfica la distribución de los datos de una señal, de esta forma, entre más uniforme sea el histograma, el algoritmo de cifrado presenta excelentes propiedades estadísticas. En la figura 5.8, se muestra la distribución de los datos claros no uniformes. Por otra parte, en la figura 5.9 se observa que los valores de señales cifradas presentan una mejor uniformidad.

5.8.5. Entropía

En la teoría de la información, la entropía es la medición de la imprevisibilidad o incertidumbre relacionada con secuencias aleatorias. En criptografía, la entropía es inyectada en la señal clara mediante el algoritmo para neutralizar su estructura de naturaleza clara. Una alta entropía indica un proceso eficiente de cifrado y un valor bajo indica un proceso de cifrado débil con cierto grado de predictibilidad del criptograma. Los valores del criptograma entre (0,1) se transforman a valores entre [0, 255] es decir

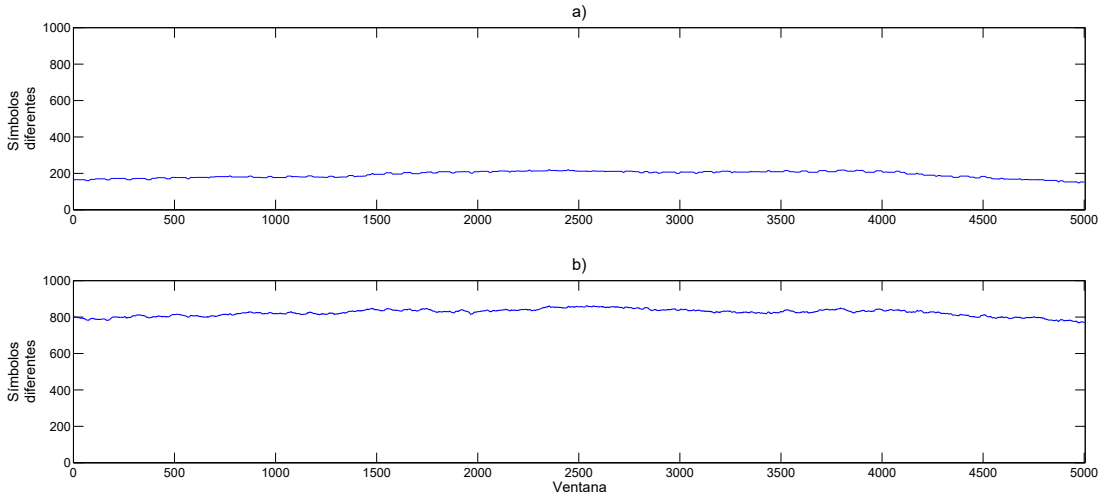

Figura 5.7: Análisis de frecuencia flotante para electrocardiograma (ECG): **a)** señal clara y **b)** señal cifrada.

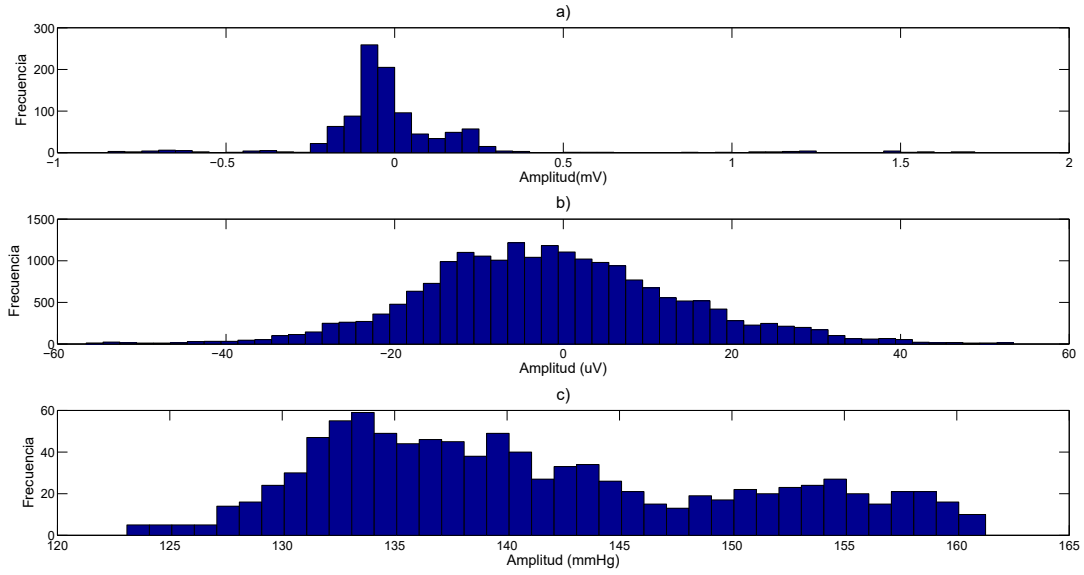

Figura 5.8: Histograma de la señal clara: **a)** ECG, **b)** EEG y **c)** BP.

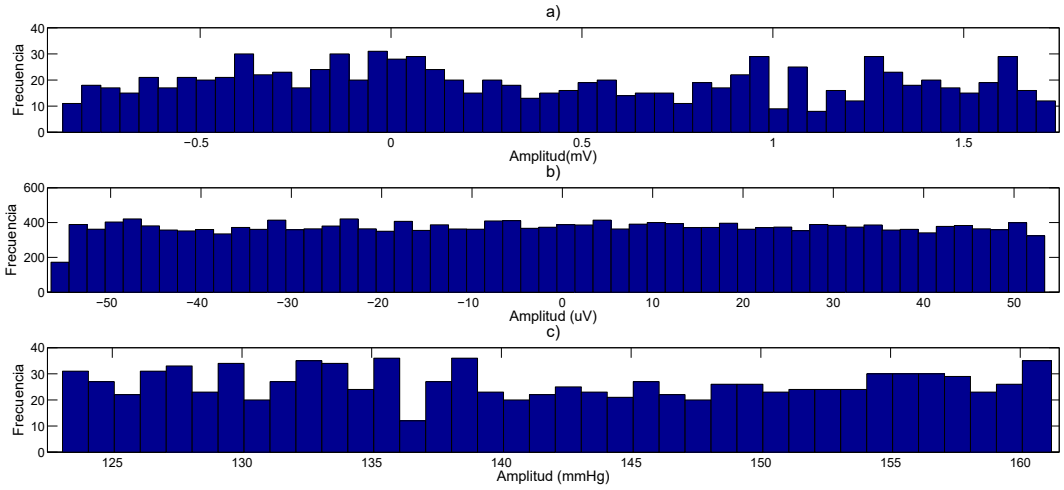

Figura 5.9: Histograma de la señal cifrada: **a)** ECG, **b)** EEG y **c)** BP.

datos de 8 bits, por lo tanto, el valor máximo de entropía es 8. La fórmula para calcular la entropía se muestra a continuación:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\ log_2(1/p(m_i)), \tag{5.10}$$

donde N es el número de bits que representan la unidad básica del mensaje m, 2^N son todas las combinaciones de la unidad básica, $p(m_i)$ representa una probabilidad de m_i, $\log_2$ es el logaritmo base 2 y la entropía esta expresada en bits, donde la máxima entropía es N. Si un mensaje m es cifrado con 2^N posibles valores, la entropía debería ser idealmente $H(m) = N$, si m es puramente aleatorio.

En la prueba se generan 100 criptogramas a partir de 100 claves secretas obtenidas aleatoriamente, la señal empleada es la BP (presión arterial) de 60 segundos y una Fs=100 Hz (frecuencia de muestreo). El promedio de entropía es 7.9680, por lo tanto, todos los criptogramas son 99.6 % impredecibles. La figura 5.10, muestra la gráfica de la prueba.

5.9. Análisis de seguridad diferencial

La tasa de cambio neto de píxeles (NPCR, por sus siglas en inglés) y la intensidad media de cambio unificado (UACI, por sus siglas en inglés) son empleadas en cifrado basado en caos de imágenes para análisis diferenciales.

En este análisis, se generan dos criptogramas (C_1 y C_2) con la misma clave secreta pero con dos señales claras altamente similares entre ellas. Dos señales claras de BP son usadas modificando un valor, en este caso $Y_{BP}(500)$ al sumarle 5×10^{-4}, para

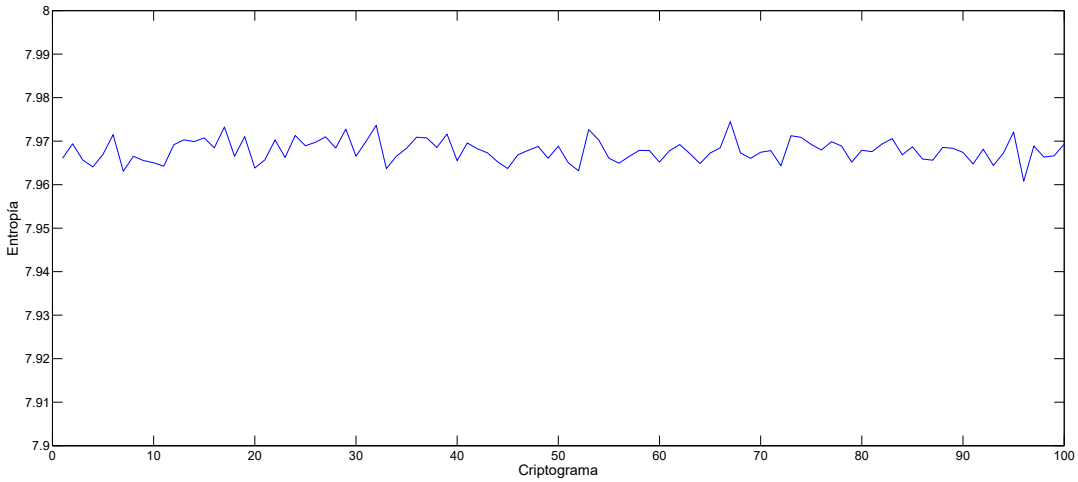

Figura 5.10: Gráfica de la entropía de 100 criptogramas generados mediante 100 claves secretas obtenidas aleatoriamente.

posteriormente cifrar la señal. El criptograma C_1 siempre se mantiene igual, mientras el C_2 es generado 1,000 veces usando 1,000 claves secretas seleccionadas aleatoriamente.

El promedio en todas las pruebas de NPCR es 100 % y de UACI es 33.9 %. Esto muestra que cada par de criptogramas tienen valores 100 % diferentes entre ellos con un promedio de 33.9 % en magnitud. La figura 5.11, muestra los resultados gráficos de la prueba.

En base a los resultados obtenidos, se verifica que el esquema propuesto es altamente sensible a pequeños cambios en la señal clara.

5.10. Sensibilidad a la clave secreta

Este análisis prueba y verifica la sensibilidad a la clave secreta. Para que un sistema criptográfico sea eficiente debe ser sensible a pequeños cambios de la clave secreta tanto para cifrado como para descifrado.

Para verificar la sensibilidad a la clave secreta en el proceso de cifrado, la señal de ECG se cifra con 3 claves similares y los criptogramas son comparados entre sí mediante el análisis de correlación, ver sección 5.8.1, una correlación de cero indica que las señales son totalmente diferentes. Los resultados se muestran en la tabla 5.3.

En el proceso de descifrado únicamente la clave correcta puede recuperar la señal original, es decir, la señal no podrá ser recuperada en caso de utilizar claves similares (1 bit de diferencia). La figura 5.12(a), muestra la señal descifrada con la clave secreta correcta para ECG. Mientras que las figuras 5.12(b-c) muestran las señales descifradas

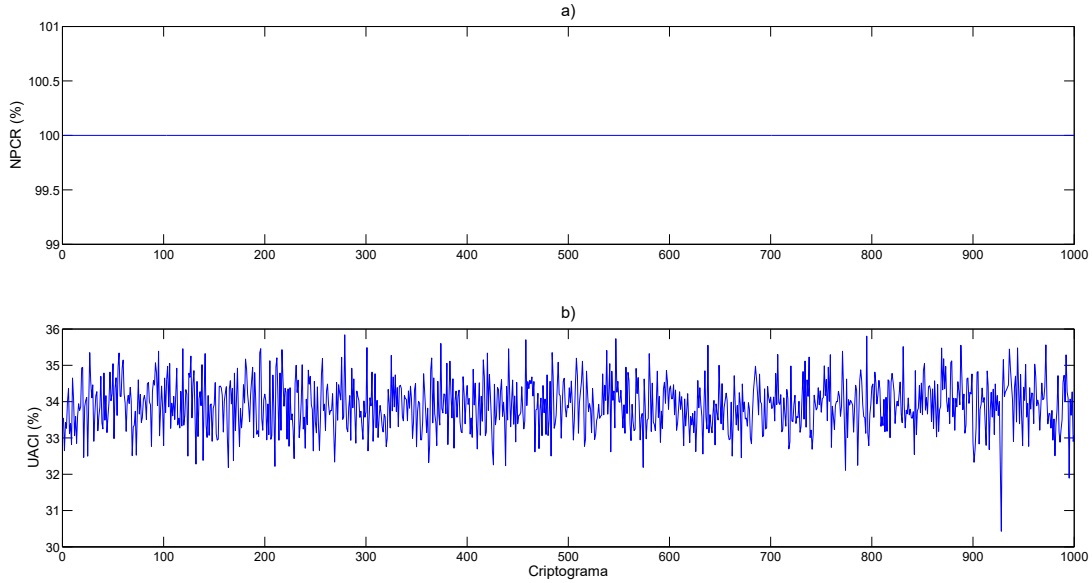

Figura 5.11: Gráfica de la sensibilidad de la señal clara: **a)** NPCR y **b)** UACI.

con claves incorrectas de un bit de diferencia.

La prueba se realizó con:

- Clave 1. E3F48B2326D641B57B0CF3EEC509D780
- Clave 2. E3F48B2326D641B57B0CF3EEC509D78**1**
- Clave 3. E3F48B2326D641**A**57B0CF3EEC509D780

Cifrado	Coeficiente de correlación
Clave 1 vs Clave 2	−0.037010732027248
Clave 1 vs Clave 3	0.063337173201966

Tabla 5.3: Sensibilidad a la clave secreta para cifrado.

5.11. Conclusiones

El algoritmo de cifrado caótico propuesto en este trabajo de tesis presenta excelentes resultados en seguridad. También, se mostró la alta eficiencia del algoritmo al generar criptogramas altamente desvinculados de la señal clara, es decir una correlación prácticamente nula y con una excelente sensibilidad a la clave secreta. Otra versión de la prueba anterior en la que la señal es desplazada k posiciones, muestra que no existen patrones periódicos o repetitivos, por lo tanto, el algoritmo es robusto para producir criptogramas sin periodicidad. Se demostró que para una señal clara

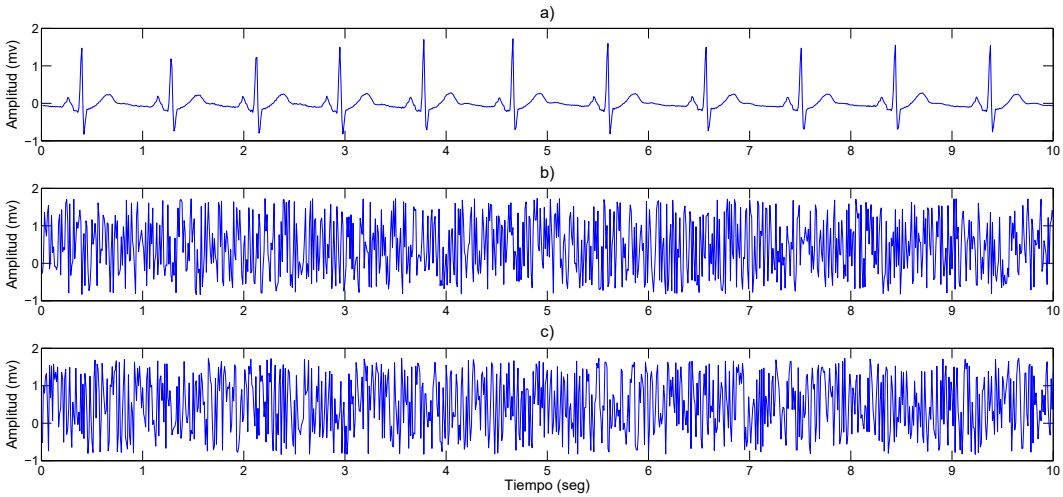

Figura 5.12: Señales de ECG descifradas con: **a)** Clave 1, **b)** Clave 2 y **c)** Clave 3.

(ECG de 60 segundos) de 1,000 elementos, en promedio solo el 19.3 % de sus valores son diferentes, mientras que para la señal cifrada es de 82.4 %, esto confirma lo antes mencionado el criptograma presenta altas capacidades de uniformidad, lo cual, indica una alta seguridad en el proceso de cifrado. Se determinó mediante histogramas, que los tres criptogramas generados a partir de cada una de las señales electrofisiológicas presentan una excelente uniformidad en comparación con las señales claras.

Se mostró la existencia de un proceso eficiente de cifrado, al generar 100 criptogramas diferentes siendo todos ellos un 99.6 % impredecibles. Finalmente, se comprobó la sensibilidad a pequeños cambios de la señal clara al tener dos criptogramas, donde uno tiene una pequeña variación en un dato y al repetir el procedimiento con 1,000 claves secretas seleccionadas aleatoriamente, se obtuvo que cada par de criptogramas son 100 % diferentes entre ellos con una magnitud promedio de 33.9 %.

Capítulo 6

Conclusiones

6.1. Conclusiones generales

En este trabajo de tesis de licenciatura, se diseñó e implementó un algoritmo de cifrado no convencional basado en caos digital y en la arquitectura de confusión-difusión. El algoritmo mostró ser eficiente, robusto y seguro para aplicaciones de telemedicina, particularmente en telemetría para la transmisión remota de forma segura de información médica de pacientes a médicos.

Se optó por emplear el mapa de Ushio de dos dimensiones en conjunto con la función exponencial y módulo 1. De esta manera, el sistema presentó una excelente aleatoriedad, una distribución más uniforme de los datos y un bajo tiempo de procesamiento. Además, con la clave secreta empleada de 128 bits se logró un espacio de clave de 2^{128} combinaciones posibles para resistir un ataque exhaustivo de fuerza bruta.

Al ser un algoritmo criptográfico no convencional, la complejidad de las operaciones aumenta, ya que al estar basado en ecuaciones diferenciales no lineales no existe una fórmula simple que defina al sistema caótico en cualquier punto dado, siendo un excelente beneficio ya que dificulta el criptoanálisis. También, al cambiar de posición y de valor a cada elemento (confusión y difusión) mediante la operación de mejoramiento de dinámicas caóticas, se logró modificar los valores de la señal clara eficientemente.

Se implementó el algoritmo criptográfico a nivel MatLab y se verificó mediante la adquisición de señales electrofisiológicas tomadas de la base de datos PhysioBank ATM disponible en internet.

En el análisis de seguridad, se logró obtener criptogramas altamente desvinculados de la señal clara (alta eficiencia) y con un porcentaje muy alto de imprevisibilidad, con nula existencia de patrones periódicos o repetitivos apto para obtener un algoritmo robusto capaz de producir criptogramas uniformes, gracias al alto porcentaje de valores diferentes presentes en el criptograma, lo que indica alta seguridad en el proceso de cifrado. Además, los criptogramas resultaron ser muy sensibles a pequeños cambios en la señal clara y clave secreta, ya que al hacer una mínima variación estos resultaron ser

100 % diferentes entre sí al compararlos a la par.

6.2. Trabajo a futuro

Como trabajo futuro de esta tesis se plantean las siguientes actividades:

- Implementación en sistema embebido de bajo costo: Comprobar el correcto funcionamiento del algoritmo en sistemas embebidos como microcontroladores, FPGA o Raspberry.
- Adquisición de señales en tiempo real: Obtener censado de las señales electrofisiológicas en tiempo real mediante la implementación de un sistema de monitoreo electrónico, de esta manera, los datos podrán ser recabados a partir de los pacientes en tiempo real.
- Multi-función: Modificar el algoritmo con el propósito de poder cifrar información de diferentes categorías, por ejemplo: texto, imágenes y video.
- Condiciones iniciales vs tiempo: Ver los resultados en tiempo mediante las condiciones iniciales, en este trabajo se implementaron condiciones aproximadamente igual a 0.5 pero al estar probando el mapa de Ushio hubo un resultado que mostró mejores resultados en aleatoriedad, esto se consigue con la modificación de las condiciones iniciales a $9.513709269685625 \times 10^{-4}$.
- Análisis de seguridad: Efectuar todos los análisis de seguridad posibles incluyendo los ya antes mencionados análisis físicos para implementaciones en sistemas digitales, como: monitoreo de consumo energético, fugas electromagnéticas, análisis de sonido o remanencia de datos y tiempos de cálculo.
- Interfaz gráfica: Elaborar una interfaz que facilite el uso del algoritmo a los usuarios, además, probarlo en otros lenguajes de programación. Por ejemplo el programa *Qt creator* que permite la creación de interfaces gráficas y tiene la propiedad de ser multiplataforma, además de contar con módulos para otros lenguajes (trabaja con C++), por ejemplo, Python.

Bibliografía

[1] Casali A., Deco C. y Beltramone S. (2016). An assistant to populate repositories: Gathering educational digital objects and metadata extraction. *IEEE Revista Iberoamericana de Tecnologias Del Apendizaje*, **11**(2): 87-94.

[2] Wu Y. y Cao G. (2017). VideoMec: A metadata-enhanced crowdsourcing system for mobile videos. *ACM/IEEE International Conference on Information Processing in Sensor Networks*, Pittsburgh, PA USA, 143-154.

[3] Al-Barhamtoshy H., Khemakhem M., Jambi K., Essa F., Fattouh A. y Al-Ghandi A. (2016). Universal metadata repository for document analysis and recognition. *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, 1-6.

[4] Pottayya R.M., Lapayre J-C. y Garcia E. (2017). An adaptative videoconferencing framework for collaborative telemedicine. *IEEE International Conference on Advanced Information Networking and Applications*, Tapei Taiwan, 197-204.

[5] Murillo-Escobar M.A., Abundiz-Pérez F., Cruz-Hernández C. y López-Gutiérrez R.M. (2014). A novel symmetric text encryption algorithm based on logistic map. *Proceedings of the International Conference on Communications, Signal Processing and Computers*, Interlaken, Suiza, 49-53.

[6] Murillo-Escobar M.A. (2015). Diseño de un algoritmo de cifrado caótico y su implementación en microcontrolador para aplicaciones embebidas. *UABC, Tesis de Doctorado en Ciencias en Eléctrica*, 1-142.

[7] Addison S.R y Gray J.E. (2006). Chaos and encryption: Problems and potential. *IEEE Proceeedings of the 38th Southeastern Sypmposium on System Theory*, Tennessee Technological University Cookevile, TN, USA, 275-279.

[8] Qi T., Jun-min J. y Jun-Li J. (2016). An image encryption algorithm based on high-dimensional chaotic systems. *International Conference on Signal Processing, Communications and Computing (ICSPCC)*, Hong Kong, 1-4.

[9] Sharma M. y Bhargava A. (2016). Chaos based image encryption using two step iterated logistic map. *IEEE Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Jaipur, India, 1-5.

[10] Guillén-Pinto E.P., Ramírez.López L.J. y Estupiñán-Cuesta E.P. (2011). Análsis de seguridad para el manejo de la información médica en telemedicina. *Ciencia e Ingeniería Neogranadina*, **21**(2): 57-89.

[11] Biblioteca Nacional de Medicina de los EE.UU. (2016). Electrocardiograma. https://medlineplus.gov/spanish/ency/article/003868.htm (2017-10-01).

[12] Biblioteca Nacional de Medicina de los EE.UU. (2016). Electroencefalograma. https://medlineplus.gov/spanish/ency/article/003931.htm (2017-10-01).

[13] Diabetes al Dia. (2016). Examen para chequear hipertensión arterial o presión de la sangre. www.diabetesaldia.com/chequeo-de-la-presion-de-la-sangre-2/ (2017-10-05).

[14] Kopec-Poliszuk A. y Salazar-Gómez A.J. (2006). Aplicaciones de telecomunicaciones en salud en la subregión andina: Telemedicina. *Lima: Organismo Andino de Salud*, 2da. Ed., 1-260.

[15] PROY-NOM-036-SSA3-2015. Diario Oficial de la Federación de México, D.F., 21 de diciembre de 2015.

[16] NOM-024-SSA3-2012. Diario Oficial de la Federación de México, D.F., 30 de noviembre de 2012.

[17] Castellano N.N., Gázquez J.A., García R.M., Gracia-Escudero A., Fernández-Ros M. y Manzano-Agugliaro F. (2015). Design of a real-time emergency telemedicine system for remote medical diagnosis. *Biosystems Engineering*, **138**: 23-32.

[18] Acevedo P.C. (2009). Einthoven y el electrocardiograma. *Revista del Hospital Italiano de Buenos Aires*, **29**(1): 42-44.

[19] Lama T.A.(2004). Einthoven. El hombre y su invento. *Rev Méd Chile*, **132**: 260-264.

[20] Murillo-Escobar M.A., Cardoza-Avendaño L., López-Gutiérrez R.M. y Cruz-Hernández C. A double chaotic layer encryption algorithm for clinical signals in telmedicine. *Journal of Medical Systems*, **41**(4): 1-17.

[21] Alligood K.T., Sauer T.D. y Yorke J.A. (1996). Chaos an introduction to dynamical systems. *Ed. Springer Verlag New York*, 1-603.

[22] Oestreicher C.(2007). A history of chaos theory. *Dialogues in Clinical Neuroscience*, **9**(3): 279-289.

[23] Lorenz E.N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, **20**(2): 130-141.

[24] Estorninho-Meador C.E. (2011). Numerical calculation of Lyapunov exponents for three-dimensional systems of ordinary differential equations. *College of Marshall University*, 1-78.

[25] May R.M. (1976). Simple mathematical models with very complicated dynamics. *Nature*, **261**(5560): 459-467.

[26] Hénon M.(1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, **50**(1): 69-76.

[27] Wen H.(2014). A review of the Hénon map and its physical interpretations. *School of Physics Georgia Institute of Technology*, Atlanta, GA, 30332-0430, 1-9.

[28] Susanto A.(2016). Stream cipher algorithm with Ikeda map trajectories. *IEEE Data and Software Engineering (ICoDSE), 2016 International Conference*, Denpasar, Indonesia, 1-6.

[29] Aboites V., Barmenkov Y., Kiryanov A. y Wilson M.(2014). Bidimensional dynamic maps in optical resonators. *Revista Mexicana de Física*, **60**: 13-23.

[30] Ushio T. (1995). Chaotic synchronization and controlling chaos based on contraction mapping. *Physics Letters A*, **198**(1): 14-22.

[31] Yamamoto S., Hino T. y Ushio T.(2001). Dynamic delayed feedback controllers for chaotic discrete-time systems. *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, **48**(6): 785-789.

[32] Jiang G.P. y Zheng W.X. (2005). A simple method of chaos control for a class of chaotic discrete-time systems. *Chaos, Solitons Fractals*, **23**: 843-849.

[33] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J. y Vo S. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. *National Institute of Standards and Technology Special Publication 800-22*, 1-131.

[34] Gómez-Urgelles J. (2010). Matemáticos, espías y piratas informáticos: Codificación y criptografía. ¿Cuán segura es la información? *Ed EDITEC*, 1-144.

[35] UNAM Facultad de Ingeniería (2012). Historia de la Criptografía. http://redyseguridad.fi-p.unam.mx/proyectos/criptografía/index.php/1-panorama-general/12-historia-de-la-criptografia (2017-08-15).

[36] Smart N. (2002). Cryptography: An introduction. The Enigma machine. *Ed. McGraw Hill*, 3ra Ed., 1-419.

[37] Shannon C.E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, **27**(3): 379-423.

[38] Shannon C.E. (1949). Communication theory of secrecy systems. *Nokia Bell Labs Journal*, **28**(4): 656-715.

[39] Granados G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, **7**(7): 1-17.

[40] Alvarez G. y Li S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, **16**(8):2129-2151.

[41] Li S., Alvarez G., Li Z. y Halang W.A. (2007). Analog chaos-based secure comunications and cryptanalysis: a brief survey. *PhysCon*, arXiv:0710.5455v1.

[42] Secretaría de Agricultura, Ganadería, Desarrollo rural, Pesca y Alimentación (SAGARPA). (2016). ¿Sabes que es la telemetría?. www.sagarpa.gob.mx/Delegaciones/veracruz/boletines/Paginas/2016B050.aspx (2017-10-04).

[43] Chen C.K., Lin C.L., Chiang C.T. y Lin S.L. (2012). Personalized information encryption using ECG signals with chaotic functions. *Information Sciences*, **193**: 125-140.

[44] Ahmad M., Farooq O., Datta S., Sohail S.S., Vyas A.L. y Mulvaney D. (2011). Chaos-based encryption of biomedical EEG signals using random quantization technique. *4th International Conference on Biomedical Engineering and Informatics (BMEI)*, 1471-1475.

[45] Raeiatibanadkooki M., Quchani S.R., KhalilZade M. y Bahaadinbeigy K. (2016). Compression and encryption of ECG signals using wavelet and chaotically huffman code in telemedicine application. *Journal of Medical Systems*, **40**(3): 1-8.

[46] Lin C.F. (2016). Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals. *Journal of Medical Systems*, **40**(3): 1-10.

[47] Kenfack G. y Tiedeu A. (2014). Chaos-based encryption of ECG signals: experimental reuslts. *Journal of Biomedical Science and Engineering*, **7**: 368-379.

[48] Lin C.F., Shih S.H. y Zhu J.D. (2014). Chaos based encryption system for encrypting electroencephalogram signals. *Journal of Medical Systems*, **38**(5): 1-10.

[49] Kotulsk Z. y Szczepañski J. (1997). Discrete chaotic cryptography. *Proc. NEEDS 1997*, 1-11.