UNIVERSIDAD POLITÉCNICA DE TULANCINGO

“Fortalecimiento de la ciberseguridad en sistemas de medición de energía eléctrica en el escenario de la red inteligente (SG) dentro de la IoT”

T E S I S

Q U E P A R A O B T E N E R E L G R A D O DE:

DOCTOR EN OPTOMECATRÓNICA

P R E S E N T A:
Maestra Francisca Angélica Elizalde Canales

ASESOR:
Dr. Iván de Jesús Rivas Cambero

AGRADECIMIENTO AL CONACYT POR EL APOYO BRINDADO COMO BECARIO CVU/Becario: 458655 /408093

Tulancingo Hidalgo, Noviembre 2019

AGRADECIMIENTOS: A todos y cada uno de los que creyeron en mí y estuvieron trabajando junto conmigo para lograr este propósito.

Contenido

Lista de Figuras

Lista de Tablas

RESUMEN

La industria de la energía eléctrica se ha vuelto cada vez más vulnerable debido al crecimiento de la red inteligente que se utiliza para la interconexión de los consumidores con las tecnologías de información, transmisión y distribución de energía basadas en sistemas de comunicación. En este sentido, los medidores inteligentes podrían proporcionar inadvertidamente acceso no autorizado a los datos del consumidor, lo cual es una preocupación en la gestión de la información para la adopción de redes inteligentes ante la posibilidad cada vez mayor de ataques cibernéticos.

Recientemente, se han introducido varios esfuerzos de investigación para superar los desafíos y encontrar soluciones apropiadas asociadas con la seguridad, especialmente la seguridad de extremo a extremo. En la preservación de la privacidad, los planes han avanzado significativamente en los últimos años, la investigación se ha centrado en crear mecanismos de seguridad adecuados para el contexto de dispositivos de medida; sin embargo, las necesidades son variadas y en aumento.

El cifrado de información en sistemas de comunicaciones inalámbricas vulnerables es un factor importante en la prevención de ciberataques. En esta tesis se presenta el diseño, desarrollo, implementación y evaluación de un algoritmo de cifrado, a través de clave simétrica que cifra los datos mediante la aplicación de generadores eficientes de secuencias pseudoaleatorias que simulan comportamiento caótico a través de los métodos de mapeo logístico y Skew-

Bernoulli Map. El objetivo del proyecto es a través de los métodos generar secuencias impredecibles para crear un flujo de claves aplicadas al cifrado/descifrado de una señal de consumo de energía eléctrica, con el fin de fortalecer la privacidad y confidencialidad de los datos de medición en redes eléctricas inteligentes.

El fortalecimiento de la seguridad para preservar la privacidad contra ataques no autorizados es el principal objetivo que guía este trabajo, sin embargo, para todas las aplicaciones prácticas, el rendimiento y el costo de implementación también son factores a tener en cuenta.

Se realizan pruebas experimentales utilizando una señal de consumo de energía eléctrica simulada, y una señal fuera de línea; los resultados obtenidos evidencian que el proceso de cifrado/descifrado no afectará la eficiencia de codificación, manteniendo una tasa de bits y un bajo consumo de recursos computacionales. Para validar el algoritmo se somete a un análisis de seguridad basado en valoración estadística del NIST (Instituto Nacional de Normas y Tecnología), cuyas pruebas son satisfactorias, lo que indica, que el algoritmo ofrece alta eficiencia de seguridad criptográfica. Para complementar la evaluación de los datos cifrados, se cifra la imagen de Lena y sus métricas se comparan con las reportadas en la literatura, lo que arroja resultados útiles en seguridad y rendimiento.

Abstract

The electric power industry has become increasingly vulnerable due to the growth of the smart grid that is used for the interconnection of users with information technologies, transmission and distribution of energy based communication systems. In this sense, smart meters could inadvertently provide unauthorized access to consumer data, which is a concern in the management of information for the adoption of intelligent networks in the face of the increasing possibility of cyber-attacks.

Recently, several research efforts have been introduced to overcome the challenges and find appropriate solutions associated with security, especially end-to-end security. In the preservation of privacy, the plans have advanced significantly in recent years, research has focused on creating adequate security mechanisms for the context of measurement devices; however, the needs are varied and increasing.

Encryption of information in vulnerable wireless communication systems is an important factor in the prevention of cyber-attacks. This work presents the design, development, implementation and evaluation of an encryption algorithm, using a symmetric key that encrypts the data through the application of efficient generators of pseudo-random sequences that simulate chaotic behavior through logistic mapping methods. Skew-Bernoulli Map. The aim of the project is through the methods to generate unpredictable sequences to create a flow of keys applied to the encryption / decryption of an electric power consumption signal, in order to strengthen the privacy and confidentiality of the measurement data in electrical networks smart

The strengthening of security to preserve privacy against unauthorized attacks is the main objective that guides this work, however, for all practical applications, the performance and the cost of implementation are also factors to be taken into account.

Experimental tests are performed using a simulated power consumption signal, and an off-line signal; the results obtained show that the encryption / decryption process will not affect the coding efficiency, maintaining a bit rate and a low consumption of computational resources. To validate the algorithm, it is subjected to a security analysis based on statistical evaluation of the NIST (National Institute of Standards and Technology), whose tests are satisfactory, which indicates that the algorithm offers high cryptographic security efficiency. To complement the evaluation of the encrypted data, the image of Lena is encrypted and its metrics are compared with those reported in the literature, which yields useful results in safety and performance.

CAPÍTULO I

INTRODUCCIÓN

Internet de las cosas (IoT del inglés Internet of Things) es la evolución de nuestra etapa actual de comunicación, donde cualquier objeto / cosa física equipado con capacidades de cálculo y de comunicación podría integrarse fácilmente, a Internet. La red inteligente (SG del inglés Sart Grid), que se considera como una de las infraestructuras más críticas, se define como la red de energía clásica aumentada con las tecnologías de información y comunicación (TIC de las ingles Tecnologic information and comnunications) a gran escala. La red inteligente, implicará miles de millones de objetos inteligentes con sensores, actuadores, además de varias infraestructuras de comunicación ya sea pública o privado, donde la seguridad puede ser visto como uno de los factores principales que obstaculizan la adopción rápida a gran escala y el despliegue tanto del internet de las cosas como de la red inteligente [1].

La electrónica fue la que propició tal desarrollo al incrementar las capacidades de procesamiento, almacenamiento y transmisión de información, y diariamente se producen incrementos de estas capacidades. Este crecimiento en las características de los equipos computacionales ayudó al desarrollo de incontables campos del conocimiento, pero también se evidenciaron muchos inconvenientes de la era de la información, siendo la seguridad uno de los más apremiantes. En el contexto de la energía eléctrica, la medición inteligente puede aportar grandes beneficios, como la posibilidad de devolver información al consumidor acerca de su consumo energético, con lo que este puede contribuir hacia una mayor conciencia sobre el uso eficiente de energía, potenciales ahorros energéticos y progresos al

preservar el medio ambiente, sin embargo, la información sensible se vuelve un imperativo de resguardar [2].

Es indispensable utilizar mecanismos que permitan resguardar la información de algún ataque cibernético, siendo uno de los más utilizados la criptografía que se encarga de ocultar los datos ante terceros, proporcionando confidencialidad mediante un método de cifrado. La teoría del caos, ha encontrado bastante aceptación en el área de la criptografía siendo una alternativa en la búsqueda de la seguridad de la información. En este trabajo se presenta la realización de un algoritmo de cifrado cuya función es la transformación de los datos

1.1. Planteamiento del Problema

Smart Grid surge con el objetivo de mejorar la eficiencia y la fiabilidad de la red de energía eléctrica, adaptándola a las necesidades actuales y garantizando la disminución de emisiones de CO_2, la reducción de costos y la integración satisfactoria de energía renovables. La industria eléctrica está decidida a transformar la red centralizada actual y para ello se ha tomado como inspiración el modelo de Internet, donde el control y la toma de decisiones están distribuidos a través de nodos dispersos a lo largo del sistema, y la información circula de forma bidireccional [3].

La situación actual muestra un futuro desabasto de energía eléctrica y se propone como solución la concientización del consumidor ante el incremento del consumo permitiéndole controlar el gasto energético, específicamente con la penetración de medidores inteligentes que lean y trasmitan los datos de consumo. Sin embargo, al estar interconectada la red de energía eléctrica a las redes de comunicación e información se ha manifestado que existe un riesgo latente de intrusión malintencionada con el fin de hacer uso inadecuado de los datos que se generan y transmiten a través de los medidores inteligentes. Debido a deficiencias en la seguridad palpables en los dispositivos de medición que los hace susceptibles de ataques maliciosos; se vuelve un deber el garantizar que los datos sensibles se mantengan privados. No obstante, actualmente se están desarrollando constantemente sistemas de seguridad para redes de datos convencionales, sin

embargo, aún no están orientadas para brindar el adecuado blindaje para los servicios que pueden ofertar las redes eléctricas inteligentes [4].

Los esquemas de preservación de la privacidad han avanzado significativamente en los últimos años, especialmente debido a la necesidad de comunicación de datos. Algunas investigaciones se han centrado en crear mecanismos de seguridad adecuados para el contexto de los dispositivos de medición inteligentes; Sin embargo, las necesidades son variadas y en aumento. Además, la privacidad cotidiana está expuesta a las intrusiones de quienes tienen propósitos maliciosos y poseen el conocimiento suficiente para encontrar datos confidenciales.

En investigaciones recientes, se han presentado varios mecanismos criptográficos para fortalecer la seguridad en los dispositivos de medición y las redes eléctricas inteligentes, sin embargo, los resultados obtenidos en [4] muestran la necesidad de nuevos esquemas para reducir la complejidad y los recursos computacionales. De esta manera, una de las fortalezas de este trabajo es la implementación de un algoritmo de "ofuscación de datos" en un sistema integrado de bajos recursos computacionales.

Por lo tanto, en este trabajo, se propone un nuevo algoritmo basado en un generador de bits pseudoaleatorio que utiliza semilla caótica. Se prueba la efectividad de la implementación del algoritmo de cifrado, combinando dos técnicas, mapa logístico y generador congruencial, para analizar la compensación entre recursos y seguridad. El fortalecimiento de la seguridad para preservar la privacidad contra ciber-ataques no pretende abarcar toda la información susceptible de ser transmitida, sino fortalecer la seguridad en los dispositivos y sistemas de medición para mitigar las amenazas y con ello atenuar los riesgos asociados. Por ello, en esta tesis se presenta el diseño, desarrollo, implementación y evaluación de un algoritmo de cifrado, a través de clave simétrica que cifra los datos de consumo de energía eléctrica mediante la aplicación de generadores eficientes de secuencias pseudoaleatorias que simulan comportamiento caótico a través de los métodos de mapeo logístico y Skew-Bernoulli Map.

1.2. Objetivos

A partir de un análisis global sobre las amenazas y vulnerabilidad de los sistemas de medición de energía eléctrica en redes de suministro inteligente, y de las normas nacionales o internacionales en materia de seguridad de la información, se propone diseño, desarrollo e implementación tecnológica que genere un sistema hardware-software basado en un algoritmo criptográfico para la protección de la medición del consumo de energía eléctrica en zonas habitacionales. (Implementar el prototipo de un sistema con plataformas Arduino Uno para cifrar y descifrar datos de consumo de energía eléctrica).

Objetivos específicos:

- Analizar las amenazas, vulnerabilidades y ataques de seguridad en la arquitectura de medición avanzada (AMI).
- Desarrollar e implementar algoritmo de cifrado por software, para fortalecer la seguridad y privacidad de los datos de medición.
- Diseñar y construir prototipo medidor de consumo de energía eléctrica.
- Un artículo de investigación científica o desarrollo tecnológico publicado en una revista internacional de arbitraje estricto.

1.3. Justificación

En las últimas décadas ha surgido como una nueva corriente para la protección de información la Teoría del Caos. Partiendo del principio de Kerckhoff, en donde se establece que la robustez de un sistema de seguridad criptográfica reside en la dificultad para obtener la clave, entonces los métodos de generación de claves deben poseer ciertas propiedades de aleatoriedad. La Teoría del Caos se ha extendido en usos y aplicaciones a muchas ramas de la ciencia y ha sido una alternativa en la búsqueda de la seguridad de la información. Esta teoría ha encontrado bastante aceptación en al área de la criptografía; particularmente, en los procesos de cifrado de flujo y por bloques [5], [6]. Un campo importante de la Teoría del Caos es el que tiene que ver con las transformaciones caóticas unidimensionales como la transformación de Bernoulli [7], la transformación Logística [8] y la transformación Tent [9]. El campo de la investigación en seguridad informática requiere de explorar la teoría del caos, para mejorar los procesos que

atiendan la problemática de confiabilidad, disponibilidad y privacidad de los datos administrados por los diferentes medios de comunicación, por lo que se busca fortalecer la seguridad en los dispositivos de medición para mitigar las amenazas y con ello atenuar los riesgos asociados. El proceso de cifrado utiliza únicamente operaciones con bytes que pueden ser fácilmente implementadas en cualquier tipo de procesadores y hardware ligero, manteniendo un equilibrio entre seguridad y consumo de recursos computacionales.

1.4. Alcance

El trabajo de grado abarcará el diseño, desarrollo, implementación y evaluación de un algoritmo de cifrado, basado en semilla caótica sobre datos de consumo de energía eléctrica; con el fin de enmascarar los datos aplicando los métodos de Skew Bernoulli y mapeo logístico apremiando bajos requerimientos computacionales y recursos tecnológicos.

1.5. Organización del documento

El siguiente trabajo está conformado de los siguientes capítulos.

En el capítulo 1, se presenta el planteamiento de la investigación, el objetivo, así como la justificación y los alcances.

En el capítulo 2, se hace un vasto recorrido por la literatura que estudia el campo de investigación de interés.

En el capítulo 3, se realiza una introducción sobre aspectos teóricos de las vulnerabilidades de los sistemas de medición de energía eléctrica.

El capítulo 4, se realiza un extracto de los métodos estudiados para la propuesta del criptosistema.

El capítulo 5, se diseña prototipo para pruebas experimentales e implementación física del criptosistema.

El Capítulo 6, muestra los resultados obtenidos de la investigación, las pruebas realizadas cifrando y descifrando varios tipos de datos centrándonos en el consumo de energía eléctrica.

1.6. Referencias

[1]. PS Shenil, Boby George, "Un digitalizador eficiente para la medición no intrusiva de voltaje de CA", Conferencia de Tecnología de Instrumentación y Medición (I2MTC) 2017 IEEE International, pp. 1-6, 2017.

[2]. Ching-Han Chen, Ching-Yi Chen, Chih-Hsien Hsia, Guan-Xin Wu, "Efficient Vision-based Smart Meter Reading Network", International Journal of Web Services Research, vol. 14, pp. 44, 2017.

[3]. S. Sofana Reka, Tomislav Dragicevic, "Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid", Renewable and Sustainable Energy Reviews, vol. 91, pp. 90, 2018.

[4]. S. Desai, R. Alhadad, N. Chilamkurti and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure", Cluster Computing, 2018

[5]. R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption", Optics & Laser Technology, vol. 101, pp. 30-41, 2018.

[6]. C. Li, G. Luo, K. Qin and C. Li, "An image encryption scheme based on chaotic tent map", Nonlinear Dynamics, vol. 87, no. 1, pp. 127-133, 2016

[7]. I. Chun-hu & LUO, Guang-chun & QIN, Ke & Li, Chunhu. “A Novel Image Encryption Algorithm Based on Bernoulli Maps.” DEStech Transactions on Computer Science and Engineering. 2017

[8]. WU XIAOLIN, BIN ZHU, YUTONG HU, AND YAMEI RAN.A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps vol. 5, pp. 6429- 6436, 2017

[9]. Chanil Pakbc Lilian Huanga. “A new color image encryption using combination of the 1D chaotic map”. Signal Processing, Vol. 138, pp. 129-137, 2017.

CAPÍTULO II

ANTECEDENTES

Internet de las cosas (IoT) es concepto reciente, en el cual Internet evoluciona de unir máquinas y personas hacia la conexión de objetos/cosas inteligentes. Así, es posible decir que las comunicaciones de Internet de las cosas son la evolución de comunicaciones de máquina a máquina (M2M). Según Cisco, hacia 2020 habrá más de 50 mil millones de objetos relacionados contra una población de 7 billones. Un objeto puede ser cualquier cosa/dispositivo/entidad equipada con cálculo, almacenaje y capacidades de comunicación diferentes (sensores, actuadores, teléfono móvil, computadora personal, portátil, impresora, automóvil, refrigerador, microondas) [1].

La red inteligente, también se conoce como la futura red que trata de una mejora de la red de energía eléctrica convencional, mediante la integración de tecnologías de computación y de comunicación digital para proporcionar una entrega segura, eficiente y confiable de la electricidad y el intercambio de información entre los generadores de energía, empresas de servicios y consumidores de la energía eléctrica. Ofrece la Inclusión de consumidores admitiendo información y opciones interactivas, lo que permite a los consumidores seleccionar una tarifa adecuada disponible y en consecuencia controlar su consumo de energía. De esta manera, los consumidores pueden hacer una mejor administración del recurso [2].

La red inteligente, es una infraestructura de energía eléctrica con capacidades intuitivas al permitir que los proveedores, distribuidores y consumidores de energía mantener los requerimientos de operación y capacidades en tiempo cuasi real [3].

En la red eléctrica, una serie de dispositivos como sensores, medidores y sistemas de control permanecen en el camino entre proveedores y consumidores de energía para facilitar la comunicación bilateral. En la red los consumidores poseen dispositivos de medición, por lo que son capaces de identificar el consumo de energía, porque estos medidores acumulan la información de consumo eléctrico, que a su vez se encuentra acumulada por la compañía de servicios públicos, para fines de seguimiento y facturación. Los consumidores también pueden tener acceso a su medidor para comprobar su nivel de consumo y ajustar en consecuencia la utilización de la energía. Para este propósito el dispositivo de medición envía mensajes al proveedor de servicios periódicamente para ajustar su utilización de la energía y participar activamente de la energía dentro de la red [4].

Los proveedores del servicio pueden enviar adicionalmente algunas ofertas especiales mediante el envío de mensajes a los medidores, por lo que los consumidores pueden ajustar su utilización en consecuencia. Durante las horas pico, si todos los dispositivos se conectan y la red de energía se percata de una situación de emergencia, entonces el proveedor del servicio envía mensajes a todos los consumidores mediante la utilización de sus dispositivos de medición para notificar acerca de eventos de emergencia o para ajustar el nivel de consumo [5].

Los medidores de consumo y los objetos inteligentes (es decir, calentador, lavavajillas, lavadora, aire acondicionado, televisión, etc.) deben tener una dirección IP única para el apoyo a la comunicación y estándares de IETF (Internet Engineering Task Force) para la gestión remota de dispositivos situados en diferentes lugares [6]. Mientras los objetos están conectados a través de aplicaciones (Zigbee, HART/ Wireless Hart, Z-Wave, etc.) y en una pequeña escala; Internet de las cosas pretende conectarlos a gran escala utilizando soluciones basadas en IP (IP, TCP/UDP, etc.), directamente para permitir interactuar con cualquier otro dispositivo a través de Internet.

La red de energía eléctrica, podría considerarse como la mayor instancia de red de internet de las cosas en el futuro próximo. Toda la red eléctrica desde la planta de generación de la energía eléctrica hasta los consumidores finales de electricidad (casas, edificios, fábricas, alumbrado público, vehículos eléctricos,

dispositivos, etc.), incluidos las redes de transmisión y distribución de energía, serán dotadas con inteligencia y comunicación bidireccional, además de capacidad para monitorear y controlar la red eléctrica desde cualquier lugar y con un alto nivel de precisión [7]. El objetivo de la red de energía eléctrica es mantener en tiempo real un equilibrio entre la generación de energía y consumo, permitiendo vigilancia y control de la cadena de suministro de energía, gracias a la comunicación bidireccional (medidores, sensores y actuadores).

Si bien el uso de Internet de las cosas es muy prominente en el contexto de la red de energía eléctrica inteligente, también podría conducir a desastres. Siendo la infraestructura de la red más atractiva para los ciberataques. Consecuencia de ello, un atacante podría provocar pérdidas financieras y afectar los activos de proveedores de energía eléctrica por romper en tiempo real el equilibrio entre el consumo de energía y producción, mediante la manipulación de los datos generados por objetos inteligentes [8].

2.1 Importancia de la seguridad en la red

Todas las redes inalámbricas son inherentemente inseguras. Lo mismo es en el caso de red inteligente, como la comunicación es bidireccional entre los diferentes componentes y es basado en IP mediante el cual los atacantes pueden explorar fácilmente la red [3], [9]. Los consumidores están equipados con dispositivos de medición, que acumulan la información de consumo de los clientes de energía eléctrica y estos a su vez envían esta información al proveedor de servicio para fines de seguimiento y facturación. Por lo que la seguridad de los medidores debiera ser eficiente, garantizar que ningún atacante puede modificar fácilmente la información crítica, como la utilización de energía, que conduce hacia la facturación errónea.

Se tienen evidencias que el sistema de energía de Estados Unidos, ha tenido pérdidas estimadas en $ 6 millones de dólares por robo de energía [3], [10]. Por lo que en el marco de comunicación se deben considerar mecanismos eficaces para que los atacantes no puedan comprometer la confidencialidad o privacidad de la información que se intercambia entre los consumidores y los proveedores del servicio de energía eléctrica [11].

La infraestructura de red inteligente es de la naturaleza de recursos limitados, por lo que, con el fin de abordar los requerimientos de seguridad de los medidores inteligentes y dadas las características de estos, se determina que deben ser ligeros, sin problemas de escalabilidad, es decir, con la posibilidad de que varias solicitudes se procesen al mismo tiempo y sin incrementar la latencia de la comunicación y generar retraso en el suministro servicio a los consumidores [12], [13]

2.2 Problemas de seguridad

Como un cyber-sistema físico, el internet de las cosas basado en la red de energía eléctrica inteligente se enfrentará a varios problemas de seguridad [14]:

• La suplantación de identidad: Este ataque pretende comunicar en nombre de un legítimo objeto en un modo no autorizado, haciendo uso de su identidad. Un atacante puede falsificar la identidad de algún dispositivo de medición inteligente, y hacer pagar por su consumo de energía.

• Espionaje: desde objetos/dispositivos en el internet de las cosas basado la red inteligente que se comunican utilizando a menudo la infraestructura de comunicación pública, un atacante puede fácilmente tener acceso a sus datos y obtener el consumo energía entre otros datos.

• La manipulación de datos: Un atacante puede modificar los datos que se intercambian, tales como tarifas en periodos pico, y pasarlos a precios más bajos. Como consecuencia, esto podría hacer que los consumidores aumentaran su consumo, en lugar de reducirlos, resultando una sobrecarga a la red eléctrica.

• Autorización y control de los problemas de acceso: desde varios dispositivos podrían ser monitoreados y configurados de forma remota, medidores inteligentes, sensores y actuadores y subestaciones, donde un atacante o incluso un empleado molesto, podría intentar obtener un acceso no autorizado, para manipularlos, provocando daños físicos que conduzcan a cortes de energía.

• Problema de privacidad: Medidores inteligentes y dispositivos inteligentes, podrían revelar más sobre el consumo de la energía generados y demás datos sensibles que podrían dañar la privacidad del usuario final, mediante la divulgación de información sobre sus hábitos, si están dentro o fuera de casa o negocio, si se encuentran laborando o en vacaciones, etc.

• Código malicioso: desde objetos de la red inteligente a través de computó y comunicación habilitados, se puede comprometer de forma física o remota. Ejecutando diferentes tipos de software, que pudieran ser objeto de otro tipo de software infeccioso o código malicioso enfocándose a medidores inteligentes o dispositivos inteligentes; además, desplegaron el código masivamente.

• Disponibilidad y direccionalidad: en la clásica red de energía, es muy difícil focalizar la disponibilidad de activos (medidores de electricidad, subestaciones, etc.), especialmente en gran escala. En la red inteligente, las Tecnologías de la comunicación e información serán de vital importancia para intercomunicación de los activos de la red eléctrica, haciendo así posible la indisponibilidad total sobre el ataque de denegación de servicio.

• Cyber-ataque: La red inteligente podría ser vista como el mayor sistema ciber- físico CPS (del inglés, Cyber-Physical-System), involucrando sistemas físicos; en representación de los activos físicos de la red inteligente (transformadores, medidores inteligentes, cables, etc.) y sistemas de tecnologías de comunicación en información, donde los elementos de tecnología de información y comunicación controlan y administran entidades físicas. Ahora, un cyber-ataque podría dañar los activos los físicos - como fue el caso con el ataque Stuxnet [15], que era difícil que pudiera darse en la clásica red eléctrica.

2.3 Desafíos de seguridad

Cuando se trabaja con algoritmos de seguridad, protocolos y políticas para internet de las cosas, la red de energía eléctrica inteligente enfrenta desafíos que deben tenerse en cuenta [16]:

• Escalabilidad: La red podría abarcar áreas grandes (varias ciudades o todo el país), e involucra a un gran número de dispositivos inteligentes y objetos. Esto hará difícil concebir las soluciones de seguridad escalables, como llaves de autenticación y gestión.

• Movilidad: con dispositivos móviles/objetos, habrá una continua necesidad de autenticación y comunicación segura con medidores inteligentes y estaciones.

• Implementación: La red podría abarcar a todo el país, los objetos/dispositivos estarán desplegados a gran escala, y podrían ser colocados en lugares remotos sin perímetro de protección físico, haciendo fácil el acceso por tanto las soluciones de seguridad deben ser capaces de detectar cualquier intento de intrusión en ellos.

• Sistemas heredados: En sistemas y dispositivos implementados, podría existir poca seguridad, ya que se crean principalmente como soluciones propietarias (hardware y software), aisladas de comunicación, o con infraestructura de comunicaciones privadas. La integración de estos sistemas heredados a internet de las cosas basadas en redes inteligentes es un verdadero desafío, ya que en la mayoría de los casos no hay manera de sustituirlos con nuevos sistemas o actualizarlos.

• Recursos limitados: varios dispositivos/objetos de la red, especialmente aquellos desplegados masivamente poseen recursos limitados. Se deben tomar en cuenta cuidados especiales a la hora de desarrollar soluciones de seguridad, para asegurarse de que sus limitados recursos puedan adaptarse a las soluciones. Esto hace un reto a la aplicación clásica de seguridad basada en la criptografía de clave pública (PKI).

• Heterogeneidad: Debido a la discrepancia sobre los recursos de los dispositivos/objetos de la red inteligente (memoria, cálculo, ancho de banda, autonomía energética, sensibilidad, etc.), y sus protocolos de comunicación implementados consiguiendo seguridad de extremo a extremo de la comunicación es una tarea ardua, que exige en su mayoría la adaptación de soluciones existentes o incluso mediante puertas de enlaces.

• Interoperabilidad: podría ser visto como una de las consecuencias de los protocolos de comunicación y la heterogeneidad entre los dispositivos/objetos en el SG. Sistemas heredados y dispositivos/objetos que no soportan los protocolos TCP/IP (Zigbee v1, HART) no podrían comunicarse con dispositivos/objetos y sistemas basados en IP, salvo a través de puertas de enlace, haciendo imposible la seguridad en la comunicación de extremo a extremo.

• Bootstrapping: Cómo un eficientemente arranque de los millones de dispositivos/objetos de la red inteligente estos deben poseer elementos necesarios (claves criptográficas, funciones criptográficas y algoritmos y parámetros).

• Administración de confianza: objetos/dispositivos de la red inteligente podría ser administrados por entidades diferentes (usuarios finales de electrodomésticos inteligentes, operadores para medidores inteligentes y sensores).

Los Objetos/dispositivos no deberán tener la posibilidad de comunicarse sin un mínimo nivel de confianza establecida. Él fomento de la confianza entre los dispositivos en propiedad o administrados por entidades diferentes es un desafío, especialmente en una red a gran. Por tanto resulta imprescindible implementar mecanismos de seguridad que permitan resguardar los datos sensibles ante algún ciberataque, dado el avance tecnológico que ha propiciado el incremento del uso sistemas de información, lo que ha generado vulnerabilidad a ataques cibernéticos, siendo la criptografía uno de los mecanismos de protección más utilizados en este ámbito, debido a que se encarga de ocultar los datos ante terceros, proporcionando confidencialidad mediante algún método de cifrado [17].

La criptografía ha sido aplicada en varios sectores críticos donde se requiere reforzar la seguridad cibernética, un ejemplo es el sector de la energía eléctrica, que se vuelve cada vez más vulnerable debido a que, en una red eléctrica inteligente además de la conexión con generación, transmisión y distribución, también se incluyen a los consumidores, todos ellos interconectados bajo las tecnologías de la comunicación y la información, proporcionada esta interacción por medio de medidores inteligentes que podrían exhibir accesos no autorizados a la privacidad del consumidor, lo que se convierte en una preocupación en el manejo de información para adopción de redes inteligentes ante la posibilidad cada vez mayor de ataques cibernéticos [18], [19].

Bajo la consideración de que, el caos es un comportamiento tan impredecible que parece aleatorio, debido a la gran sensibilidad a pequeños cambios en las condiciones iniciales, muchos métodos o esquemas de comunicación segura se han desarrollado para cifrar información basándose en sistemas discretos caóticos, El término caos [20] se refiere a una interconexión subyacente que manifiesta acontecimientos que parecen aleatorios y desordenados. La teoría del caos puede ser definida como el estudio de la conducta aperiódica de sistemas determinísticos no lineales, los cuales no solo tienen dependencia sensitiva, sino que también son determinísticos y no lineales, por lo que estas propiedades específicamente son de gran utilidad al trabajar con sistemas que no pueden ser explicados de una manera lineal como lo es el clima, el cuerpo humano, la densidad de las poblaciones, etc. [21]. Existe una relación cercana entre el caos y la criptografía porque los sistemas caóticos tienen características de ergodicidad, propiedades de mezcla, sensibilidad en los parámetros y en las condiciones iniciales, que pueden considerarse análogos a las técnicas de difusión y confusión, integrados en muchos sistemas criptográficos [22].

El uso de pruebas estadísticas en la criptografía parece que se remontan al primer milenio después de Cristo, debido a Abu Yaqub Yusuf Ibn Ishaq al-Sabah Al-Kindi (801-873), que fue un pionero en el criptoanálisis y criptología [23], se le atribuye el desarrollo de un método en el que se podría analizar las variaciones en la frecuencia de la aparición de cartas y utilizarlo para romper el cifrado; es decir criptoanálisis por análisis de frecuencias. Más tarde, en 1863, Friedrich Kasiski publicó un libro, que fue el primer relato divulgado de un procedimiento para atacar

cifras de sustitución polialfabéticos, especialmente el sistema de cifrado de Vigenère, cuyo método se basó en el análisis de las diferencias entre los fragmentos repetidos en el texto cifrado; este tipo de análisis puede dar pistas sobre la longitud de la clave utilizada [24]. Posteriormente, durante la Segunda Guerra Mundial, se transmitieron códigos secretos a través de redes de comunicaciones de radio que usaban códigos formales e informales desarrollados en sus lenguas maternas [25].

Para enfrentar la problemática actual y abordar el inconveniente de seguridad [26], presentan una distribución gradual en el que agregan cifrado homomórfico a los medidores inteligentes implicados en el envío de datos, desde la fuente hasta la unidad de recolección para garantizar que los resultados intermedios no sean revelados a cualquier dispositivo en la ruta. La historia de la criptografía nos da pruebas de que puede ser difícil mantener en secreto los detalles de un algoritmo usado extensamente, siendo una clave más sencilla de proteger, que todo un sistema de cifrado, y es más fácil de substituir si ha sido descubierta. Al diseñar un sistema de seguridad, es recomendable asumir que los detalles del algoritmo de cifrado ya son conocidos por el hipotético atacante, como se enuncia en el Principio de Kerckhoff [27], sólo el mantener la clave en secreto proporciona seguridad.

El objetivo de realizar un cifrado, es el de dificultar o imposibilitar la comprensión de la información a personas ajenas [28]. Shannon, denominado el padre de la teoría de la información [29], determina la entropía como la incertidumbre de una fuente de información. Mucha entropía indica gran imprevisibilidad. El concepto de entropía basado en la teoría de la información es en realidad la medida de la inconsistencia, los datos no estructurados o la aleatoriedad de las variables, siendo menos vulnerable cuanta más entropía contenga [30], [31].

Con los avances tecnológicos de hoy día, se ha incrementado el uso cotidiano de los sistemas de información, lo que ha generado que éstos a su vez sean vulnerables a ataques cibernéticos, por tanto, es indispensable utilizar mecanismos de seguridad, que permitan resguardar la información ante algún ciber-ataque, siendo la criptografía unos de los más utilizados, debido a que se encarga de ocultar los datos ante terceros, proporcionando confidencialidad mediante algún método de cifrado [32].

En las últimas décadas, la información digital ha sido ampliamente difundida a través de Internet y las redes inalámbricas debido a la rápida evolución de la industria multimedia y de comunicaciones. Los sistemas caóticos se caracterizan por su ergodicidad, pseudo-aleatoriedad y la sensibilidad a las condiciones iniciales y parámetros de control, que tienen conexiones estrechas con confusión y difusión en la criptografía. Estas propiedades hacen de los sistemas caóticos una opción potencial para la construcción de sistemas criptográficos [33], [34], [35], [36]. Debido a las características de ergodicidad, propiedades de mezcla, sensibilidad en parámetros de control y en las condiciones iniciales, específicas de los sistemas caóticos, los métodos de encriptación basados en caos parecen ser más eficientes para el uso práctico considerando su complejidad, velocidad y alta seguridad [37].

En [38], se propone un esquema eficiente de cifrado de imágenes, basado en un mapa generalizado de Arnold y un mapa de Bernoulli. Donde el esquema genera un proceso eficaz de permutación y un efecto de difusión en dos vías, mejorando este último a través de generación de secuencias de valores pseudoaleatorios utilizando el mapa de Bernoulli. Así también en [39], se propone una alternativa para la construcción de un algoritmo de ocultación de datos en imágenes digitales, basado en la teoría del caos utilizando mapas caóticos de Bernoulli para cifrar los bits del mensaje antes de su incorporación a la imagen.

En [40], se presenta un algoritmo de cifrado y descifrado de imagen, donde se proporciona una técnica de codificación garantizado en el uso de mapeo múltiple circular basada en caos, formando parte de ellos el mapa de Bernoulli, donde se muestran características confusas de mezcla, impredecibilidad y sensibilidad a los valores iniciales generando números pseudoaleatorios de forma computacionalmente económica y rápida teniendo como propuesta aplicarlo en comunicaciones inalámbricas. En [41], se discute el problema de seguridad de información en datos biométricos, proponiendo una estrategia de cifrado combinando el sistema caótico Bernoulli y mapeo Logístico para mejorar la efectividad en el cifrado, mostrando con resultados experimentales que el cifrado proporciona un desempeño eficiente y seguro.

Los sistemas caóticos han demostrado ser una buena fuente de señales aleatorias para valores específicos dado que los mapas unidimensionales son sistemas dinámicos simples y adecuados para la generación de caos, en este sentido en [42], se presenta la iteración aleatoria de cuatro variantes del mapa Bernoulli a escala discretizada utilizados para diseñar un generador de números pseudoaleatorios que puede producir secuencias binarias con distribución estadística; donde los valores del parámetro de control para el cual el sistema de múltiples mapas produce ruido digital se determinan mediante herramientas matemáticas como: diagramas de bifurcación, función de entropía y exponentes de Lyapunov. En [43], se presenta un diseño de difusión de secuencias con autocorrelación negativa a generar por registros de desplazamiento con realimentación lineal (LFSR), basado en la teoría del caos a través del mapa caótico de Bernoulli y módulo 2, añadiendo secuencias binarias. También en [44] se presenta un análisis y diseño de un generador de ruido caótico a través de un circuito analógico CMOS, que genera señales caóticas utilizando cuatro mapas caóticos de Bernoulli, donde la condición inicial puede ser considerada como la clave secreta en la generación de ruido caótico dado que el parámetro de control se puede seleccionar dentro de un intervalo mayor.

En el trabajo experimental de una comunicación segura basada en caos Zapateiro [45]. Muestra la utilidad del Arduino no solo para trabajos de medición y control, sino de procesos que requieren el uso de operaciones matemáticas y algoritmos. Se hace uso de un generador de señales para obtener una señal sinusoidal que se muestra en la entrada análoga del Arduino, convirtiéndola en digital con una resolución de 10 bits, posteriormente se generan valores en un mapa logístico que servirán para cifrar el mensaje que se quiere enviar, y finalmente se sigue el proceso inverso en el lado del receptor para obtener de nuevo la señal enviada. En ese trabajo se puede ver el desarrollo e implementación de un algoritmo para la comunicación segura con muestreo y transmisión de señales análogas, adicionalmente, aunque la encriptación usa operaciones que no requieren un alto grado de complejidad y tiempo de procesamiento, logra ser segura.

En el estudio de sistemas con capacidades de hardware limitadas se miden aspectos como vida de batería, memoria, latencia, ancho de comunicación, etc.,

estos aspectos se tienen en cuenta a la hora de diseñar sistemas embebidos y a menudo se escogen soluciones minimalistas que se ajusten a estas capacidades. Un estudio exhaustivo de soluciones modernas en criptografía simétrica se muestra en [46], donde se realiza una recopilación para entornos con recursos limitados, permitiendo tener un panorama completo de las necesidades de cada algoritmo ya que esta elección afecta dinámicamente el tiempo de vida y desempeño en los aspectos anteriormente mencionados de un dispositivo.

Se muestra el desarrollo de un sistema embebido robusto para la autenticación basado en la huella y encriptación caótica en [47], donde se implementó un sistema orientado al acceso lógico y físico en entornos que requieren seguridad, usando la información biométrica de un individuo previamente almacenada en un microcontrolador de 32 bits con velocidad de reloj de 48 MHz, con un algoritmo de encriptación basado en caos con una clave de 128 bits. La encriptación de la información biométrica se realiza con un mapa logístico, que se genera con unas condiciones iniciales muy susceptibles a cambios y le dan robustez al proceso de encriptación. Este sistema tiene una capacidad máxima de 370 usuarios registrados y se logró una tasa de falso reconocimiento que es una medida para calcular cuántas veces se le da acceso a un individuo porque se emparejo adecuadamente su huella con la almacenada y una tasa de falso rechazo que es una medida para contar cuántas veces se rechaza a alguien que legítimamente está registrado, este sistema puede considerarse un sistema experto ya que puede realizar autenticación con alto índice de seguridad a un bajo costo y alto desempeño. Se verificó la seguridad de esta propuesta mediante un análisis completo en un nivel estadístico confirmando las altas capacidades de seguridad de este esquema.

La familia de cifrados ARX tiene una alternativa conocida como cifrado de fase, y se diferencia en las operaciones básicas que hacen para lograr la encriptación del texto plano, en [48] se realizó un estudio comparativo para diferenciar claramente la seguridad y desempeño y en ese estudio se encontró que la encriptación de fase en la capa física puede resistir ataques de análisis de tráfico al compararse con la encriptación XOR, y que en términos de desempeño, al tener un tamaño menor en el vector generado de llave puede ahorrar energía y hacer que los ataques de canales laterales sean más difíciles de realizar, sin embargo,

la implementación en hardware puede incurrir en costos adicionales porque requiere un módulo de multiplicación, situación en la que la encriptación XOR es más eficiente en términos de uso de recursos en hardware.

Recientemente, se han realizado varios esfuerzos de investigación para superar los desafíos y encontrar soluciones apropiadas asociadas con la seguridad, especialmente la seguridad de extremo a extremo [49], [50]. Los esquemas de preservación de la privacidad han avanzado significativamente en los últimos años, especialmente debido a la necesidad de comunicación. Algunas investigaciones se han centrado en crear mecanismos de seguridad adecuados para el contexto de los dispositivos de medición inteligentes; Sin embargo, las necesidades son variadas y en aumento. Además, la privacidad cotidiana está expuesta a las intrusiones de quienes tienen propósitos maliciosos y poseen el conocimiento suficiente para encontrar datos confidenciales.

En una investigación reciente, se han presentado varios mecanismos criptográficos para fortalecer la seguridad en los dispositivos de medición y las redes eléctricas inteligentes, según la literatura revisada en [51]; sin embargo, los resultados obtenidos muestran la necesidad de nuevos esquemas para reducir la complejidad y los recursos computacionales en los trabajos revisados [51].

2.4 Referencias

[1]. K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon and H. Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector", Computers & Electrical Engineering, vol. 52, pp. 114-124, 2016

[2]. G. Locke, P.D. Gallagher, "Nist framework and roadmap for smart grid interoperability standards, release 1.0", National Institute of Standards and Technology p. 33, 2010

[3]. M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu, X. Shen. "A lightweight message authentication scheme for smart grid communications",IEEE Trans Smart Grid,vol. 2 (4), pp. 675–685, 2011

[4]. M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu, X. Shen. "Towards a light-weight message authentication mechanism tailored for smart grid communicationsProceedings of the 2011", IEEE conference on computer communications workshops (INFOCOM WKSHPS), IEEE (2011), pp. 1018–1023, 2011

[5]. M. Kgwadi, T. Kunz Securing rds broadcast messages for smart grid applications Int J Auton Adapt Commun Syst, 4 (4), pp. 412–426, 2011

[6]. NIST, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (last accessed April 10th, 2016),

[7]. D. He, N. Kumar, J. Chen, C. Lee, N. Chilamkurti and S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks",Multimedia Systems, vol. 21, no. 1, pp. 49-60, 2013.

[8]. K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon and H. Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector", Computers & Electrical Engineering, vol. 52, pp. 114-124, 2016.

[9]. T. Baumeister. "Literature review on smart grid cyber security.Technical report", University of Hawaii at Manoa (2010).http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf.

[10]. P. McDaniel, S. McLaughlin. "Security and privacy challenges in the smart grid".IEEE Secur Priv, 7 (3), pp. 75–77, 2009.

[11]. A. Irshad, M. Sher, E. Rehman, S. Ashraf Ch, M.U. Hassan, A. Ghani.A single round-trip sip authentication scheme for voice over internet protocol using smart card.Multimed Tools Appl, 74 (11) , pp. 3967–3984, 2015.

[12]. M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai. "Authentication in mobile cloud computing: A survey".J Netw Comput Appl, 61, pp. 59–80, 2016.

[13]. M. Alizadeh, M. Zamani, S. Baharun, A.A. Manaf, K. Sakurai, H. Anada,et al..Cryptanalysis and improvement of “a secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks”.PloS One, 10 (11), pp. 1–21, 2015.

[14]. J.E. Dagle. “Cyber-physical system security of smart grids”. IEEE PES Innovative Smart Grid Technologies, Washington DC, USA. pp. 1-2, Jan. 16-20 2012.

[15]. R. Langer. “Stuxnet: Dissecting a Cyberwarfare Weapon”, IEEE Security&Privacy, Vol.9, N. 3, 2011.

[16]. C. Bekara, T. Luckenbach and K. Bekara. “A Privacy Preserving and Secure Authentication Protocol for the Advanced Metering Infrastructure with Non-Repudiation Service », 2nd IARIA ENERGY Conference, pp. 60-68, March 25-30, 2012.

[17]. M. Mogollon. "Cryptography and security services: mechanisms and applications”, Hershey, PA: CyberTech, pp. 51-97, 2007.

[18]. F. Li, B. Luo and P. Liu. Secure information aggregation for smart grids using homomorphic encryption.In: 2010 First IEEE international conference on Smart Grid Communications (SmartGridComm), Gaithersburg, Mayryland, USA, pp.327–332. 2010

[19]. A. Kerckhoffs. "La cryptographie militaire", Journal des sciences militaries, vol. 9, pp. 161-191, 1983.

[20]. J.A. Coppo, “Teoría del caos y método científico”. The Free Library: Revista Veterinaria, Universidad Nacional del Nordeste, 2010.

[21]. B. Rajan, & P. Saumitr. "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system ", IEEE Transactions on circuits and system (4), pp. I- 53, 2006.

[22]. M. Jiménez, F. Flores, and G. González. "System for Information Encryption Implementing Several Chaotic Orbits". Ingeniería, Investigación y Tecnología, vol.16 (3), pp. 335-343, 2015.
[23]. A. Radwan, S. AbdElHaleem, and S. Abd-El-Hafiz. "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review". Journal of Advanced Research. (7(2), pp. 193–208, 2016.
[24]. S. Singh. 2016). "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography",Anchor Books, 1999.
[25]. D. Kahn. The Codebreakers - The Story of Secret Writing, revised ed, Scribner, 1996.
[26]. N. Aaseng. Navajo Code Talkers: Americas Secret Weapon in World War II, New York: Walker & Company, 1992
[27]. E. McKenna, I. Richardson, and M. Thomson. "Smart meter data: Balancing consumer privacy concerns with legitimate" applications.Energy Policy.vol. 41, pp. 807-814, 2012.
[28]. S. Zeadally, A. S.K. Pathan, C. Alcaraz, and M. Badra. Towards privacy protection in smart grid". Wireless personal communications, vol 73(1), pp.23-50, 2013.
[29]. H. Hennawy, A. Omar, and S. Kholaif. LEA: Link "Encryption Algorithm Proposed Stream Cipher Algorithm.Ain Shams" Engineering Journal, vol. 6(1), pp.57-65, 2015.
[30]. C. Shannon. "A mathematical theory of communication. Bell Sys"t. Tech J., vol. 27, pp.379–423, 623–656, 1948.
[31]. S. Kumar, K. Abhishek, and M. Singh. "Accessing Relevant and Accurate Information using Entropy". Procedia Computer Science, vol. 54, pp. 449-455 2015.
[32]. C. Shannon. "Theory of communication Secrecy Systems", Bell Tech System. J. vol. 28, pp. 656-715, 1949.
[33]. Mogollon, M. "Cryptography and security services: mechanisms and applications". Hershey, PA: CyberTech, pp. 51-97, 2007.
[34]. D. Xiao, XF Liao, "Analysis and improvement of a chaos-based image encryption algorithm" Chaos, Solitons & Fractals., vol. 40 (5), pp. 2191-2199, 2009.
[35]. D. Xiao, Shih, "Using the self-synchronizing method to improve security of the multi chaotic", Optics Communications, vol. 283 (15), pp. 3.030 a 3036, 2010
[36]. YS. Zhang, Xiao D. "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform",Optics andLasersinEngineering vol. 51 (4), pp. 472-480, 2013.
[37]. E.Yavuz, R. Yazıcı, M., Kasapbaşı, & E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions".Computers & Electrical Engineering, vol. 54, pp.471–483, 2017,
[38]. R. Ye. "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism". Optics Communications, vol. 284(22), pp.5290-5298, 2011.
[39]. R., Martínez-González, J. Díaz-Méndez, L., Palacios-Luengas, L., J. López-Hernández, and R. Vázquez-Medina, "A steganographic method using Bernoulli's chaotic maps",Computers & Electrical Engineering,vol. 54, pp. 435-449, 2016.
[40]. G.A.Sathishkumar, .K.Bhoopathy and .N.Sriraam,"Image encryption based on diffusion and multiple chaotic maps", Network Security & Its Applications vol.3, (2), pp. 181-194 2011.

[41]. C., Liew, Shaw, R., L. Li, and Y. Yang, “Survey on Biometric Data Security and Chaotic Encryption Strategy with Bernoulli Mapping. 2014 International Conference on Medical Biometrics.2014.

[42]. J. López-Hernández, R. Vázquez-Medina, , M. Ortiz-Moctezuma, Digital Implementation of a Pseudo-Random Noise Generator using Chaotic Maps, Journals & Books vol. 45 (12),pp. 209-214, 2012.

[43]. Y. Miyazaki, Tsuneda, A., and Inoue, T.Spreading Sequences with Negative Auto-correlations Generated by LFSRs Based on Chaos Theory of Modulo-2 Added Sequences.In ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications pp. 541-544, 2008

[44]. J. López-Hernández, Díaz-Méndez, A., Del-Río-Correa, J., Cruz-Irisson, M. and Vázquez-Medina, R. A current mode CMOS noise generator using multiple Bernoulli maps, Microelectronic Engineering, vol. 90, pp.163-167, 2012.

[45]. M. D. Zapateiro, Acho, L., & Vidal, Y. “An Experimental Realization of a Chaos-Based Secure Communication Using Arduino Microcontrollers”, The Scientific World Journal, Volume 2015, ID 123080, 10 pgs, 2015.

[46]. J.,Kong, H., Ang, M. l.-, & K. P.Seng, " A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments". Journal of network and computer applications, vol. 49, pp.15–50, 2015

[47]. M. A., Murillo-Escobar, C., Cruz-Hernández, F., Abundiz-Pérez, & R. M. López-Gutiérrez, A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Expert Systems with Applications, vol.42 (21), pp. 8198–8211, 2015.

[48]. F. Huo and G. Gong, "XOR Encryption versus Phase Encryption, an In-Depth Analysis", IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 4, pp. 903-911, 2015.

[49]. Z. Mrabet, N. Kaabouch, H. Ghazi and H. Ghazi, "Cyber-security in smart grid: Survey and Challenges", Computers & Electrical Engineering, vol. 67, pp. 469-482, 2018.

[50]. Y. Benslimane and K. Ahmed “Efficient End-to-End Secure Key Management Protocol for Internet of Things” International Journal of Electrical and Computer Engineering, vol.7, no. 6, pp. 3622-3631, 2017

[51]. S. Desai, R. Alhadad, N. Chilamkurti and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure", Cluster Computing, Vol. 22(1), pp.43-69, 2018

CAPÍTULO III

VULNERABILIDAD EN SISTEMAS DE MEDICIÓN

El mundo está experimentando una evolución derivada de las innovaciones en la tecnología de la información que, si bien se crean nuevas oportunidades económicas y sociales, plantean desafíos a nuestra seguridad y expectativas de privacidad. Los medidores de energía, dispositivos de seguridad y aparatos inteligentes están siendo utilizados en muchas ciudades, todo ello conducirá a mejoras sin precedentes en la calidad de vida y para beneficiarse de ellas, las infraestructuras y los servicios están cambiando a nuevos sistemas interconectados de seguimiento, control y automatización [1].

Los cambios traen consigo dos importantes desafíos: la seguridad y la privacidad. La seguridad incluye el acceso ilegal a la información y los ataques físicos causando interrupciones en la disponibilidad del servicio teniendo en cuenta que como ciudadanos digitales se está cada vez más equipados con datos disponibles acerca de ubicación y de las actividades que se realizan donde la privacidad tiende a desaparecer, proteger la privacidad de sistemas que recopilan datos es uno de los desafíos tecnológicos que van mano a mano con los retos de seguridad continua [2].

Debido al aumento de la conectividad y la apertura a la Internet, y un mayor uso de hardware y software, las redes inteligentes son más vulnerables a ataques

cibernéticos. La red inteligente (Smart Grid) es una modernización de la red eléctrica, para supervisar, inspeccionar, proteger y optimizar automáticamente el control y la fiabilidad de las operaciones de la red eléctrica a través de sistemas de monitoreo y control distribuido. A esta red se integran las de Tecnologías de Información y Comunicación (TIC) que permiten el monitoreo y control remoto, sin embargo, la integración expone a los sistemas de energía inteligentes a las amenazas de seguridad y vulnerabilidad, que podrían verse comprometidos por usuarios maliciosos y atacantes

El Sistema de Medición es una infraestructura que integra una serie de tecnologías para lograr sus objetivos de medición que incluye medidores inteligentes, redes de comunicación en los diferentes niveles de la jerarquía de la infraestructura, sistemas de gestión de datos de medición, y los medios para la integración de los datos recogidos en las plataformas e interfaces de aplicaciones de software Al analizar la arquitectura de comunicación de las redes, se exponen los componentes y la infraestructura de comunicación por cable e inalámbrica comúnmente utilizada para comunicar la información relacionada con la energía y se identifican las principales amenazas a la seguridad bajo esta arquitectura [3],[4].

La medición inteligente es una herramienta que implementa una infraestructura que se ha materializado para llevar a cabo la adquisición de datos en tiempo real de los consumidores y transmitirlos. Los datos adquiridos pueden ser utilizados para la regulación del consumo, tanto de los consumidores, y como proveedores. La vulnerabilidad en los dispositivos de medición de energía eléctrica se debe a las características de seguridad débiles, a los protocolos de comunicación y sistemas operativos utilizados en los dispositivos que han sido diseñados para garantizar la calidad de conectividad, control y rendimiento, pero adolecen de seguridad. Garantizar la seguridad y privacidad de la información de los usuarios, requiere un análisis de riesgos potenciales de problemas de ciberseguridad en los sistemas de medición [5].

Considerando que se está en riesgo latente se analizan los métodos que podrían ser utilizados por los atacantes para substraer los datos transmitidos y almacenados a través de la red de AMI. En [6] se ofrece una visión general de las principales consecuencias resultantes de la violación de la seguridad de los sistemas de

información en el caso de la medición. En [7] se discute la confianza, la seguridad de los sistemas, y las cuestiones de privacidad, integridad y disponibilidad, y la facilidad de uso.

Con el uso de las TIC en la red de energía eléctrica, la carga de potencia se puede controlar de forma remota a través de Internet. La comunicación inalámbrica se integra en el sistema de distribución de energía, proporcionando enlaces de alta velocidad de bajo costo y fácil configuración entre dispositivos distribuidos a través del sistema de distribución. Pero, las comunicaciones inalámbricas también son vulnerables a ataques a la seguridad, al igual que los cableados.

Hoy por hoy las redes inteligentes son monitoreadas y controladas mediante el sistema de Supervisión, Control y Adquisición de Datos (SCADA del inglés Supervisory Control And Acquisition), sin embargo es importante analizar las amenazas a la seguridad y los riesgos en los sistemas SCADA para desarrollar una solución adecuada. En [8], [9] y [10] proponen una evaluación sistemática de las vulnerabilidades del sistema SCADA utilizando un marco de evaluación de la vulnerabilidad basado en tres niveles: puntos del sistema, escenarios, y de acceso.

En [11], se presenta un análisis de la seguridad de las tecnologías de la comunicación de las redes inteligentes. Donde se proporciona una descripción detallada de las tecnologías de la comunicación, requisitos y normas. También se presentan las ventajas y desventajas de estas tecnologías de la comunicación. Las tecnologías de la comunicación incluyen ZigBee, comunicación de la red celular, Power Line Communication (PLCom), y línea de abonado digital.

En [12], se estudia y discute experimentalmente sobre las formas de utilizar algoritmos de seguridad en el sistema de monitorización de consumo de energía. En [13] , se discuten los ataques de comunicación y nivel de red que hacen que la red sea más vulnerables a los ataques de seguridad, y cómo estos ataques afectan al funcionamiento de la red inteligente. Se discute en [14], el papel de la seguridad y el sistema de comunicación. Las cuestiones de seguridad se discuten, como la disociación entre SCADA operativa y Sistema de Gestión de la Energía (EMS) y las TIC, las amenazas y las posibilidades, los dominios de seguridad de la información, y los sistemas SCADA y la seguridad SCADA.

En [15], se analiza las vulnerabilidades y los riesgos de seguridad que afectan al funcionamiento de la red. Se discute la dependencia en los sistemas SCADA, intrusiones inalámbricas y de seguridad y encriptación. Se presenta en[16], algunos desafíos de seguridad para la red de AMI y los medios para mitigar las amenazas resultantes de esos desafíos. Por último en [17], presentan una descripción de los problemas relacionados con la seguridad de la red inteligente, incluyendo la confianza y la privacidad, la gestión de la seguridad y la seguridad de las comunicaciones. También proponen requisitos para las soluciones de seguridad eficaces con soluciones de autenticación y cifrado en diferentes niveles, como la generación, la transmisión y la distribución.

3.1 Amenazas a la seguridad de la red inteligente

En esta sección se presenta el análisis de las principales amenazas a la seguridad de red inteligente a través de los requisitos de calidad de la seguridad. En la red, los datos podrían verse comprometidos en el momento de su registro, almacenamiento o transmisión dado que los atacantes pueden inyectar valores manipulados entre el Medidor Inteligente (SM) y los nodos para modificar el tráfico de datos. Esto puede suceder si los atacantes obtienen las claves criptográficas utilizadas para el cifrado de los datos almacenados [18].

Los ciberdelincuentes pueden interceptar la comunicación de datos en la red inalámbrica que se utilice para conectar los nodos con el centro de control, utilizando el ataque man-in-the-middle con la posibilidad de comprometer los enlaces de comunicación, puertas de enlace y enrutadores de datos. Los atacantes también pueden leer y modificar los datos transferidos a través del equipo comprometido e interceptar los datos importantes, además de interceptar los informes de consumo de energía, la fijación de precios, los mensajes urgentes y demás datos del medidor inteligente. Los datos que se transmiten a través de Internet, que posee canales inseguros para la transmisión de datos, posibilita el acceso de forma remota a los datos de consumo de energía que se almacena en una base de datos [19].

Los dispositivos inteligentes envían datos a través de los canales de comunicación con el centro de control. El medidor es un componente crítico en la

red inteligente. La contraseña de la red podría verse comprometida por la captación de los datos transmitidos desde el puerto de comunicaciones ópticas de los medidores o comprometer la interfaz de administración de inicio de sesión. Los atacantes pueden cambiar la cantidad de su cuenta para mostrar un consumo de energía eléctrica más bajo que el gasto real, de manera que se reduce la cantidad de pago. Esto se logra mediante la ejecución de una operación de restablecimiento de la demanda para restaurar el sistema de facturación partiendo de cero. Además, los atacantes pueden utilizar un dispositivo lector inteligente con el programa de software de supervisión para capturar los datos transmitidos a través del puerto de comunicación óptica de dispositivo de medición. Las señales en este caso podrían ser detectadas y registradas para capturar la contraseña [20].

La manipulación de los datos almacenados, es otra amenaza que afecta a la medición inteligente, Si los atacantes pueden obtener el control sobre los datos almacenados, esto puede afectar a la operación del medidor. Los atacantes podrían manipular las tarifas de tiempo de uso, fijación de precios, los registros de eventos físicos además los atacantes pueden aumentar o disminuir la tasa de consumo real para afectar el precio de facturación del consumidor. Al sobrescribir el firmware del medidor inteligente se puede proveer el control del dispositivo y de otros dispositivos inteligentes relacionados por el firmware manipulado, facilitando el robo de energía y de desconexión de la fuente de alimentación de estos.

El uso de software engañoso podría permitir a los atacantes hacerse pasar por el medidor inteligente (bajo tráfico de inyección). El software de suplantación se distribuye por los atacantes para gestionar y contestar las solicitudes de los medidores y no dejan alguna evidencia de manipulación. En este caso suplantar a usuarios válidos y capturar sus registros. Los atacantes también pueden alterar los datos y la información enviados desde los dispositivos al centro de control, como el informe de consumo de energía y señales de precios. Por ejemplo, los atacantes pueden engañar al control de conexión / desconexión y causar un exceso de generación de energía causando pérdidas financieras; e incluso interrumpir el funcionamiento de los dispositivos, causar daños, apagar los dispositivos y causar la pérdida del servicio lanzando comandos de control inexactos [21].

Los protocolos de sistemas de comunicación y sistemas operativos utilizados en los dispositivos evidencian características de seguridad débiles; como el Protocolo dinámico de red (DNP 3.0), Inter-Control Center Communication Protocol (CIPC), la Comisión Electrotécnica Internacional (IEC) 61850. El DNP 3.0 que son utilizados principalmente para el sistema SCADA, mientras que el CIPC se utiliza para la comunicación de datos entre los centros de control. Estos protocolos de comunicación y sistemas operativos están diseñados para la calidad de la conectividad, pero adolecen de debilidades de seguridad de sistemas [22].

El uso de protocolos de comunicación diferentes conduce a dificultades en la construcción de una solución común de seguridad de los sistemas basados en la red en comparación con las redes comunes de computadoras. En contraste, el protocolo de comunicación IP que se utiliza comúnmente facilita el diseño y desarrollo de una solución de seguridad de los sistemas basados en la red común.

Los recursos disponibles de los dispositivos de medición inteligente son limitadas y esto no proporciona flexibilidad a los diseñadores a desarrollar, ejecutar y aplicar todas las características de seguridad necesarios para los sistemas. El espacio de memoria es tan limitado que apenas puede contener su firmware y esta desventaja no permite la actualización del firmware, que es inevitable debido al aumento del número de vulnerabilidades encontradas y los errores de software. Además, la potencia de cálculo de los medidores inteligentes es limitada. Si los datos transferidos se reciben cuando el espacio de memoria está lleno y la CPU está ocupada, esto conducirá a negar y perder el servicio. Además, por ahora existen pocos dispositivos de medición que puedan ejecutar los modernos sistemas de seguridad, como programas antivirus y cortafuegos, mientras que este tipo de programas de software pueden ayudar a detectar o prevenir intrusiones internas o externas [8] .

Ciertos puntos críticos de la red inteligente podrían verse comprometidos a través de Internet. Por ejemplo, los ciber-delincuentes pueden entrar en el router que transmite datos al sistema SCADA, e inyectar datos falsos en contra de ciertas variables de estado o enviar señales de encendido falsa para un grupo de dispositivos eléctricos para perturbar la demanda de carga e incluso ejercer control directo sobre aire acondicionado, agua caliente y refrigeración.

La señal de los precios podría verse comprometida por la inyección de falsos valores. Las señales de precios se obtienen a través de Internet por las aplicaciones, que permite a los consumidores controlar su carga de forma independiente. Los atacantes pueden explotar esta característica para inyectar señales de precios falsos a través de Internet. El aumento de las demandas de carga de los consumidores puede afectar a la programación automática del consumo de energía, cambiar el consumo total de energía de cientos de residencias, y cambiar el perfil de la carga de los consumidores [23].

Los enlaces de comunicación que conectan los dispositivos e Interfaz Hombre-Máquina (HMI) en el dominio de transmisión podrían verse comprometida porque un ataque de interferencia podría ser realizada mediante el envío de señales inalámbricas desde un nodo malicioso con la misma frecuencia de las señales de servicios públicos. Además, la amenaza de espionaje de paquetes, podría llevarse a cabo en caso de que un nodo malicioso haya pasado por alto el procedimiento de autenticación y considerado como uno de confianza con acceso legal a la red. Espionaje de paquetes se realiza de una manera pasiva, sin la necesidad de llevar a cabo cualquier ataque a la seguridad activa.

El sistema de interfaz hombre máquina, es utilizado por los operadores la red inteligente para monitorear y controlar dispositivos remotos de forma remota. Si los ciber-delincuentes pueden obtener acceso no autorizado y el control del sistema HMI y si se están utilizando métodos estándar, podría mostrar una gran cantidad de información relacionada con las operaciones del sistema SCADA, Entonces será posible ejecutar los comandos arbitrarios necesarios para controlar y supervisar el funcionamiento de los dispositivos inteligentes conectados al sistema HMI [24].

El centro de control está conectado a través de red de área local (LAN) a otros servidores redundantes, incluyendo internamente estaciones de trabajo y sistemas HMI. Entonces es posible suplantar al sistema HMI para presentar otra interfaz HMI al operador del centro de control. El usuario externo accede a la información en línea utilizando portales web a través del servidor Web redundante para acceder a los datos a través de la web. Los ciber_delincuentes pueden robar identificador de sesión del usuario (ID), suplantar la sesión, haciéndose pasar por el propietario de la sesión y explotar el portal web del cliente para acceder de forma remota los datos

relacionados con la energía, y los sistemas de información en línea de servicios públicos. Esta amenaza podría afectar al servidor de base de datos, al servidor web para el acceso a datos a través de web, servidor de cálculo para hacer el cálculo de series de tiempo, y al servidor de comunicación para el sistema de adquisición de datos de medición [25].

Los sistemas de software de servidor del centro de control también son vulnerables, los atacantes pueden interceptar o modificar los datos transferidos desde el módem del medidor hasta la sub-estación, que se recoge y almacena en el sistema de software de gestión de adquisición de datos. Los datos recogidos por el software de gestión de datos de los medidores inteligentes podrían verse comprometidos, esto incluye el factor de potencia, demanda activa / reactiva, voltajes y corrientes y tensiones de línea. [26].

3.2 Vulnerabilidad en la Seguridad de los sistemas de redes inteligentes

El software de gestión de datos se conecta con el Sistema de Información Geográfica (SIG) cuando requiere recuperar mapas de fondo, se realiza a través de protocolos públicos, que podrían ser aprovechadas para cometer actos ilícitos; también se considera como otra amenaza, la interfaz de visualización de datos disponible para los usuarios externos para acceder a los datos del medidor a través de Internet, debido a que los enlaces de comunicación web remotos a veces no están protegidos por cortafuegos o una red privada virtual (VPN), los atacantes pueden obtener directamente el acceso no autorizado al sistema SCADA[27].

En [28] y [29], se muestra un amplio análisis de los requisitos de seguridad de los sistemas, las amenazas y vulnerabilidades en la infraestructura de medición avanzada (AMI), dominio del cliente y sistema SCADA. También incluye una evaluación a sistemas de seguridad en las redes inteligentes con el fin de identificar amenazas y vulnerabilidades, análisis de probabilidad, análisis de impacto, y la determinación de los riesgos. Además, se analizan los principales requisitos de seguridad de sistemas para asegurar la red inteligente contra ataques a la seguridad.

En [30] y [31], se evalúa la pertinencia propuesta como la de NISTIR 7628 que presenta un marco analítico para la seguridad de las redes inteligentes y proporciona

una línea de base para las organizaciones para facilitar el desarrollo de soluciones eficientes y estrategias para problemas de seguridad. Aunque NISTIR 7628 es considerado como el más amplio esfuerzo de normalización entre los esfuerzos industriales existentes que investigan la seguridad de las redes inteligentes, NISTIR 7628 se centra en la seguridad a nivel del sistema y no en la transferencia de información entre los componentes, donde la demanda es que cada organización sea responsable de desarrollar la arquitectura de seguridad para la información de dominio, y por consiguiente, dicha organización debe asignar los requisitos de seguridad a cada componente .

El término privacidad transmite numerosas ideas, como privacidad de pertenencias, actividades, privacidad de decisión, etc. La forma de privacidad a la que se hace referencia en esta sección es la privacidad de la información que se refiere al control de una entidad sobre la adquisición, divulgación y uso de información personal [32], [33]. La capacidad de un individuo para controlar personalmente su propia información se considera un desafío ético y de derechos humanos clave de la era de la información [34], [35]. La Figura 3.1, muestra los cuatro tipos principales de privacidad y se describen a continuación [36]:

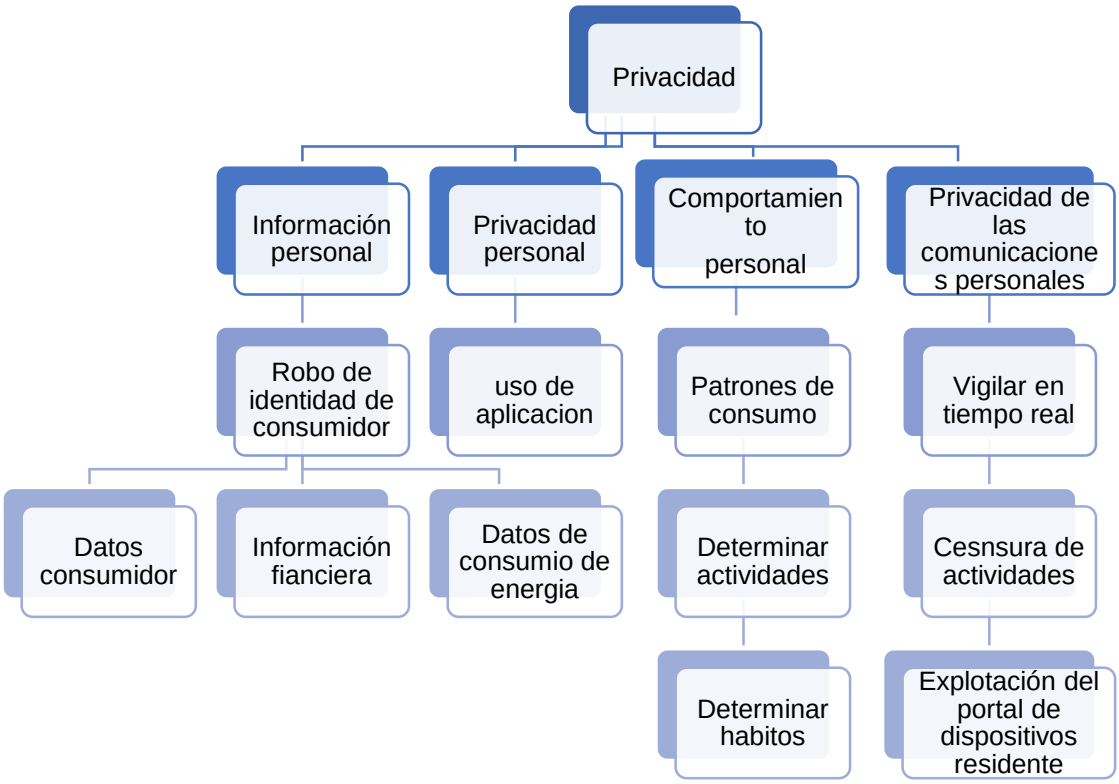


Figura 3.1 Tipos principales de privacidad AMI.

La privacidad de la información personal implica el derecho a controlar cuándo, dónde, cómo, a quién y en qué medida un individuo comparte su información personal, así como el derecho de acceder a la información personal que se proporciona a otros, para corregirla y garantizarla. De igual manera el derecho a controlar la integridad del propio cuerpo, cubre cosas como los requisitos físicos, problemas de salud y dispositivos médicos necesarios. Los individuos tienen el derecho a tomar sus propias decisiones sobre lo que hacen y evitar que ciertos comportamientos personales sean compartidos con otros, derecho a comunicarse sin vigilancia, supervisión o censura indebidas.

3.3 Amenazas en la seguridad en el sistema de redes inteligentes

Los ataques de integridad de datos intentan modificar los datos transmitidos por la red inteligente como la facturación, la contabilidad o la fecha de la información. Aunque los ataques de integridad pueden no afectar directamente a la funcionalidad de las redes de energía como un todo, todavía representan un impacto crítico; por ejemplo la clase de ataques de integridad y de inyección de datos falsos presentados en [37], donde estos ataques pueden pasar por alto las comprobaciones de integridad de datos en el sistema, y explotar las configuraciones del sistema de potencia e inyectar datos falsos en el centro de monitoreo.

A diferencia de los atacantes a la integridad de datos, los ataques dirigidos a la confidencialidad y privacidad de la información amenazan los datos sobre el mercado de energía y la privacidad de los consumidores. Por ejemplo, tratan de adquirir información histórica de consumo de energía, números de identificación, espiar enlaces de comunicación, canales inalámbricos o datos almacenados sin alterar o eliminar registros. Por lo tanto, para garantizar un entorno operativo legalmente dentro de la red inteligente, la confidencialidad debe tenerse en cuenta para asegurar las transacciones financieras seguras y proteger la privacidad de los consumidores [38].

La integración del sistema de las tecnologías de la información y comunicaciones (TIC) dentro de la red eléctrica expone la red inteligente a las amenazas que podrían resultar en un impacto significativo en las operaciones de la red de energía, en

particular, la transmisión y distribución de energía. Vale la pena señalar que es difícil comprometer un enlace de comunicación en una red de energía con la autenticación, sin embargo debido a la naturaleza distribuida y ubicua de la red, además de la integración de la tecnología inalámbrica, los ataques contra la integridad de los datos y la información confidencial mediante el establecimiento de una conexión a la red de energía aún son posibles, por lo que deben ser identificados y abordados adecuadamente [39] .

La evaluación de las amenazas identificadas, su análisis y la categorización, necesitan mayor investigación y dependen del contexto; evaluar las amenazas ayudará a determinar la factibilidad de cada ataque de seguridad para permitir a las partes interesadas evaluar las vulnerabilidades y el grado de protección necesaria, y las normas mínimas de seguridad. La Figura 3.2, refiere la tendencia reciente en el número de esquemas de preservación de la privacidad publicados por investigadores de 2011 a 2017. La gráfica muestra la cantidad de artículos publicados por año que se centran principalmente en preservar la privacidad de los datos de consumo de energía del consumidor. Esta renovada atención se debe a los recientes despliegues de medidores inteligentes en varios países y sus preocupaciones sobre la privacidad [40].

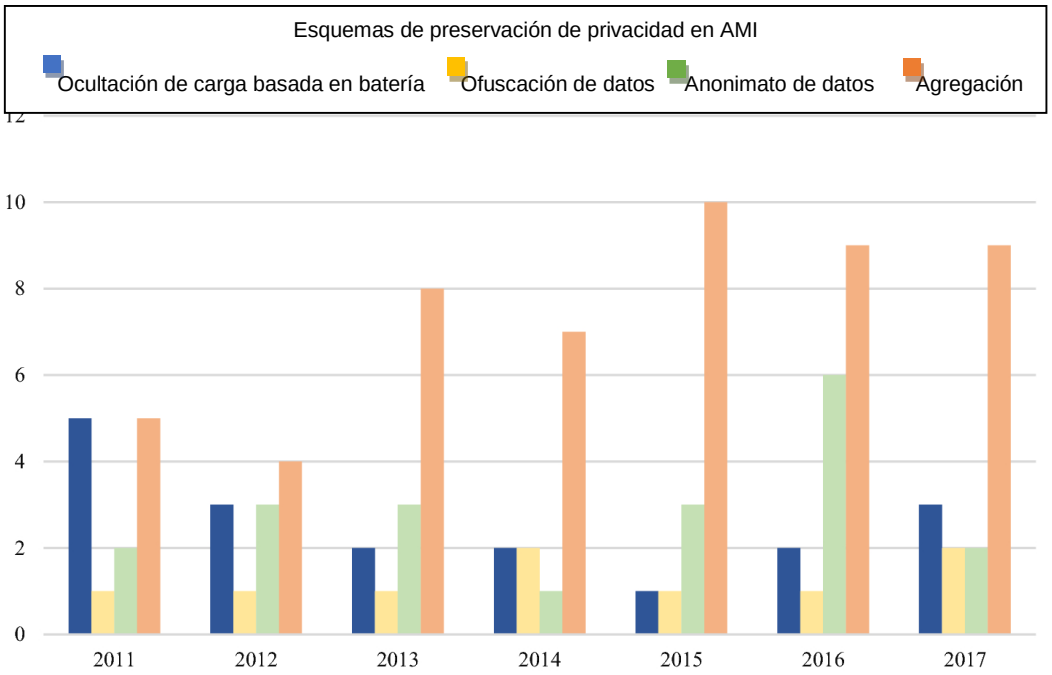


Figura 3.2 Tendencia en esquemas de preservación de la privacidad publicados de 2011 a 2017

La preocupación por la privacidad de los datos relacionados con la energía ha motivado a varios investigadores a proponer nuevos enfoques de preservación de la privacidad para la infraestructura de medición. Estos enfoques se clasifican en dos categorías: esquemas criptográficos y no basados en criptografía, dada la perspectiva que tiene nuestra investigación se orienta hacia esquemas criptográficos, como se muestra en la Figura 3.3. El enfoque criptográfico se puede definir como una manera de limitar la información que se filtra [41].

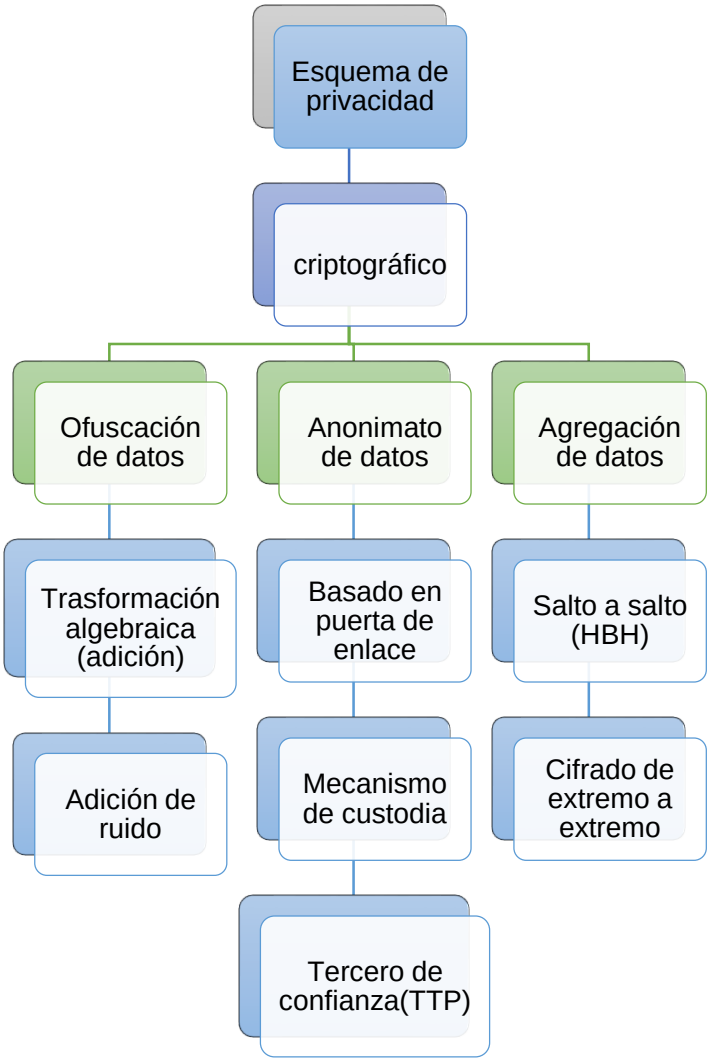


Figura 3.3 Esquemas criptográficos para preservación de la privacidad en infraestructura de medición.

El enfoque criptográfico se divide en tres categorías: ofuscación de datos, anonimización de datos y agregación de datos. Además, a partir de la literatura, se identifican los pros y los contras de trabajos actuales que utilizan estos enfoques criptográficos como se evidencia en la Tabla 3.1, que permite conocer las investigaciones reportadas sobre la preservación de la privacidad en los dispositivos de medición inteligente [41], [42].

La ofuscación de datos brinda una oportunidad única para enmascarar los datos de consumo de energía originales a través de la aplicación de ruido aleatorio mediante una transformación algebraica adecuada en los datos de uso de energía.

El segundo enfoque es la anonimización de los datos; donde su objetivo clave es separar la identidad de los clientes de los datos de consumo de energía. La idea es que las empresas de servicios públicos reciban suficiente información para calcular la información requerida, pero no lo suficiente como para asociar los datos con un medidor específico o un usuario.

El tercer enfoque es la agregación de datos. La idea básica detrás de ésta técnica es utilizar agregadores en la red para concatenar y resumir paquetes de datos de varios dispositivos utilizando funciones como la suma o el promedio. Aunque la agregación de datos reduce la transmisión de los mismos, tiene problemas de privacidad, ya que, esta operación requiere acceso a datos de texto simple.

En la tabla 3.1, se presenta la clasificación de los esquemas existentes de agregación de datos que preservan la privacidad en diferentes categorías según las técnicas centrales de preservación que se utilizan en cada esquema.

Tabla 3.1.Técnicas de preservación de la privacidad.

Autor	Método	Pros	Contras
Yan et al. [2015]	Protocolo IAC	Eficiente en términos de demora de extremo a extremo y pérdida de paquetes	Nodo defectuoso no considerado Tema de eficiencia energética no considerado
Bartoli et al. [2010]	Agregación mediante la operación de concatenación.	Seguridad de extremo a extremo	Gastos generales adicionales No se guarda ancho de banda notable

			Alta tasa de caída en el canal con pérdidas
Tonyali et al. [2016]	FHE o polinomio generado aleatoriamente (MPC seguro)	Preserva las lecturas reales del medidor	Tamaño significativo de los datos y alto retraso.
Badra y Zeadally [2017]	Encriptación homomórfica simétrica y métodos de intercambio de claves.	Bajos gastos de transmisión y mensajes. Resiliencia contra numerosos ataques.	Alto tiempo de intercambio y cálculo de DH.
Li et al. [2017]	Esquema de PPMA	Garantiza la privacidad de las personas.	Precios dinámicos no soportados Medidores inteligentes averiados no considerados Alta complejidad
Wang [2017]	Protocolo de agregación de datos basado en identidad	Logra firma basada en identidad con una agregación.	Alto costo de rendimiento
Ford et al. [2017]	Nuevo protocolo de agregación de datos para una comunicación segura y eficiente.	Soporta facturación por tiempo de uso Alcanza la confidencialidad deseada, la integridad y la privacidad del consumidor.	La asunción de TTP y UC no va a conspirar
He et al. [2017]	Agregación de datos ligeros utilizando ECC	Thwarts ataques internos y externos. Logra confidencialidad, integridad y autenticación.	Mayor costo de cálculo en comparación con [118] Consiste en un agregador y un tercero de confianza (TTP) Lecturas de consumo de energía conocidas por agregador.
Shen et al. [2017]	Eficiente preservación de la privacidad Agregación de datos de cubos	Eficiente en términos de costos de comunicación y escalable.	Mayor costo computacional Operación adicional de emparejamiento
Ferrag [2017]	Cifrado bilineal basado en identidad cifrado	Logra datos y privacidad. Previene la reproducción de	El ataque de inyección de datos falso no se considera Parcialmente resistente al ataque de colusión y dicción

		datos, modificación, ataques de hombre en el medio.	
Bae et al. [2016]	PECA	Privacidad con servicios de DR específicos del usuario	Altos gastos computacionales Altos gastos de comunicación
Abdallah y Shen [2017]	Criptosistema homomórfico ligero basado en celosía	Previene los ataques de repetición y asegura la integridad de los datos.	Alto costo computacional
He et al. [2017]	Esquema de agregación de datos que preserva la privacidad contra atacantes internos	Coste computacional eficiente	La privacidad del costo de la energía no se considera Privacidad de ubicación no considerada
Lu et al. [2015]	Enfoque de agregación basado en conjuntos	Resultado de agregación de datos más detallado Eficiente en términos de costos computacionales y de comunicación.	Carece de integridad de datos
Tahir et al. [2017]	Enfoque de agregación basado en conjuntos con integridad de datos	Asegura la integridad de los datos.	Sufre gastos generales adicionales
Shi et al. [2015]	Protocolo de agregación diverso basado en agrupación	Admite la agregación de datos con detección de errores.	Implementación compleja Solo se considera el ataque de minería de datos maliciosos.
Li et al. [2015]	Esquema de agregación de doble función basado en la técnica criptográfica de celosía	Coste computacional eficiente Eficiencia en la comunicación.	Solo se considera el ataque de texto plano. No hay análisis de comparación con otros esquemas. Ataques internos no considerados
Chen et al. [2015]	PDAFT	Soporta tolerancia a fallos	Falta análisis de costos de cómputo

			Alta complejidad
Jia et al. [2014]	Agregación de datos para datos de series de tiempo.	Soporta datos de medición de alta frecuencia	No se admiten datos de medición de baja frecuencia
Lu et al. [2015]	EPPA	Resistir diversas amenazas Menos gastos de computación y comunicación	Claves de sesión sin cambios Ataques internos no considerados Datos de usuario expuestos
García y Jacobs [2011]	Cifrado de Paillier en el intercambio aditivo	Notable detección de fugas	Alta sobrecarga de comunicación Cifrado caro No escalabilidad

3.4 Criptografía en el fortalecimiento de la seguridad de los sistemas de medición

Dentro del ámbito de la seguridad en redes inalámbricas, a nivel mundial existen dos protocolos muy fuertes, que son Z-Wave y Zigbee ambos pertenecen a organizaciones sin fines de lucro que buscan ir perfeccionando las características de esta tecnología. Al ser en su mayoría implementaciones inalámbricas, pueden implementarse diferentes protocolos ya sea abiertos o propietarios, pero las vulnerabilidades que puede sufrir son las mismas que cualquier otra red inalámbrica. La opción de implementar criptografía de clave simétrica, tiene una desventaja y es que tanto el emisor como el receptor deben de conocer la clave para cifrar y descifrar el mensaje. A continuación, se mencionarán los tipos de criptografía simétrica que existen para reforzar la seguridad en este tipo de redes. Cifrado en flujo: Cifrado Cesar, Cifrado con máquina enigma, Cifrado de Vernam y el cuaderno de uso único (one use pad). En cifrado de bloque: Cifrado de Hill, DES y AES [43].

La tecnología ZigBee, es un conjunto de protocolos de red de área personal inalámbrica (WPAN), fiable, eficiente, alta disponibilidad, bajo precio, bajos requisitos de recursos, seguro y basado en el estándar IEEE802.15.4. La seguridad es un tema primordial en las redes de comunicaciones, más cuando de una red

inteligente se habla, los protocolos de seguridad más usado en estas redes (ZigBee / Z-Wave) donde todos los componentes que la conforman son fundamentales y cumplen una función esencial, es importante la validación de todos los dispositivos que deseen tener acceso a la red, con el fin de evitar accesos no deseados y la manipulación de los paquetes que viajan a través de la red, Con el objetivo de que un intruso no pueda conectarse y transmita información falsa, alterando los informes de consumo de energía en el hogar del consumidor [44]

La seguridad que ofrece ZigBee, utiliza algoritmo criptográfico simétrico o de secreto compartido específicamente AES-128 (Advanced Encryption Standard) con claves de 128 bits, [45], este estándar ha sido emitido por el Instituto Nacional de Estándares y Tecnología (NIST) y especifica que es un estándar de cifrado de clave simétrica, adoptado por el gobierno de Estados Unidos y utilizado para la protección de datos electrónicos. Debido a sus características, AES se considera confiable y eficiente ya que es un estándar adoptado por esta gran potencia mundial, la cual se ha caracterizado por ser uno de los pioneros en cuanto a seguridad se trata [46].

En [47], se considera importante complementar Zigbee con otro tipo de cifrado para asegurar y minimizar las vulnerabilidades que este estándar pueda presentar, entre algunas sus recomendaciones es el de implementar cifrado asimétrico. Ya que este tipo de criptografía es más confiable y mucho más complejo, al utilizar dos claves diferentes para el proceso de encriptación, una clave pública o compartida para cifrar y una clave privada o secreta para descifrar. Ejemplos utilizados en Zigbee son la autenticación basada en firma digital como RSA (Rivest, Shamir y Adleman) y el intercambio de claves D-H (DiffieHellman) basado en ECC (Elliptic Curve Cryptography) [48].

En [49], se analizan los dos tipos de criptografía que pueden ser utilizadas en Zigbee, tanto la asimétrica y simétrica, según características especificadas y se determinó que ambos mecanismos tienen características diferentes y se enfocan en diferentes puntos, por un lado la encriptación simétrica sacrifica el aseguramiento de la información para ser más eficiente en términos de velocidad en el procedimiento de encriptación (cifrado y descifrado) al ser con una sola clave conocida tanto por el emisor como por el receptor, y por otro lado el mecanismo de criptografía asimétrica sacrifica la velocidad, volviéndolo más lento al utilizar dos

claves, con tal de ofrecer mayor confiabilidad, mayor integridad y una autenticación e identificación más eficientes en la red.

En [50], se analizan las características y mecanismos de encriptación del protocolo Z-wave, con el fin de hacer una comparación entre los dos protocolos para generar una propuesta ideal para las SG. Z-wave, opera en frecuencias diseñadas para comunicaciones de bajo ancho de banda en los dispositivos integrados, como los sensores de seguridad, alarmas y paneles de control domótica, posee una transmisión de datos con velocidades de hasta de 100 kbps, el cual necesita tener la seguridad necesaria para el aseguramiento de la información en la red, cuenta con diferentes opciones de encriptación, como mecanismos de cifrado por bloques, entre ellos, CTR – Counter Mode, OFB – Output Feedback Mode, CFB – Cipher Feedback Mode, (CBC-MAC), este último es con un código para autenticar los mensajes como, el valor MAC, asegura que el protocolo no sea manipulado durante la transmisión de los datos y que haya sido enviado por el nodo que dice ser la fuente del mensaje .

Por lo anterior se determina que el protocolo ZigBee y Z-wave tiene una serie de características similares y de igual forma cuenta con una serie de atributos que los diferencian el uno del otro, ambas son tecnologías de comunicación en redes inalámbricas, basadas en chip, son utilizadas para la creación de sistemas que controlen funciones específicas en las SG como por ejemplo sistemas de seguridad, acceso a puertas, sistemas de iluminación, entre otros sistemas que puedan implementarse en un hogar inteligente, ambos son de muy bajo consumo de energía, fiables, eficientes, de alta disponibilidad, la gran diferencia entre ambos según el análisis de las características de cada protocolo es que Zigbee, es respaldado por el estándar IEEE802.15.4 y en el caso de Z-wave, no cuenta con el respaldo de ningún estándar internacional, en cuanto a seguridad se trata. ZigBee también toma ventaja de acuerdo a su comparación en este artículo, al implementar AES-128, la velocidad de datos, y la capacidad de dispositivos conectados en la red. Según datos recopilados que incluyen una serie de características tanto en ventajas, encriptación y capacidad de cada protocolo estudiado en este apartado [39], [40].

Se han mencionado algunas vulnerabilidades en las redes y en este caso específico hablando de redes locales y de hogar, que son las comúnmente utilizadas para la red inteligente y en sistemas de medición además de ser las utilizadas en conexiones a casas inteligentes, el problema surge porque aún no se tiene una solución cien por ciento segura, ya que si por ejemplo se maneja la seguridad por medio del anonimato ¿quién es el responsable de asignar claves robustas y fuertes y de estar cambiándolas cada tiempo determinado?, además de qué manera se asegura que no surjan confusiones y malestar en los consumidores quienes cuenten con poco conocimiento sobre la seguridad en redes, cabe destacar que todavía hay muchas incógnitas en cuanto al modus operandi de este tipo de tecnologías tan recientes, ya que estamos hablando de poco más de una década de la puesta en marcha mundial de estas tecnologías y hasta hoy día el acceso a ella aun es limitado dado que es la mínima población quienes ya cuentan con ella. También queda la incertidumbre sobre la garantía que dichas claves por muy robustas que estas sean puedan ser interceptadas por un hacker.

3.5 Vulnerabilidades en las redes inteligentes y los medidores inteligentes.

Como es mencionado en este capítulo las tecnologías de la información son de gran importancia al implementar una red eléctrica avanzada como lo son las redes inteligentes, que cuenta con una comunicación bidireccional entre el proveedor de servicio eléctrico y el cliente final. Convirtiendo la distribución de la energía en un proceso automático más eficiente ya que desaparece la lectura manual a cada medidor. Además las redes inteligentes ofrecen ventajas importantes tanto a los proveedores del servicio eléctrico como al consumidor, entre ellas está el poder administrar en tiempo real el consumo de energía eléctrica en los hogares, también facilitar a la empresa proveedora de energía llevar un control con mayor eficiencia del abastecimiento de todos los hogares que utilizan medidores inteligentes, así como también generar avances al país en los sectores; productivo (electricidad), el económico (ahorro en el hogar y en la empresa proveedora de energía eléctrica) y el ambiental (menos contaminaciones en las plantas hidroeléctricas) .

Por el otro lado, la necesidad de tener conexión a Internet y el uso fundamental de las TICs, hace que la red inteligente sea más vulnerable a las amenazas, ya

que serán expuestas a los ciberataques por tener una conexión 24/7 y podría generar resultados con pérdidas importantes tanto para el consumidor como para el proveedor de la energía [51]. En el ámbito de las TICs se conoce que ningún método o proceso es totalmente seguro, todo sistema cuenta con diferentes tipos de vulnerabilidades las cuales se tienen que identificar y tratar de evitar que se convierta en un peligro latente para los sistemas o tratar de mitigar su impacto de llegar a suceder, como por ejemplo una vulnerabilidad que se presenta en el protocolo ZigBee utilizado en las redes inteligentes es que este utiliza la encriptación simétrica AES-128 [40].

Hoy en día alrededor del mundo se está dando una situación de suma importancia en cuanto al avance de las tecnologías, por el hecho que van avanzando muy rápidamente, pero no así la seguridad los controles de diagnóstico y recomendaciones que deben tenerse para las mismas [52], el hecho es que eso trae muchos riesgos, ya que al adquirir tecnologías nuevas e instalarlas sin los debidos estándares mínimos de seguridad puede traer muchas complicaciones a corto, mediano o largo plazo como lo son la suplantación de identidad, el quedar abiertos o expuestos a la manipulación y el espionaje de datos por ciberdelicuentes al quedar vulnerables al usar tecnologías poco maduras en cuanto a seguridad se refiere.

Según pruebas hechas en el Reino Unido y partes de Europa un ciberdelicuente que ataca un medidor inteligente puede inclusive provocar un apagado remoto a un hogar lo cual podría traer serios problemas a los habitantes, ya que luego del apagón podrían suscitarse asaltos a dicha vivienda [53]. El asunto con los medidores inteligentes es que por sus ventajas como la de tener un mejor control de los gastos en electricidad, hasta el de poder controlar toda una vivienda por medio de estas tecnologías, está en auge y corporaciones como ejemplo google creó una aplicación para el uso de monitoreo de medición mediante redes inteligentes llamada PowerMeter, que brinda información de consumo de energía a los usuarios con casas inteligentes y sugerencias de ahorro, sin embargo para acceder a esta aplicación se deben facilitar algunos datos del usuario que podrían quedar comprometidos[54].

Existe gran diversidad de sistemas de anonimato, encriptación, cifrados, antivirus, firewall, otros, [45], [48],[50], [52], [54], pero al ser las tecnologías de los medidores inteligentes tan recientes en el mercado aún existen muchas brechas al respecto y de cuál es la mejor solución contra la cantidad de vulnerabilidades que existen como las maneras de llegar a la mejor forma de vivir en un mundo totalmente informatizado que se ha generado con el internet de las cosas y su gran auge e incremento visto en estos últimos años en las redes y medidores inteligentes.

Las vulnerabilidades no depende solo de que sistema de protección se pueda acceder o utilizar, sino también es de suma importancia de la manera en que se manejen los procesos con los SM desde su propio inicio (creación e instalación), la puesta en marcha hasta la verificación constante del tipo de manipulación de los datos que viajen a través de las SG, se deben dar capacitaciones sobre seguridad y riesgos a los clientes que adquieran estas tecnologías ya que de nada valdría tener las mejores herramientas de seguridad en los SM si los clientes caen ignorantes ante cualquier tipo de estafa u ataque informático, proporcionando datos o claves como se logra ver a menudo hoy en día [55].

3.6 Consumidores en el escenario de las redes inteligentes

Los consumidores buscan la mejor prestación del servicio de energía eléctrica, que se representa en la calidad de la energía, en mediciones exactas y en precios razonables, por ello las empresas proveedoras de este servicio se ven obligadas a modernizar el sistema de medición, adaptándose a las nuevas condiciones del mercado y brindando una información más detallada sobre el consumo de cada cliente [46], [56]. Una de estas alternativas que ha tomado auge en los últimos años es la denominada “medición inteligente”. Concepto que nace a partir de la búsqueda de la optimización de los procesos de medición, lectura del medidor y facturación, principalmente con el fin de contribuir a los objetivos mundiales de eficiencia energética de reducir el impacto climático generado por emisiones de gases de efecto invernadero y de satisfacer en general las necesidades de una red inteligente.

La red inteligente requiere de información en tiempo real, por lo que necesita una nueva forma de medir denominada Smart Metering o “medición inteligente”, refiriendo a un multiproceso simultáneo que incluye: medición, registro, almacenamiento y transferencia bidireccional de información en tiempo real (o cercano), de las cantidades de energía consumida junto con otras variables útiles para la gestión de la red. Mediante la “medición inteligente” se mantiene informado al consumidor para que pueda proponer sus propias políticas de consumo, según lo considere [47], [51].

Las comunicaciones para las aplicaciones de redes inteligentes manejan datos sensibles, la seguridad física como la seguridad cibernética y la privacidad constituyen factores clave para su amplio despliegue y adopción. Para determinar las vulnerabilidades dentro de estas aplicaciones en esta tesis se evalua la metodología de ataque, debido a que los métodos exactos pueden variar. La comprensión de los motivos del atacante y las vulnerabilidades inherentes de los sistemas ayudan a determinar cómo podría acercarse un atacante, evaluar y romper la seguridad de un sistema.

lectura remota de la energía consumida mejorando la gestión operativa de los proveedores y facilitando la comprensión del consumidor de energía y costo, permitiendo la inhabilitación del suministro de energía en casos de emergencia, la detección de fugas de energía o fraude y finalmente el apoyo a los métodos de pago (prepago).

En esta tesis se presenta el ámbito de utilización de los medidores de energía actuales en el entorno de la red eléctrica inteligente, a través de una revisión de la literatura sobre vulnerabilidades detectadas en los sistemas de medición, y se muestran los principales riesgos cibernéticos, revisando una serie de propuestas que permitan fortalecer la integridad, disponibilidad y confidencialidad de los datos involucrados estableciendo contramedidas.

Existen diferentes funciones de los medidores inteligentes, dentro de las cuales destacan:

- Control de robo de energía eléctrica: Algunos medidores pueden detectar la manipulación del medidor, detectando situaciones anormales como el no registro del consumo de energía por un período de 24 horas.

- Registro y almacenamiento de datos: En general, los medidores tienen la capacidad de registrar y almacenar datos de perfiles de carga, eventos como perturbaciones, caídas y elevaciones de tensión, cortes y suministros del servicio, etc.

- Control de electrodomésticos inteligentes: Algunos medidores inteligentes pueden reducir el tiempo de utilización de electrodomésticos inteligentes.

Los medidores inteligentes tienen dos tareas específicas: medición y comunicación, y por lo tanto cada medidor tiene dos subsistemas: metrología y comunicación. La parte de metrología varía dependiendo de un número de factores que incluyen región, fenómeno medido, precisión requerida, el nivel de seguridad de los datos, la aplicación. El método de comunicación también hay factores como la seguridad y encriptación [49], [52].

Como el número de medidores inteligentes aumentan exponencialmente, los problemas de seguridad asociados con la red inteligente y el sistema de medición crecen sustancialmente desde dentro y fuera del sistema. La información detallada del consumo de los clientes es fundamental, ya que puede revelar su estilo de vida. La transmisión de datos a larga distancia, así como el almacenamiento de los datos en varios lugares para la retransmisión o análisis también puede crear vulnerabilidades en términos de robo de datos o la manipulación de estos. La señal de precio y comandos recibidos por los consumidores también son áreas potenciales para ciberataque con el objeto de espionaje, dañando la infraestructura o el robo de energía [53].

Al analizar los datos de los medidores inteligentes, es posible llevar a cabo un perfil del consumidor con una precisión alarmante. Los ejemplos van desde cuántas personas viven en la casa, tipo de dispositivos utilizados, la seguridad y los sistemas de alarmas, el comportamiento de los residentes, incluso sin la utilización de sofisticados algoritmos y herramientas asistidas por computadora, ya que es posible identificar el uso de los electrodomésticos en una casa, mediante el análisis de sólo

unos 15 minutos de datos de consumo energético acumulado, y una vez que se tenga acceso a los datos de la red en el sistema de medición, también se tendrá acceso a la información de nombre y dirección del cliente, recogida y almacenada para fines de facturación[54] y [55].

Las intrusiones contra sistemas de medición deben ser estudiadas desde la perspectiva de los atacantes y sus motivaciones que puede ser por intereses propios, fines de sabotaje o terrorismo. Categorizar a los ciber-delincuentes y su motivación es especialmente importante cuando se trata de diseñar contra medidas; considerando que los atacantes con suficientes recursos y nivel de experiencia tienen poca motivación para cometer robo de energía, sin embargo, pueden utilizar las vulnerabilidades de los medidores inteligentes para la denegación de servicio o invasión de la privacidad.

En otro escenario, los datos podrían ser alterados mientras se transfiere a través de la red. Esto comprende de inyectar datos falsos en el sistema, o interceptación de las comunicaciones dentro de la infraestructura.

Algunos ejemplos de estos ataques se listan a continuación:

- Puerto Rico (2009), los medidores inteligentes puertorriqueños fueron pirateados en masa, lo que dio lugar a un fraude de facturación generalizado.
- EE.UU. (2010) Tom Donah de la CIA, intrusiones en compañías de suministro de energía eléctrica ocasionan cortes de suministro en varias ciudades.
- Reino Unido (2011) se obtienen de manera fraudulenta millones de libras, mediante claves de recarga atacadas en medidores de prepago.
- Termineter (2012), programa que permite modificar el software o cambiar la tarifa de factura de consumo.
- Investigadores españoles (2014), logran hackear un medidor inteligente de electricidad a través de la reingeniería, provocando cortes en el suministro y suplantar la identidad del usuario.
- Reino Unido (2017), los nuevos medidores de energía inteligente que se instalarán en 27 millones de hogares fueron considerados vulnerables por GCHQ (Cuartel General de Comunicaciones del Gobierno.) Los atacantes los

saquean para robar datos personales y defraudar a los consumidores al manipular sus cuentas.

El cliente está equipado con un dispositivo medidor que recoge los datos basados en el tiempo y puede transmitir los datos recogidos a través de redes fijas comúnmente, así como las redes públicas tales como teléfono fijo o celular. Los datos de consumo medidos son recibidos por el sistema host. Posteriormente, se envía a un sistema que gestiona el almacenamiento y análisis de datos y proporciona la información en una forma útil para el proveedor. [56], [57].

La investigación de vulnerabilidades y módulo de verificación tiene como objetivo identificar las vulnerabilidades en los servicios de trasmisión de los datos basado en la metodología SQUARE (Security Quality Requirements Engineering) para la obtención, análisis, clasificación y priorización de los requisitos de seguridad [58], [59].

La metodología SQUARE, está compuesta por los siguientes pasos:

Paso 1: Definiciones. Entre los más importantes, vulnerabilidad se define como un punto débil en un sistema que puede ser explotada por amenaza de código y los resultados en incumplimiento o violación de la política de seguridad del sistema y una amenaza se define como la capacidad de código para desencadenar una vulnerabilidad.

Paso 2: Identificar los Objetivos de Seguridad. Confidencialidad, integridad, autenticación, autorización, control de acceso, la disponibilidad y el no repudio.

Paso 3: Diseños de la arquitectura.

Paso 4: Realizar la evaluación de riesgos. El riesgo se define como "una función de la probabilidad de que una amenaza de determinada fuente ejerza vulnerabilidad potencial en particular y el impacto resultante de ese acontecimiento adverso en la organización."

Paso 5: Técnicas de selección de requisitos.

Paso 6: Elección de requerimientos de seguridad.

Paso 7: Clasificar Requisitos bajo las siguientes categorías: Integridad, confidencialidad, autenticación, autorización, control de acceso, de rendición de cuentas (no repudio), y la disponibilidad.

Paso 8: Priorizar Requisitos. Se Priorizan los requisitos de seguridad: alta, mediana y baja.

Paso 9: Requisitos de Inspección. Se examinan los requisitos para garantizar la exactitud, la organización y la corrección.

Se debe tener en cuenta que es de suma importancia evitar exponer a los usuarios a escenarios donde se presenten vulnerabilidades que puedan afectar el desempeño de esta tecnología, así como para minimizar el número de víctimas que pueden ser afectadas por un ataque, así como el poner en riesgo la integridad y seguridad de la empresa proveedora. Se concuerda que por más que se programen nuevos sistemas o medios de seguridad, considerando que siempre van a existir atacantes que podrán quebrantar la seguridad; por tanto, día a día deben diseñarse e implementarse nuevos métodos para fortalecer la seguridad de las redes inteligentes y con ello blindar las vulnerabilidades en los sistemas de medición de energía eléctrica para lograr crear una red segura e integra tanto para la empresa proveedora como para el consumidor final [60].

Las mejoras en funciones y privilegios AMI han dado como resultado una superficie más amplia para los ataques cibernéticos, lo que permite la explotación remota de estos dispositivos inteligentes sin ningún acceso físico. Por lo tanto, la privacidad y seguridad del consumidor se ha convertido en un problema crítico debido a la interconexión de diferentes dispositivos inteligentes en varias redes de comunicación y la información que llevan [61].

3.7 Referencias

[1]. MA. Faisal, Z. Aung, JR. Williams, A. Sanchez. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasi- bility study. IEEE Syst J;9(1):31–44, 2015.

[2]. DB. Rawat, C. Bajracharya. Cyber security for smart grid systems: status, challenges and perspectives. In: Proceedings of the SoutheastCon; p. 1–6, 2015.

[3]. M. Lehtonen, A. Ortiz, et al. “Evaluation of Energy Meters’ Accuracy Based on a Power Quality Test Platform,” En: Electric Power Components and Systems, vol. 35, no. 2, pp. 221–237, Feb. 2007.

[4]. National Energy Technology Laboratory for the U.S. Department of Energy. Advanced metering infrastructure, NETL modern grid strategy; 2008.

[5]. S. Magazine, P. Policy, S. Grid, NIST interoperability framework and action plans, in: IEEE Power and Energy Society General Meeting, 2010, pp. 1–4.

[6]. L. AlAbdulkarim, Z. Lukszo, Information security implementation difficulties in critical infrastructures: smart metering case, in: IEEE International Conference on Networking, Sensing and Control (ICNSC), Chicago, IL, pp. 715–720, 2010.

[7]. G. Lenzini, M. Oostdijk, W. Teeuw, B. Hulsebosch, M. Wegdam, N. Enschede, Trust, Security, and Privacy for the Advanced Metering Infrastructure, Novay/RS/2009/010, 2009.

[8]. C.-W. Ten, C.-C. Liu, M. Govindarasu, Vulnerability assessment of cybersecurity for scada systems using attack trees, in: IEEE Power Engineering Society General Meeting, Tampa, FL, pp. 1–8, 2007.

[9]. H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, D. Svetinovic,”Integrated smart grid systems security threat model”, Journal Information Systems, vol. 53, pp. 147-160, 2014.

[10]. C. W. Ten, C.-C. Liu, M. Govindarasu, “Cyber-vulnerability of power grid monitoring and control systems, in: Proceedings of the 4th ACM Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, ser. CSIIRW‘08, ACM, New York, NY, USA, , pp. 43:1–43:3, 2008

[11]. V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G. Hancke, “Smart grid technologies: communication technologies and standards IEEE Trans”. Ind. Inf., vol. 7 (4) pp. 529–539, 2011.

[12]. M. Qiu, W. Gao, M. Chen, J. Niu, L. Zhang,”Energy efficient security algorithm for power grid wide area monitoring system IEEE Trans”. Smart Grid, vol. 2 (4), pp. 715–723, 2011.

[13]. D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, An integrated security system of protecting smart grid against cyber-attacks, in: IEEE Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, pp. 1–7 2010.

[14]. G. Ericsson, “Cyber security and power system communication-essential parts of a smart grid infrastructure IEEE Trans.’ Power Deliv., vol. 5 (3), pp. 1501–1507, 2010.

[15]. D. Watts, “Security and vulnerability in electric power systems, in: 35th North American power symposium (NAPS)”, University of Missouri-Rolla, pp. 559–566, 2003.

[16]. R. Shein, “Security measures for advanced metering infrastructure components, in: IEEE Asia-Pacific Power and Energy Engineering Conference (APPEEC)”, Chengdu, pp. 1–3 2010.

[17]. H. Khurana, M. Hadley, N. Lu, D. Frincke Smart-grid security issues IEEE Secur. Priv., vol. 8 (1), pp. 81–85, 2010.

[18]. H. Suleiman, D. Svetinovic, Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure, in: Requirements Engineering, pp. 1–29, 2012.

[19]. F. Keblawi, D. SullivanApplying the common criteria in systems engineering IEEE Secur. Privacy, 4 (March–April (2)), pp. 50-55, 2006.

[20]. D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security ESORICS 2006, ser. Lecture Notes in Computer Science, vol. 4189, Springer, Berlin, Heidelberg,2006.

[21]. N. Zafar, E. Arnautovic, A. Diabat, D. SvetinovicSystem security requirements analysis: a smart grid case study Syst. Eng., 17 (1), pp. 77-88, 2014.

[22]. A. Chan, J. Zhou**On** smart grid cybersecurity standardization: issues of designing with nistir 7628 IEEE Commun. Mag., 51, pp. 58-65, 2013.

[23]. Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, “Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation,” IEEE Transactions on Power Systems, vol. 31, no. 6, pp. 4379–4394, 2016.

[24]. A. Stefanov, C.-C. Liu, M. Govindarasu, and S.-S. Wu, “SCADA modeling for performance and vulnerability assessment of integrated cyber-physical systems,” International Transactions on Electrical Energy Systems, vol. 25, no. 3, pp. 498–519, 2015

[25]. S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, “Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques,” in Proceedings of the 14th IEEE International Conference on Intelligence and Security Informatics, ISI 2015, pp. 25–30, USA, September 2016.

[26]. A. Mahmood, M. Aamir, M. Anis, Design and implementation of amr smart grid system, in: IEEE Canada Electric Power Conference (EPEC), Vancouver, BC, pp. 1–6, 2008.

[27]. H. Suleiman, D. Svetinovic, Security requirements analysis of smart grid advanced metering infrastructure: a case study using the SQUARE method, in: IEEE PES International Asia-Pacific Power and Energy Engineering Conference (APPEEC), Shanghai, China, IEEE, 2012.

[28]. H. Suleiman, D. Svetinovic, Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure, in: Requirements Engineering, pp. 1–29, 2012.

[29]. The Smart Grid Interoperability Panel Cyber Security Working Group, Introduction to NISTIR 7628, Guidelines for Smart Grid Cyber Security, 〈 http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf〉, September, 2010.

[30]. A. Chan, J. Zhou On smart grid cybersecurity standardization: issues of designing with nistir 7628 IEEE Commun. Mag., vol. 51 (1), pp. 58–65, 2013.

[31]. J. Kang, “Information privacy in cyberspace transactions”. Stanf. Law Rev. vol.50, pp.1193–1294, 1998

[32]. H., Wang, L., Sun, and E.Bertino, “Building access control policy model for privacy preserving and testing policy conflicting problems”, J. Comput. Syst. Sci., vol.80 (8), pp.1493–1503, 2014.

[33]. R. O. Mason, “Four ethical issues of the information age”. Mis Q. vol.10, pp. 5–12, 1986

[34]. H. J. Smith,” Managing privacy: information technology and corporate America”, UNC Press Books, Chapel Hill, 1994

[35]. E. F., Stone, H.G., Gueutal, D.G., Gardner and S.McClure,” A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations”, J. Appl. Psychol, Vol. 68(3), pp.459, 1983

[36]. N. S. Grid, “Guidelines for smart grid cyber security: vol. 2, privacy and the smart grid”. Guideline 2010.

[37]. Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS′09. ACM, New York, NY, USA, pp. 21–32, 2009.

[38]. A. W. Atamli and A. Martin, “Threat-based security analysis for the internet of things,” in Secure Internet of Things (SIoT), 2014 International Workshop on, pp. 35–43, IEEE, 2014.

[39]. Z. Lu, X. Lu, W. Wang, C. Wang, Review and evaluation of security threats on the communication networks in the smart grid, in: Military Communications Conference – MILCOM 2010, pp. 1830–1835, 2010.

[40]. Tarrant, “Ami global forecast: H1 2017”. https://www.greentechmedia.com/research/report/ami-global-forecast -2017-2021, 2017

[41]. X., Liao, P.,Srinivasan, D.,Formby and A.R.Beyah, “Di-prida: differentially private distributed load balancing control for the smart grid”. IEEE Trans. Dependable Secure Comput. 2017.

[42]. N., Saputro, K. Akkaya, “On preserving user privacy in smart grid advanced metering infrastructure applications”. Secur. Commun. Netw. Vol.7 (1), pp. 206–220, 2014

[43]. Hui Shi, J. L. h. Y. J. h. C. W. h. J. G. h. Y. D. h., h. “The new key-stream generator based on the ofb mode of aes”. Applied mechanics & materials, pp. (644-650), 2768-2771, 2014.

[44]. L. Zhongmin, “Design of Smart Home System Based on Zigbee Zhongmin LI1, Mao SONG and Lu GAO, 2014.

[45]. J. A. Bertolín. Identificación, análisis y evaluación de la seguridad enlas comunicaciones con tecnología zigbee, pp. 115-121, 2011.

[46]. W. P. R. S., N. Kangude. Advanced encryption standard. International journal of computer science engineering & technology. Vol. 1(3), pp. 5-10, 2011.

[47]. K. A. a. S. M. s. M. M. m. K. S. s., O. o. Barukab, Secure communication using symmetric and asymmetric cryptographic techniques.international journal of information engineering & electronic business. 4(1), pp.36-42, 6 -10, 2012.

[48]. Alliance, Z.-W. Z-wave technology comparation”. Web. Retrieved From http://z-wave.sigmadesigns.com/about z-wave#technology comparison pp. 8, 2015.

[49]. Circle. Survey: Energy security pros believe smart meters vulnerable to false data injection. Business wire (English). Survey, pp.8, 2014.
[50]. K. Sangani, “You’re being monitored”, Engineering & Technology (17509637)”, vol. 5(10), pp. 28-29, 2010.
[51]. D. Kundur, X. Feng, S. Liu, T. Zourntos, K.L. Butler-Purry, Towards a framework for cyber attack impact analysis of the electric smart grid. In: 2010 First IEEE International Conference on Smart Grid Communications, pp. 244–249, 2010.
[52]. B. Fouladi, S. G.”Security evaluation of the z-wave wireless protocol”, Research.sensepost.com. pp.10, 2014.
[53]. Chim, Y. S. L. V. O. H. L. C. Z. J., T. W. “Prga: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid”, IEEE Transactions On Dependable & Secure Computing, vol. 12(1), pp. 85-97, 10-15, 2015.
[54]. C. Díaz, J. Hernandez, “Smart Grid : Las TICs y la modernización de las redes de energía eléctrica - Estado del Arte.” En: Revista S&T, vol. 9, pp. 53–81, 2011.
[55]. H. Li, X. Lin, H. Yang, X. Liang, R. Lu, X. Shen, Eppdr: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. IEEE Trans. Parall. Distrib. Syst. 25(8), 2053–2064, 2014.
[56]. Silicon Laboratories, Inc. smart metering brings intelligence and connectivity to utilities, green energy and natural resource management. Rev.1.0. http://www.silabs.com/Support%20Documents/TechnicalDocs/Designing-Low-Power-Metering-Applications.pdf> accessed August, 2015.
[57]. BJ. Murrill, EC. Liu, Thompson II, RM. Smart Meter Data: Privacy and Cyber security. Congressional Research Service; 2012.
[58]. National Energy Technology Laboratory for the U.S. Department of Energy. Advanced metering infrastructure, NETL modern grid strategy; 2008.
[59]. H. Suleiman D. Svetinovic. Security Requirements Analysis of Smart Grid Advanced Metering Infrastructure: A Case Study Using the SQUARE Method,” IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC 2012), Shanghai, China, March 2012.
[60]. S, Shapsough F. Qatan, R. Aburukba , F, Aloul , A. Al Ali. Smart grid cyber security: challenges and solutions. In: Proceedings of the international conference on smart grid and clean energy technologies, pp. 170–5, 2015.
[61]. S. Desai, R. Alhadad, N. Chilamkurti. ”A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure” Cluster Computing, vol. 22, pp.43-69, 2018.

CAPÍTULO IV

MÉTODOS CRIPTOGRÁFICOS

El cifrado es una de las medidas defensivas con que cuenta cualquier tecnología de la información que desee proteger una instancia. Los algoritmos de cifrado definen transformaciones de datos que los usuarios no autorizados no pueden revertir con facilidad. Se tiene a disposición varios algoritmos para elegir, incluidos DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, RC4 de 128 bits, DESX, AES de 128 bits, AES de 192 bits y AES de 256 bits. Aunque ningún algoritmo único resulta idóneo para todas las situaciones, no obstante, se aplican los siguientes principios generales [1]:

- El cifrado seguro suele consumir más recursos de la CPU que un cifrado menos seguro.
- Las claves largas suelen producir un cifrado más seguro que las claves cortas.
- El cifrado asimétrico es más lento que el simétrico.
- Las contraseñas largas y complejas son más seguras que las contraseñas cortas.
- Por lo general, el cifrado simétrico se recomienda cuando la clave solo se almacena de forma local; el asimétrico se recomienda cuando las claves deben compartirse a través de la conexión.
- Si cifra una gran cantidad de datos, debe cifrar los datos con una clave simétrica y cifrar la clave simétrica con una clave asimétrica.

- Los datos cifrados no se pueden comprimir, pero los datos comprimidos se pueden cifrar. Si usa compresión, debe comprimir los datos antes de cifrarlos.

En este capítulo se aborda el diseño de un criptosistema con semilla caótica y clave simétrica. Se inicia con la descripción de los métodos: Mapeo logístico, Generador Congruencial Lineal y Mapeo de Bernoulli analizados para cifrado y descifrado de datos de consumo de energía eléctrica, se propone el acoplamiento de los dos primeros métodos para conformar un criptograma con bajos requerimientos computacionales, y con el mismo propósito se diseña un criptograma usando el método de Bernoulli mismos que serán evaluados para posteriormente ser implementados en un modelo físico.

4.1 Mapeo Logístico

Parte del proyecto de tesis se centra en el caso de la aplicación logística. Esta viene dada por la función unidimensional dependiente de un solo parámetro μ

$$x_{t+1} = \mu x_t(1 - x_t) \quad (1)$$

donde x Є (0; 1) y μ Є (0; 4)], de modo que al ser iterada a partir de un valor inicial x_0 se va generando una órbita o trayectoria {x1, x2, x3…} según el proceso

$$x_{t+1} = \mathrm{f}(\ x_t) = \mu x_t(1 - x_t)$$

La aplicación fue introducida por primera vez por Verhulst en 1845. Fue popularizada en un artículo de 1976 del físico May, como análoga en tiempo discreto a la ecuación diferencial logística para el crecimiento de una población. May, en su artículo, enfatizó que incluso aplicaciones no lineales simples pueden presentar dinámicas muy complejas [2], [3].

Una de sus aplicaciones, como ya se ha mencionado, es la de modelar el crecimiento de una población en un área cerrada. La densidad de población x_{n+1} en la generación n + 1 es proporcional a la densidad en la generación anterior x_n si x_n << 1 y por tanto la población crece. En cambio, si x_n ~ 1, el término (1 - x_n) << 1 y la población disminuye. El efecto conjunto de ambos factores junto con el valor del

parámetro son los que determinan la complejidad de la evolución de la población. El parámetro r representa la fertilidad y demás influencias externas.

El modelo describe en tiempos discretos la evolución de una población a partir del conocimiento de la misma en un instante inicial. La variable x_n es la fracción de individuos en un territorio (respecto de un n máximo que puede ser sustentado) a un tiempo dado. O sea, que el valor "0" representa la ausencia de población y el valor "1" la existencia de tantos individuos como sea posible. El modelo describiría el valor futuro de la población a partir del conocimiento del valor presente. En principio se multiplica la fracción de la población presente por una constante. Pero, además, para tener en cuenta el hecho de que, al haber más población, la competencia entre los individuos aumenta y la población crece con más dificultad, multiplica a la fracción poblacional por la diferencia entre 1 y el valor poblacional actual.

Sin embargo, pronto se dio cuenta de que el modelo presentaba una gran cantidad de soluciones según cual fuera el valor del parámetro que se utilizara, y que esas soluciones eran muy distintas entre sí. En efecto, en algunos casos la solución consistía en una compleja alternancia de valores que no convergían ni a valores estacionarios ni a soluciones periódicas.

El hecho de que la iteración del cálculo para distintos valores del parámetro μ condujese a soluciones complejas, que parecían aleatorias en su comportamiento pese a tratarse de un modelo determinista muy sencillo causó gran impacto a nivel científico, y fue uno de los detonantes del estudio de lo que se llamaría teoría del caos.

También ha sido usada como generador de números pseudo-aleatorios. En [4] se han realizado ciertos tests estadísticos sobre las series de números obtenidas de la aplicación logística. Han encontrado que la aplicación los pasa satisfactoriamente y por tanto posee muchas de las propiedades requeridas por un generador de números pseudo-aleatorios.

Según el valor que se le adjudique a "μ", se observan los siguientes comportamientos:

- Si 0 < μ <= 1 la población terminará desapareciendo independientemente del valor de la población inicial.
- Si 1 < μ <= 2 la población rápidamente tenderá al valor: μ-1/μ, independientemente del valor de la población inicial.
- Si 2 < μ<= 3 a la larga la población también se estabilizará en: μ-1/μ, pero previamente fluctuará en el entorno de ese valor. La tasa de convergencia es lineal, excepto para μ = 3, en que es muy lenta, menor que la lineal.
- Si 3 < μ <= 3.45 en casi todos los casos la población oscila siempre entre condiciones iniciales de la población se aproximará a oscilaciones permanentes entre los cuatro valores.
- Con μ entre 3.45 y 3.54 (aproximadamente), la población tendrá oscilaciones permanentes aproximándose a 4 valores.
- Si μ es ligeramente mayor de 3,54, la población oscilará entre 8 valores (16, luego 32, etc). La relación entre la longitud de los dos intervalos sucesivos de las bifurcaciones se aproxima a la constante de Feigenbaum δ = 4,669. Este comportamiento es un ejemplo de un período doble de bifurcación.
- Cerca de 3,57 es el inicio del caos, pero todavía hay ciertos rangos aislados de μ que muestran un comportamiento no caótico, estas son a veces llamadas islas de estabilidad. Por ejemplo, a partir de 1 + √8 (aproximadamente 3,83) existe una serie de parámetros r que muestran oscilación entre los tres valores, y para valores ligeramente más altos de r oscilación entre 6 valores, luego 12, etc.
- Además, si μ = 4, los valores dejan el intervalo (0,1) y divergen para casi todos los valores iniciales.

El diagrama de bifurcación con distintos valores en μ que se muestra en la figura 4.1, resume todos los comportamientos antes mencionados. El eje horizontal muestra los valores del parámetro μ, y el eje vertical muestra el valor x en el intervalo (0,1), además, el diagrama es un fractal [5].

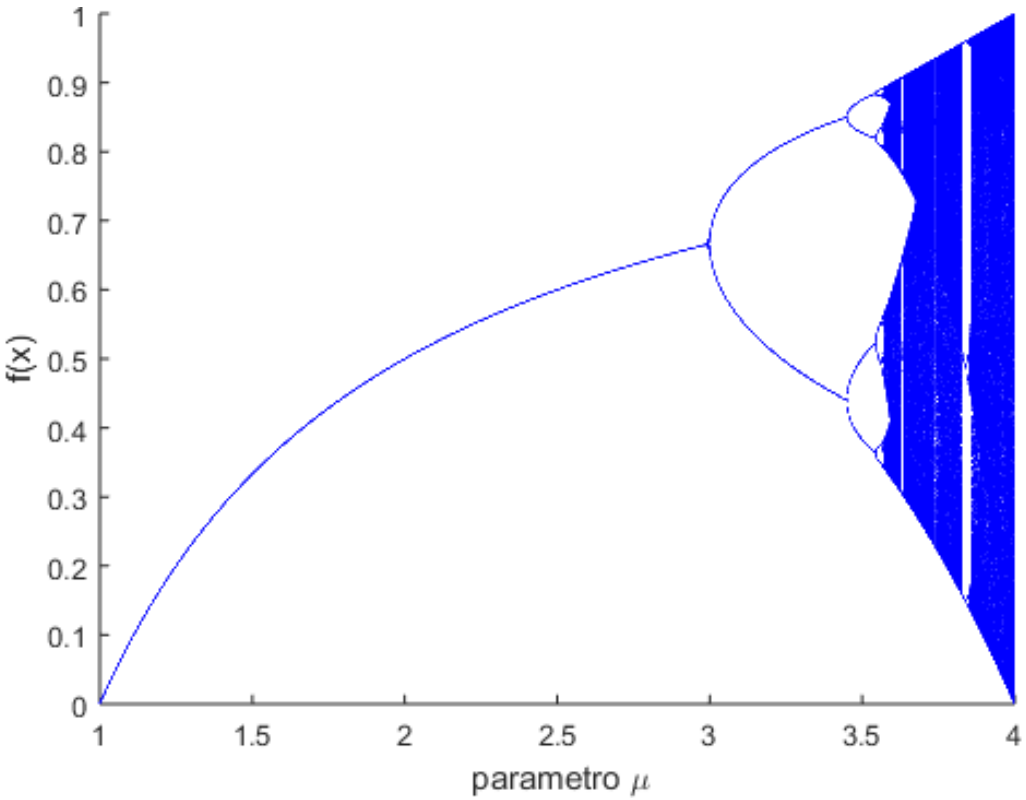


Figura 4.1 Diagrama de bifurcación

El gráfico del diagrama de bifurcación básicamente representa el valor de μ contra los puntos donde la dinámica se ha concentrado, después de algunas iteraciones iniciales. El primer paso abarca el fenómeno de los puntos fijos estables, en la parte comprendida entre μ=1 y μ=3, ésta presenta una dinámica simple, una situación estable en la que el proceso de iteración conduce siempre a un mismo punto para un valor fijo de μ.

El desarrollo de la teoría de caos y su status actual ha sido fruto en buena medida del uso de la computadora, una herramienta que ha modificado significativamente la manera de hacer la ciencia. Es tanta la importancia que ha cobrado la computadora que hasta la fecha han surgido dos ramas científicas: la matemática experimental y la física computacional, que se distinguen de la matemática y la física tradicionales en cuanto el apoyo que reciben de la computadora. En los últimos 20 años, el juego simbiótico entre la matemática experimental y la teórica ha provocado una revolución en nuestra comprensión de los sistemas dinámicos, en particular los sistemas caóticos.

La ecuación logística ha sido estudiada extensivamente por diversos autores. La investigación primaria de este tema se debe a autores tales como Feigenbaum [2] y May [3], Aun cuando denotemos con x_t a la población, en un contexto de ciencias biológicas, existen muchas disciplinas científicas donde se aplica esta ecuación fundamental. La siguiente es una lista parcial de aplicaciones de la ecuación logística:

Epidemiología: x_t es la fracción de la población infectada en el tiempo t.

Economía: modelación de la relación entre la cantidad de la mercancía y el precio: la teoría de los ciclos financieros, y las secuencias temporales generadas por diversas variables económicas.

Ingeniería: difusión de innovaciones.

Sociología: modelos de aprendizaje, donde X_t es el número de unidades de información que pueden recordarse después de un intervalo t; propagación de rumores en sociedades bien establecidas, donde x_t es el número de personas que han escuchado el rumor tras un tiempo t.

Economía: ciclos de negocios, crecimiento de mercados.

El modelo continuo está dado por la siguiente ecuación diferencial ordinaria:

$$\frac{dx}{dt} = \mu x$$

Para $\mu > 0$, la relación está indefinida para la dinámica poblacional.

Esta relación es la ecuación de crecimiento o decaimiento exponencial que se utiliza para estudiar la población, x_t, de cierta especie (biológica, química, etc.). En esta relación, t es el tiempo y x es una constante. La ecuación diferencial modela el sistema en tiempo continuo. En la práctica, se considera mejor la evolución del sistema en etapas discretas de tiempo. Cada etapa o paso podría ser una generación, o quizá una semana en la vida de la población.

Sin embargo, este sistema no es tan realista en el siglo pasado, [2] introdujo en esta ecuación un término que daba como resultado un modelo más exacto como

muestra en la ecuación 1, donde 1 es el límite de la población. Al escribir la ecuación de esta manera se hace una verificación de crecimiento/muerte. Esta relación, en la forma análoga de una ecuación de diferencias, conduce a una dinámica extremadamente compleja y eventualmente al caos [6].

En consecuencia, el tamaño de la población será un número que puede variar entre 0 y 1, es decir, x_t Є [0, 1]. Esta normalización de x_t permite la comparación de poblaciones diferentes. Por lo tanto, $x_t = 1$ representará la máxima población, y $x_t = 0.5$ será la mitad de la población. No importará el tipo de la población, lo mismo da si se trata de peces que de mariposas. Si x_t es mayor que 1, entonces x^i será negativo, lo cual no tiene significado para una dinámica poblacional. A esto se debe porqué el análisis se restringe al intervalo $0 < x < 1$. En resumen, la ecuación logística transforma un punto cualquiera en el intervalo unitario en otro punto dentro del mismo intervalo.

Por último, la ecuación logística, en la forma dada arriba, representa una familia de parábolas, con un parámetro de afinación o de control, el número real μ. En el análisis que realizaremos de la ecuación logística encontraremos que μ debe confinarse al intervalo cerrado (0, 4).

Los sistemas dinámicos discretos evolucionan en el tiempo por el proceso de iteración, en el que el siguiente estado del sistema viene determinado por su estado actual. El comportamiento de la función (1): bajo los parámetros de μ y x_t: cuando $0 <= \mu <= 4$, y $0 <= x_t <= 1$. La función es una parábola, la cual es iterada. $x_1 = f(x_0)$, $x_2 = f(x_1) = f2(x_0)$ ... $x_t = f(x_{t-1}) = ft(x_0)$, donde x_t, es la nueva iteración de x_0 y el conjunto de todas las iteraciones es el mapeo.

La forma de la curva representada por la ecuación logística es parabólica, cada punto de la curva tiene coordenadas (x_t* x_{t+1}), donde la abscisa es el valor de x_t, y la ordenada es el valor de x_{t+i} (f(x). La siguiente figura 4.2, muestra la gráfica de la ecuación logística para varios valores del parámetro μ. Naturalmente, la parábola tendrá un grado de curtosis que dependerá del valor del parámetro de control μ [7].

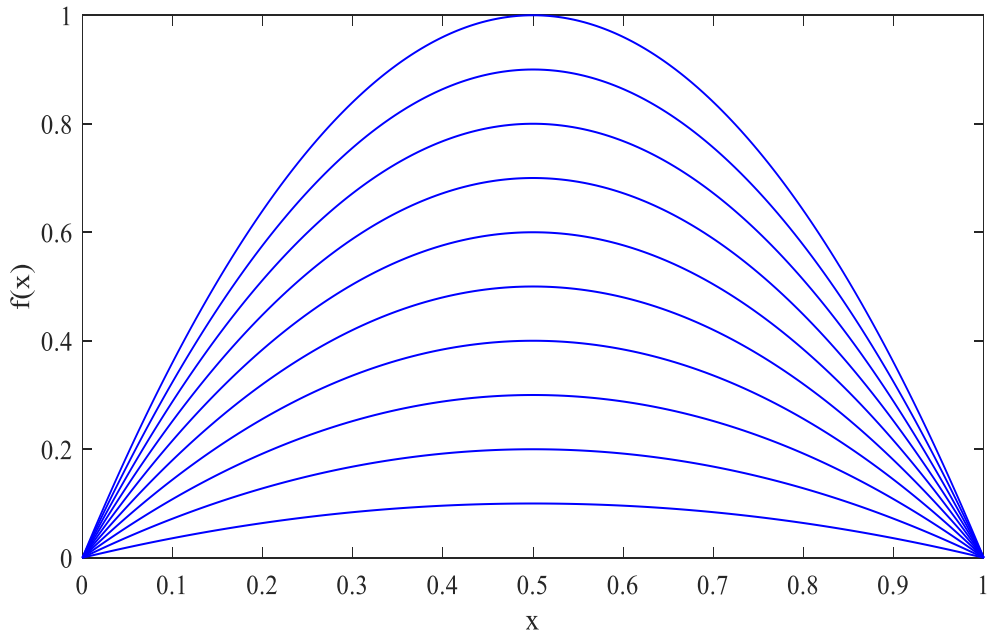


Figura 4.2 Familia de curvas de la ecuación logística para varios valores del parámetro μ.

La primera parte a presentar es la determinación gráfica de los puntos fijos de la ecuación logística. Por definición, los puntos fijos son aquellos para los cuales la expresión x = x + i es verdadera. Esta ecuación tiene como gráfica una recta de 45°, que inicia en el origen (0, 0). Utilizando esta definición, los puntos fijos, ya sean estables o inestables, se encuentran siguiendo un proceso iterativo: a partir del valor inicial x_t (valor semilla) se traza una recta vertical hasta la curva. Desde ese punto se dibuja luego una línea horizontal que intersecte la diagonal. Así se tendrá el valor x_1(que prácticamente es una nueva semilla). Estos pasos se repiten indefinidamente. El resultado de este procedimiento nos proporcionará un conjunto de valores de la variable, {x_i, x_j, X_2...}, es decir, obtendremos la órbita del sistema dinámico. La determinación de los puntos fijos se realizará observando precisamente el comportamiento asintótico de la órbita, es decir, nos interesa conocer [8],

$$\lim_{t\to\infty}\{(x_t)\} \tag{3}$$

Las siguientes figuras fueron obtenidas iterando la función logística un número determinado de veces (100), para diversos valores del parámetro μ, y para diferentes valores iniciales de x_t, con t = 0. Cada punto graficado corresponde al orden de la

iteración versus el valor de la función, (t, x_t). Tomando los parámetros iniciales para x= 0.7 y para μ = 0.4 se puede observar en la figura 4.3, que después de algunas iteraciones la dinámica se ubica en cero corroborando la existencia un punto fijo.

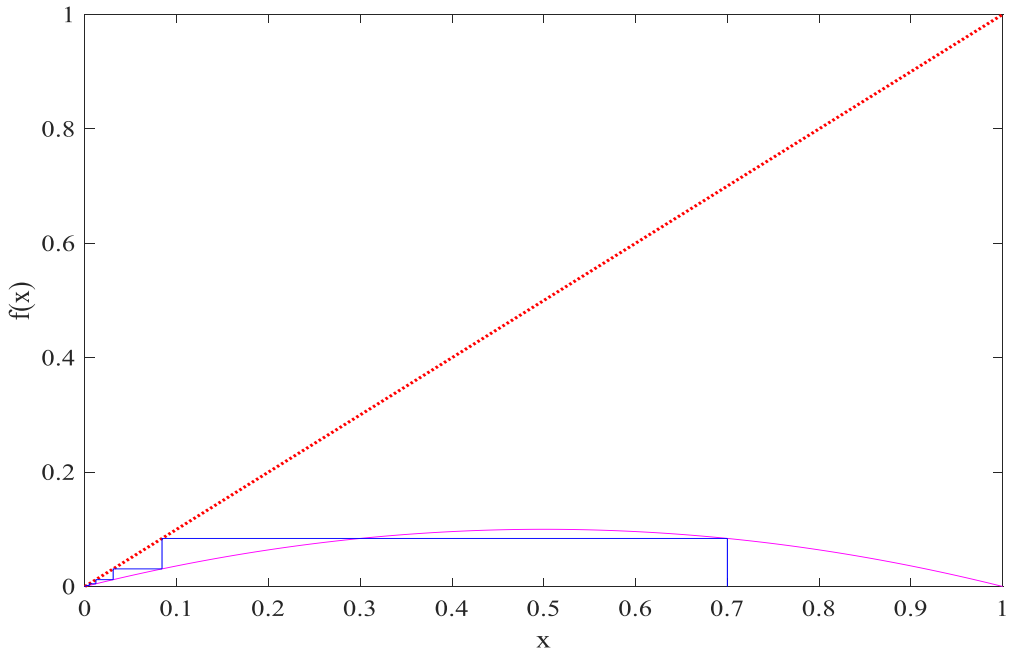


Figura 4.3 Iteración de la ecuación logística con μ=0.4 y x=0.7

Un examen de la figura nos lleva a concluir que el punto fijo 0 se alcanza sin importar el punto inicial o semilla.

Cuando el parámetro de control se incrementa hasta tomar un valor de 2, como se aprecia en la figura 4.4. Nuevamente, se presenta un valor fijo (además del caso trivial cero), que de hecho es 0.5833. Como se acaba de mencionar, el a tractor se alcanza sin importar el valor inicial, y esto se muestra en la figura siguiente (nótese que el número de iteraciones es de 100) [9]:

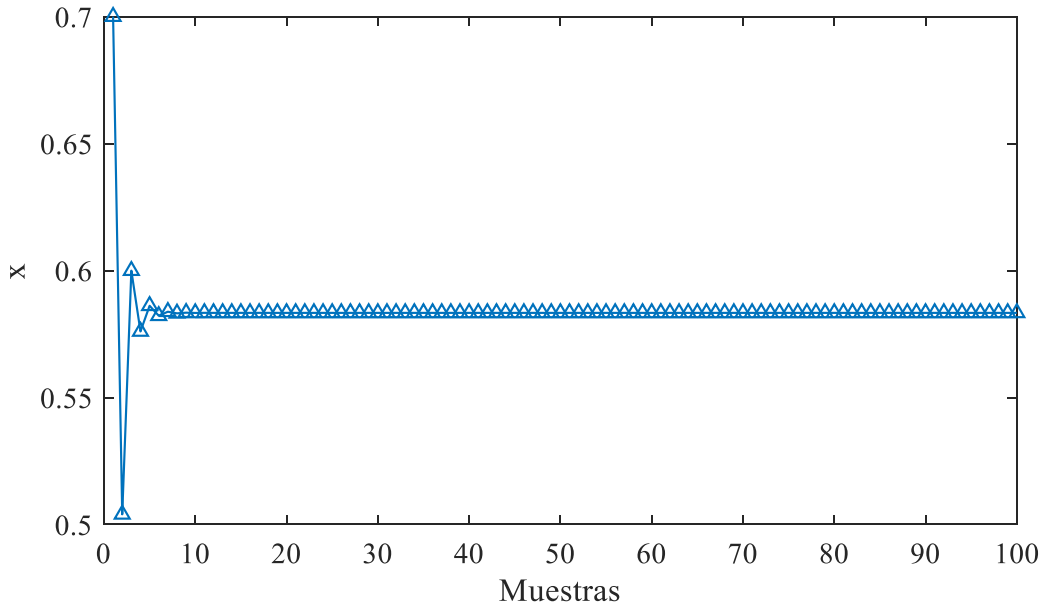


Figura 4.4 Punto atractor en ecuación logística con parámetros μ=2 y x=0.7

La obtención del punto fijo x = 0.5833 se puede observar igualmente en la parábola de la figura 4.5:

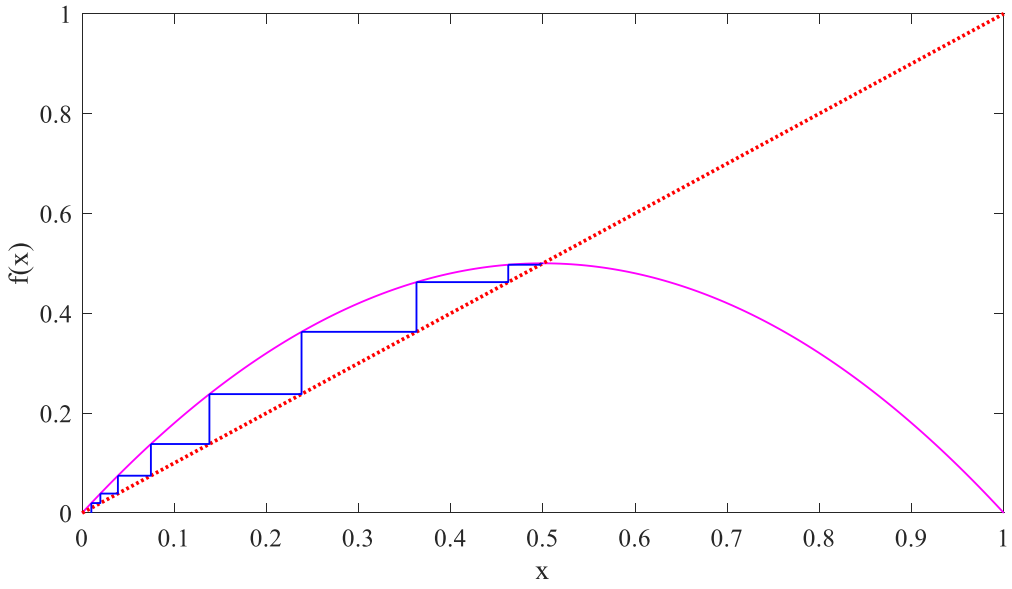


Figura 4.5 Iteración de la ecuación logística con μ=2 y x=0.58

El comportamiento de las órbitas es similar para valores de μ < 3.0, es decir, existe un solo atractor o punto fijo (exceptuando el cero). Sin embargo, para valores de μ > 3.0 (pero menores que 3.57), sucede algo inesperado: los valores de x^ no se establecen en un solo nivel. Por ejemplo, figura 4.6, para μ= 3.0 se tienen dos puntos

fijos. Decimos entonces que en μ = 3.0 existe un punto de bifurcación. Esto se muestra en las figuras siguientes, utilizando dos valores iniciales diferentes [10]:

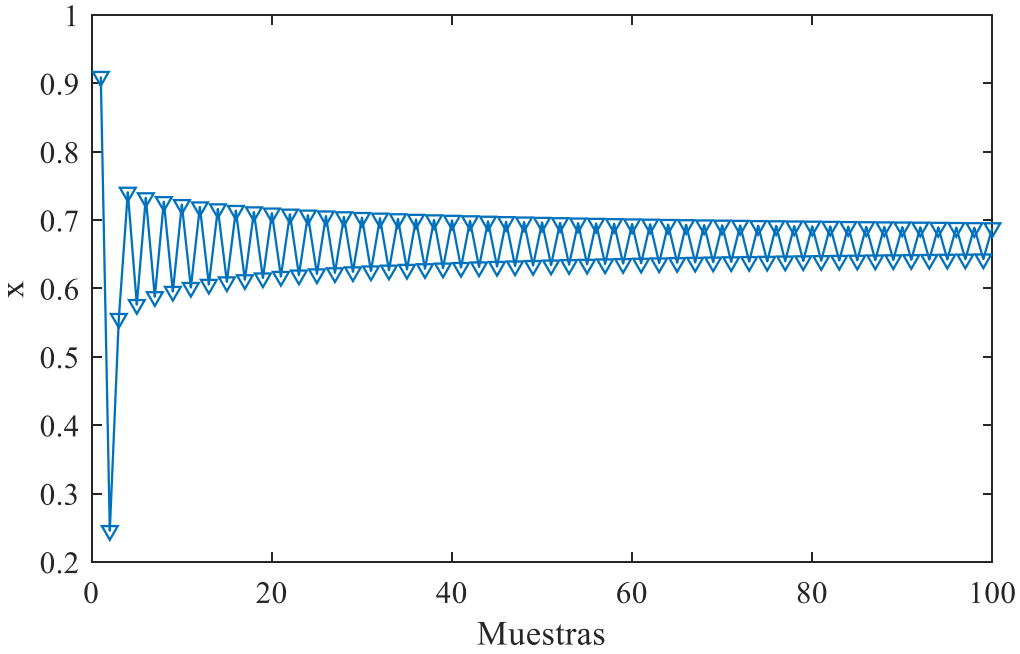


Figura 4.6 Puntos atractor en ecuación logística con parámetros μ=3.0 y x=.90

Siguiendo el procedimiento para encontrar los puntos fijos, se obtiene la siguiente figura 4.7, donde se muestra que cualquier valor semilla (exceptuando X = 0) será atraído hacia los dos puntos fijos con la misma energía:

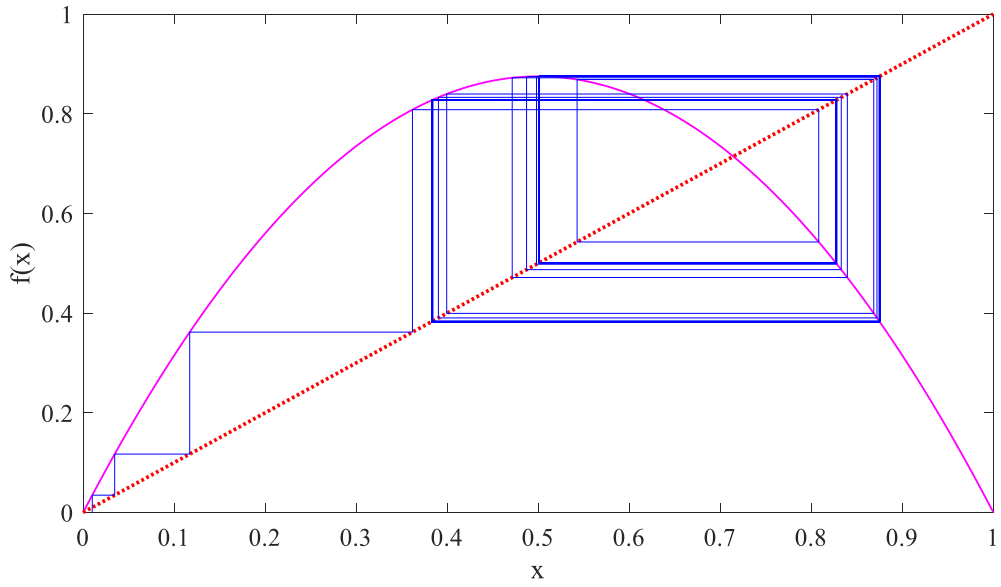


Figura 4.7 Iteración de la ecuación logística con μ=3.5 y x=.91

En los puntos de bifurcación, encontraremos que las iteraciones entran en ciclos de periodo armónico 2, 4, 8...»; 3, 6, 12 5. 10, 20 «; etc. (según el teorema de Sarkovskii,). Se habla entonces de la "duplicación del periodo". Si continuamos moviéndonos en el espacio de parámetros {μ_{ij}, encontraremos que la duplicación del periodo conduce finalmente al caos [11].

Para μ = 3.5, y x = 0.6, el sistema se estaciona en un ciclo de periodo cuatro, es decir, hay cuatro puntos fijos como se observa en la figura 4.8:

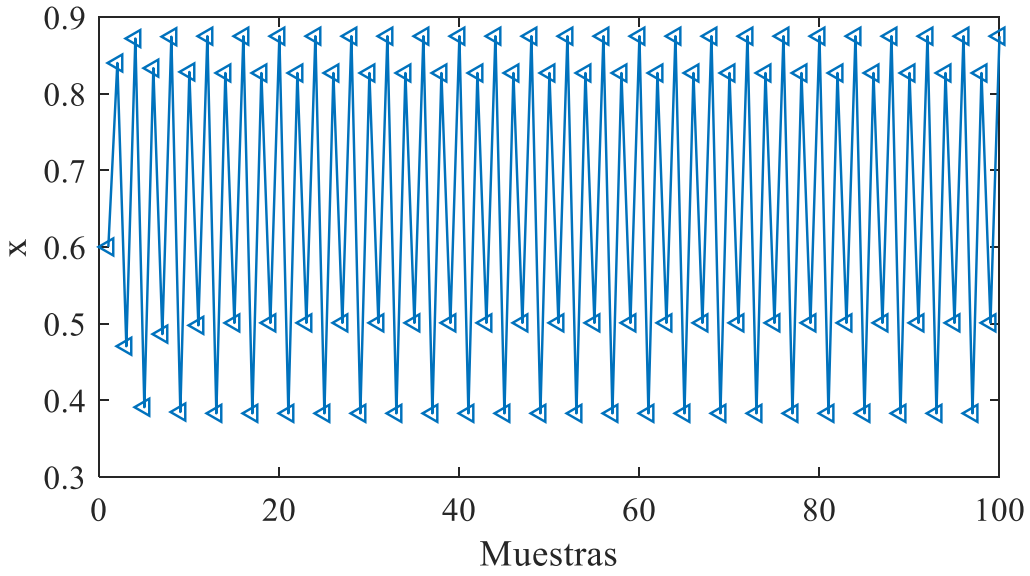


Figura 4.8 Punto atractor en ecuación logística con parámetros μ=3.5 y x=0.6

Para la figura anterior, se tienen cuatro valores fijos, a los cuales se llega en menos de 30 iteraciones, para luego repetirse indefinidamente:

0.38281968
0.82694070
0.50088421
0.87499726

Periodo cuatro.

0.38281968
0.82694070
0.50088421
0.87499726

En figura 4.9; donde μ = 3.57, aparece el estado caótico, la región caótica está entre μ = 3.57 y μ < 4. Es una región donde los X_t parecen estar aleatoriamente distribuidos dentro de la banda de valores (0, 1). La figura siguiente muestra la situación para μ = 3.57 y un valor inicial (irrelevante) de x= 0.1:

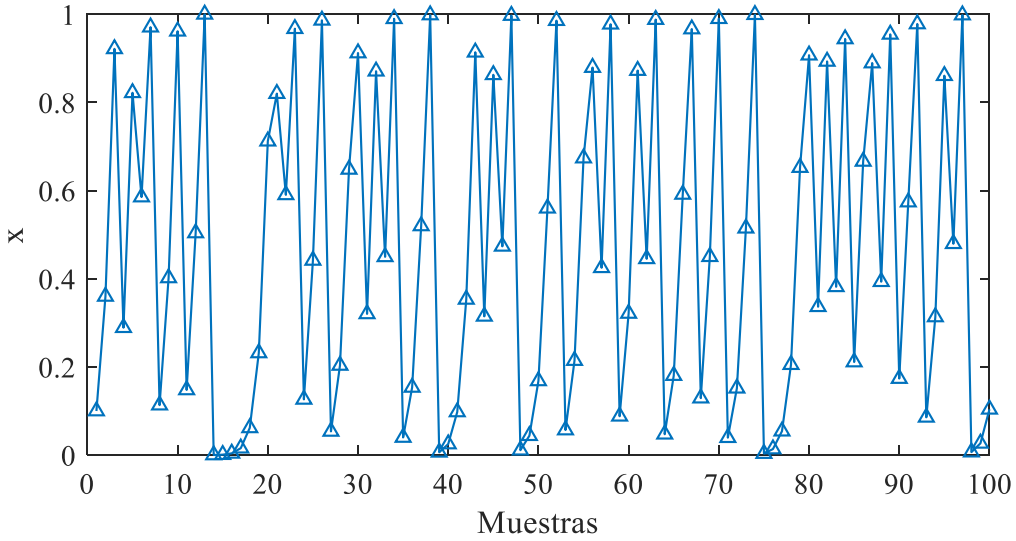


Figura 4.9 Punto atractor en ecuación logística con parámetros μ=3.57 y x=0.1

Es interesante notar el hecho de que el comportamiento de los valores x_t en la región caótica no es verdaderamente aleatorio. Por el contrario, es determinístico, en el sentido que se conoce una regla (la dinámica del sistema, en este caso la ecuación logística) con la cual exactamente los mismos valores de μ y x_t producen exactamente el mismo valor de x_t al cabo de un número dado de iteraciones. Por esta razón, a veces el fenómeno del caos se denomina caos determinístico [12].

Se muestra un ejemplo final en la figura 4.10, para un valor del parámetro μ superior a 3.57. Se proporcionan a continuación las gráficas de las órbitas y la parábola. Nótese que, en el caso de la parábola, el procedimiento para encontrar los puntos fijos no tiene terminación. Esto significa presencia de un "atractor extraño". Para el caso presente, μ = 3.86 y x_t = 0.32:

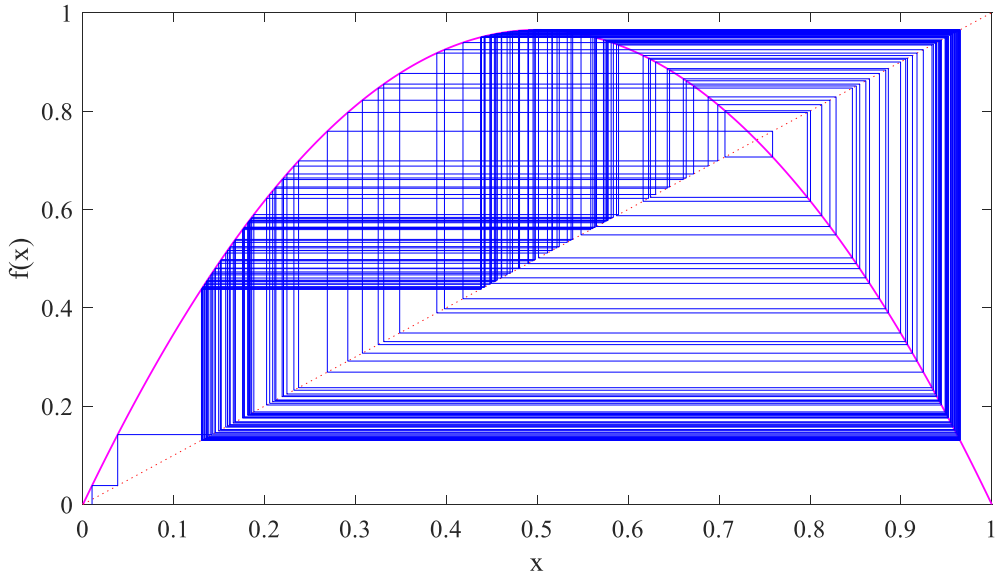


Figura 4.10 Iteración de la ecuación logística con μ = 3.86 y x = 0.32

El diagrama de bifurcaciones con estructura fractal que se muestra en la figura 4.11, es una herramienta que permite la visualización del comportamiento completo de un mapeo, es decir, proporciona una imagen del atractor extraño del sistema dinámico. El diagrama se construye explorando todo el espectro del parámetro de control μ. Computacionalmente, esto Implica partir de un valor inicial x_t y luego efectuar un proceso iterativo de la ecuación para todos los valores posibles de μ (se parte de μ = 0.0 y se incrementa en alguna cantidad pequeña, hasta que alcance el valor μ = 4.0).

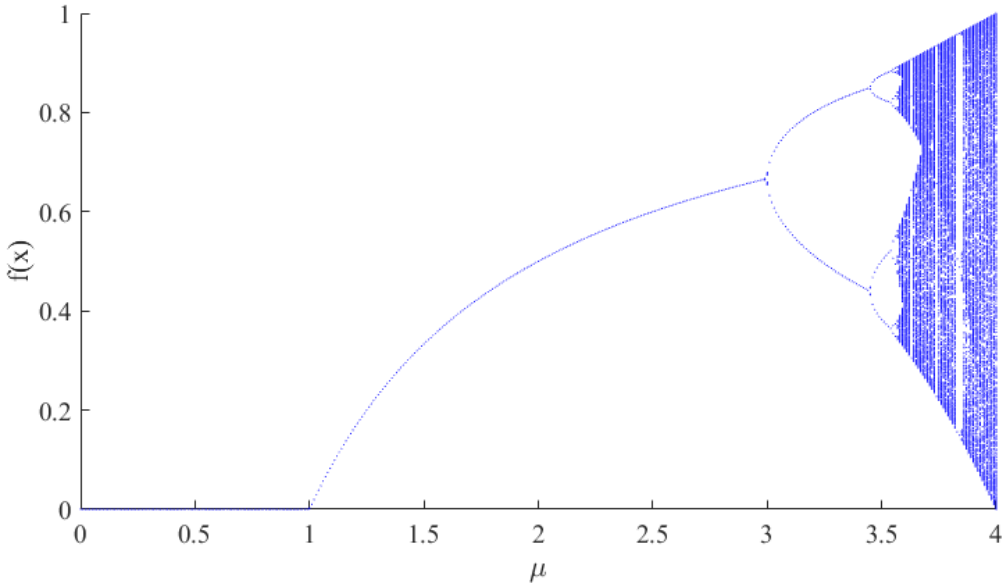


Figura 4.11 Diagrama con estructura fractal.

El diagrama de bifurcaciones posee una estructura fractal, como puede notarse en las siguientes figuras. La duplicación del periodo, es una de las varias rutas que existen que conducen al caos. Para la ecuación logística vimos que la región caótica se presenta en el subespacio del parámetro μ (3.57, 4). Sin embargo, Feigenbaum encontró que el valor crítico μ «3.57 no era exclusivo de la ecuación logística, y que más bien era compartido por cualquier mapeo unidimensional que presentara un solo pico.

El siguiente es un diagrama de bifurcaciones para mapeos unidimensionales que muestra la figura 4.12, donde para cada punto de bifurcación μ da lugar a dos ramas (duplicación del periodo).

Para determinar la densidad se puede utilizar la siguiente ecuación:

$$d_{n=}x_n*-0.5 \tag{4}$$

Esta ecuación da una medida de la distancia que existe entre un punto crítico x* y el punto fijo x = 0.5. Feigenbaum definió la razón de la distancia como sigue:

$$\alpha= \lim_{n\to\infty}\left(\frac{dn}{dn+1}\right) \tag{5}$$

y encontró el valor constante

$$\alpha = 2.502907875...$$

Otra constante universal descubierta por Feigenbaum está dada por la relación

$$\alpha = \lim_{n\to\infty}\left(\frac{An+1}{An+2}-\frac{An}{An}\right) \tag{6}$$

Con valor de α = 4.6692016091

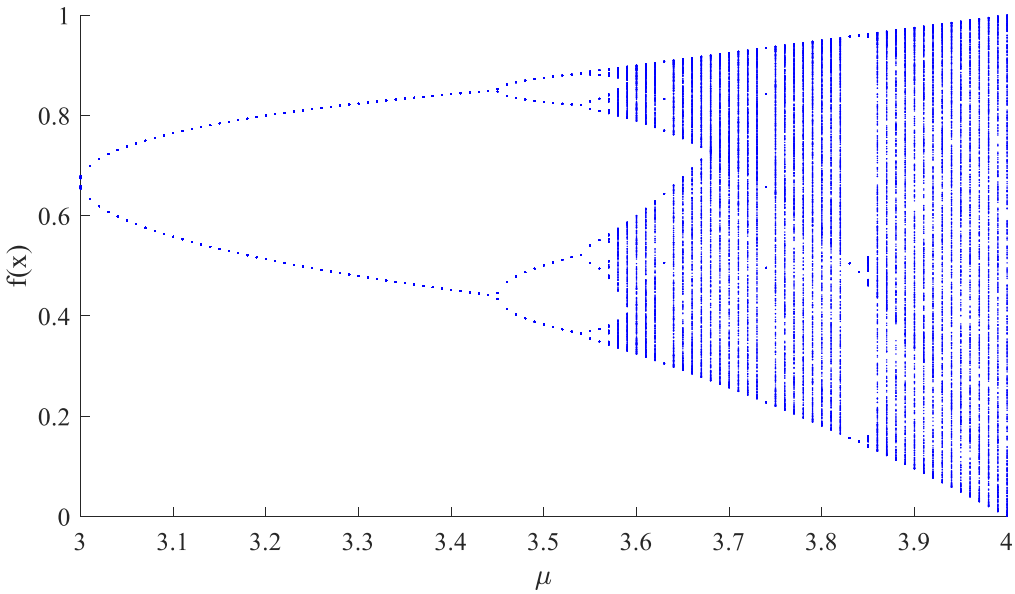


Figura 4.12 Duplicación de periodo.

A medida que se incrementa el valor de μ, aumenta la densidad de los puntos de bifurcación y de los puntos fijos.

Antes del advenimiento de los productos electrónicos, y con mayor razón de las computadoras, varios científicos famosos sabían que algunos sistemas dinámicos exhibían una gran sensibilidad a cambios pequeños en las condiciones iniciales. Cuando una causa muy pequeña determina un efecto considerable que no podemos ignorar, decimos entonces que este efecto es debido al azar. Si conociésemos las leyes de la Naturaleza y la situación del Universo en el instante inicial, podríamos predecir con exactitud la situación de este Universo en un instante ulterior. Pero aun cuando las leyes naturales no tuvieran más secretos para nosotros, no podríamos conocer la situación inicial más que aproximadamente.

Si esto nos permite prever la situación ulterior con la misma aproximación, es todo lo que necesitamos, decimos entonces que el fenómeno ha sido previsto, que es regido por las leyes. Pero no acaece siempre así, puede suceder que pequeñas diferencias en las condiciones iniciales engendren muy grandes en los fenómenos finales; un pequeño error sobre los primeros produciría un error enorme sobre los últimos. La predicción se ha vuelto imposible y nos encontramos con el fenómeno fortuito [13], [14].

La función logística es interesante porque reúne, en un solo sistema unidimensional y dependiente solo de un parámetro, un abanico de comportamientos diversos para las trayectorias x_t, cuando se varía el valor de $\boldsymbol{\mu}$ y/o $\boldsymbol{x_t}$. Se dice que sus características dinámicas son universales en ese sentido. Ejemplos de estos rasgos son la sensibilidad a las condiciones iniciales, la ruta al caos por duplicación de periodo o el fenómeno de la intermitencia.

Posteriormente se generan nuevas bifurcaciones que muestran un comportamiento caótico como el que puede observarse en la figura 4.13, donde se muestra la trayectoria de la señal cuya zona será aprovechada para generar los números impredecibles.

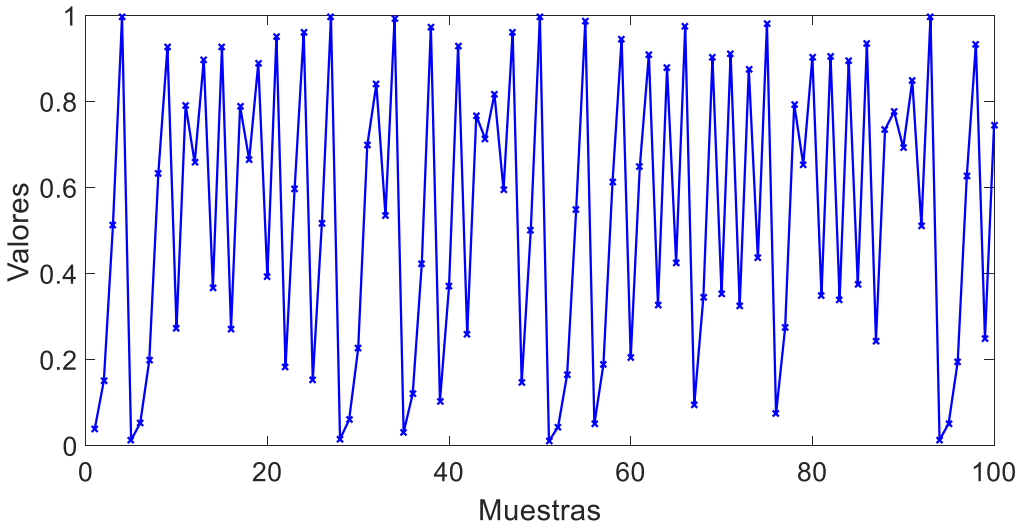


Figura 4.13 Diagrama de trayectoria de señal caótica con μ= 3.98

Para garantizar secuencias impredecibles, es necesario utilizar una semilla que se encuentre dentro de la zona en que el sistema se comporta de forma caótica. Por éste motivo se utilizarán los resultados obtenidos en donde se muestra el análisis dinámico de generadores caóticos, evaluándolos a través de los exponentes de Lyapunov, con el fin de delimitar el rango del parámetro que muestre un comportamiento impredecible, como se observa en el rectángulo a la derecha en la

figura 4.14A y puede apreciarse de forma más clara en la figura 4.14B.

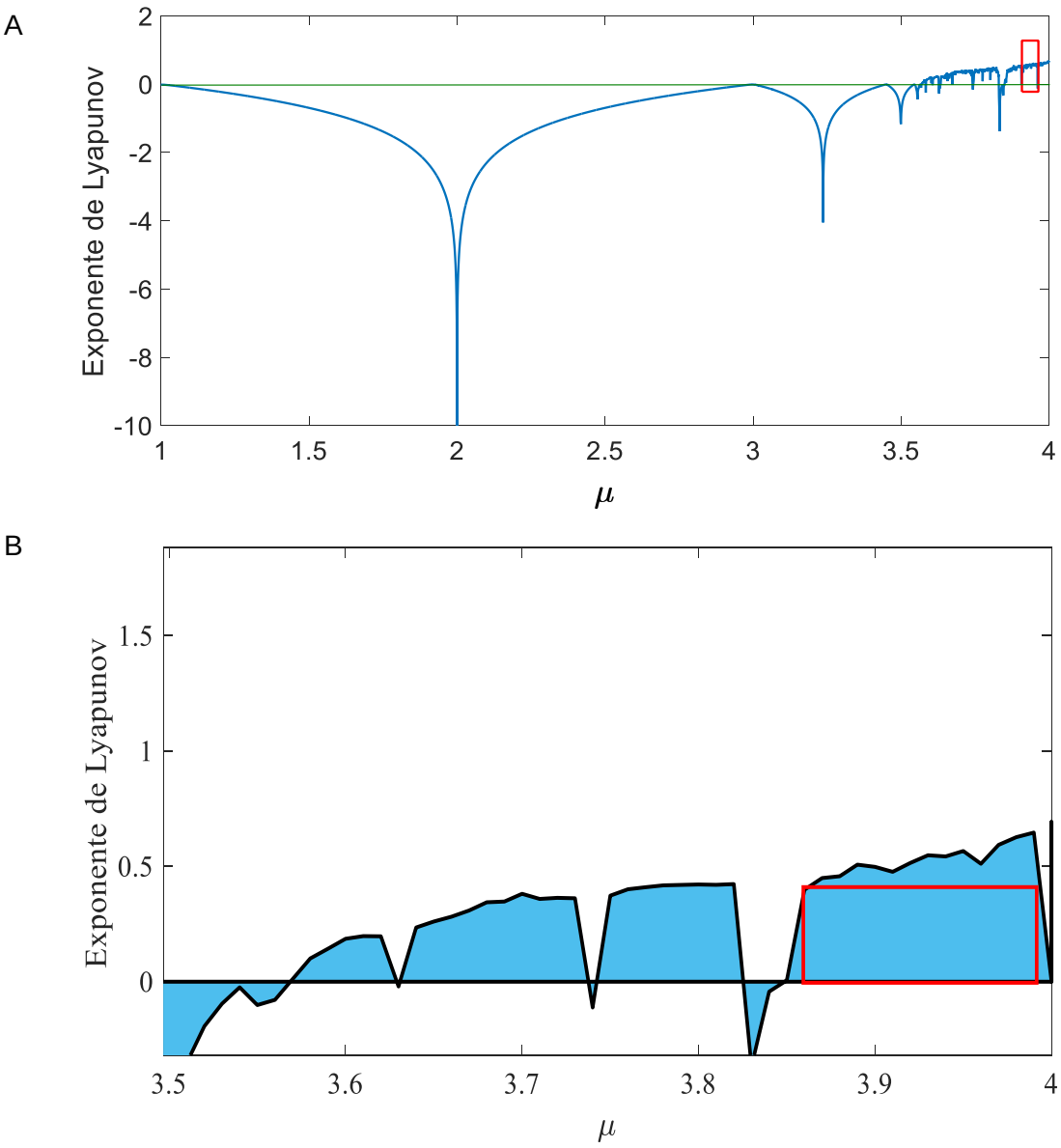


Figura 4.14 Diagramas de exponentes de Lyapunov. A) Área de caos. B) Acercamiento al área de comportamiento caótico

El exponente de Lyapunov cuantifica el grado de "sensibilidad a las condiciones iniciales" (es decir, la inestabilidad local en un espacio de estados) mediante la ecuación siguiente:

$$\lambda = \lim_{n\to\infty}\{\frac{1}{2}\sum_{i=0}^{n-1} ln|f'(x_i)|\} \quad (7)$$

Que puede definirse como el promedio del logaritmo natural del valor absoluto de las derivadas de la función del mapeo evaluadas en los puntos de la trayectoria [3], [15].

La tabla 1.4, muestra un resumen de los rangos seguros de los parámetros y las condiciones iniciales en los que la ecuación logística presenta y mantiene comportamiento caótico.

Tabla 1.4. Rangos seguros del parámetro y condiciones iniciales

Ecuación logística	Parámetro	Condición inicial
$x_{t+1} = \mu x_t(1 - x_t)$	$3.86 < \mu < 4$	$0 < X_t < 1$

Con este parámetro y condiciones iniciales se generan series de números que son utilizados como semilla para complementar la llave de cifrado aplicando la técnica de confusión que consiste en ocultar la relación entre la información original, la cifrada y la clave.

4.2 Generador Congruencial Lineal

La generación de números pseudo-aleatorios juega un papel crítico en gran número de aplicaciones tales como, simulaciones numéricas, las comunicaciones o la criptografía. Un generador de números pseudoaleatorios se define como un algoritmo que permite generar secuencias de números con algunas propiedades de aleatoriedad. Las principales ventajas de tales generadores son la rapidez y las sucesiones de números aleatorios con periodos máximos. En la práctica, la generación de números pseudo-aleatorios no es trivial y la calidad aleatoriedad de la secuencia producida puede ser esencial en la elección de la aplicación [16].

Los generadores de números pseudoaleatorios son de vital importancia en muchas aplicaciones criptográficas para la generación de claves y códigos de acceso. Uno de los generadores más antiguos y sencillos es el generador de

congruencia lineal, propuesto por D.H. Lehmer en 1949, que consiste en, a partir de un número inicial llamado semilla, generar una secuencia por recurrencia; cuya relación es: [14], [17]

$$X_{n+1} = (\mathrm{a}X_n + c)\ mod\ m \tag{7}$$

Donde debe tenerse en cuenta que los valores *a*, X_n y *c* tienen que ser mayores que cero. Y la variable *m*, tiene que ser un número primo suficientemente mayor que los tres anteriores.

Este tipo de generador es computacionalmente rápido y de fácil implementación; sin embargo, posee propiedades no tan ideales, como la producción de secuencias de valores que se repiten con un período máximo de es *m-1*, por otra parte, las secuencias producidas por un generador congruencial lineal son muy sensibles a cambios en sus parámetros, lo cual es una propiedad útil [18].

Los dos métodos descritos anteriormente se combinan en el diseño del algoritmo de cifrado propuesto, aprovechando las características principales de cada método. Dichas características son la velocidad de procesamiento y el bajo costo, en términos de recursos de hardware computacional requeridos.

El mapa logístico definido en la ecuación (1), localizada en el inicio del capítulo, muestra una alta sensibilidad a las condiciones iniciales, que se aplica para el ajuste de parámetros y para generar secuencias pseudoaleatorias, los valores de los parámetros se citan en los intervalos $x_t \in (0, 1)$ y $\mu \in (3.85, 4)$ para forzar la operación dentro de la zona caos [19]. Dentro de estos intervalos, junto con las condiciones iniciales, la ecuación logística (1) presenta y mantiene un comportamiento caótico; por lo tanto, se generan series de números y se utilizan como semillas caóticas para complementar la clave de cifrado mediante la aplicación de una "técnica de confusión". Esta técnica oculta las relaciones entre la información original, la cifrada y la clave generada.

Para obtener dos generadores de secuencia pseudoaleatorios, la función logística se itera con los siguientes parámetros y valores iniciales: $\mu = 3.89$ y $x0 = 0.00499$ para la primera secuencia y $\mu = 3.86$ y $x0 = 0.01999$ para la segunda secuencia. Se observa que para μ, se utilizan solo dos cifras significativas dado el

riesgo que implica usar más cifras por las características que se evidencian en el diagrama de bifurcación, que muestra ventanas en las zonas de caos. Estos valores se eligen, debido a su comportamiento caótico simulado y corroborado bajo sus métricas estadísticas, llenando todo el mapa generado con 125,000 iteraciones. Además, estos dos generadores de secuencia se comportan como parámetros del generador lineal congruente; por lo tanto, la mezcla generada es útil para cifrar señales de consumo de energía eléctrica.

En la figura 4.15A, se muestra el diagrama de flujo que contiene al algoritmo generador pseudoaleatorio, éste ilustra el flujo de los datos desde las condiciones iniciales de las variables que alimentan el método de mapeo logístico, la mezcla de estas secuencias con la señal de interés a través del operador de disyunción; hasta el momento de parada de cifrado.

La figura 4.15B muestra el algoritmo, evidenciando los datos de condiciones iniciales que alimentan las funciones de mapeo logístico y originan las secuencias utilizadas por el generador congruencial. Este diagrama representa el procedimiento seguido para generar dos secuencias (GNPR1 y GNPR2), a través de un mapa logístico unidimensional, ubicado los parámetros en una zona caótica, evaluada por los exponentes de Lyapunov. Estas secuencias se acoplan al generador congruencial para aumentar el nivel de aleatoriedad en las secuencias generadas [20]; para este trabajo de investigación, se cifra una señal de consumo de energía eléctrica a través del operador lógico de disyunción XOR; la señal cifrada fue simulada y físicamente implementada. Posteriormente, la información está totalmente encriptado y lista para ser enviada de forma inalámbrica a través de un canal probablemente inseguro.

Una vez que se reciben los datos enviados por el transmisor, estos deben ser descifrados con la clave de cifrado y el uso de un algoritmo de recuperación Figura 4.16. El receptor realiza la operación reversible para recuperar el mensaje de la señal recibida. Así los datos fusionados pueden ser regenerados; siendo el proceso de descifrado muy similar al cifrado, excepto porque se aplican los métodos de manera inversa como se muestra en la figura 4.16.

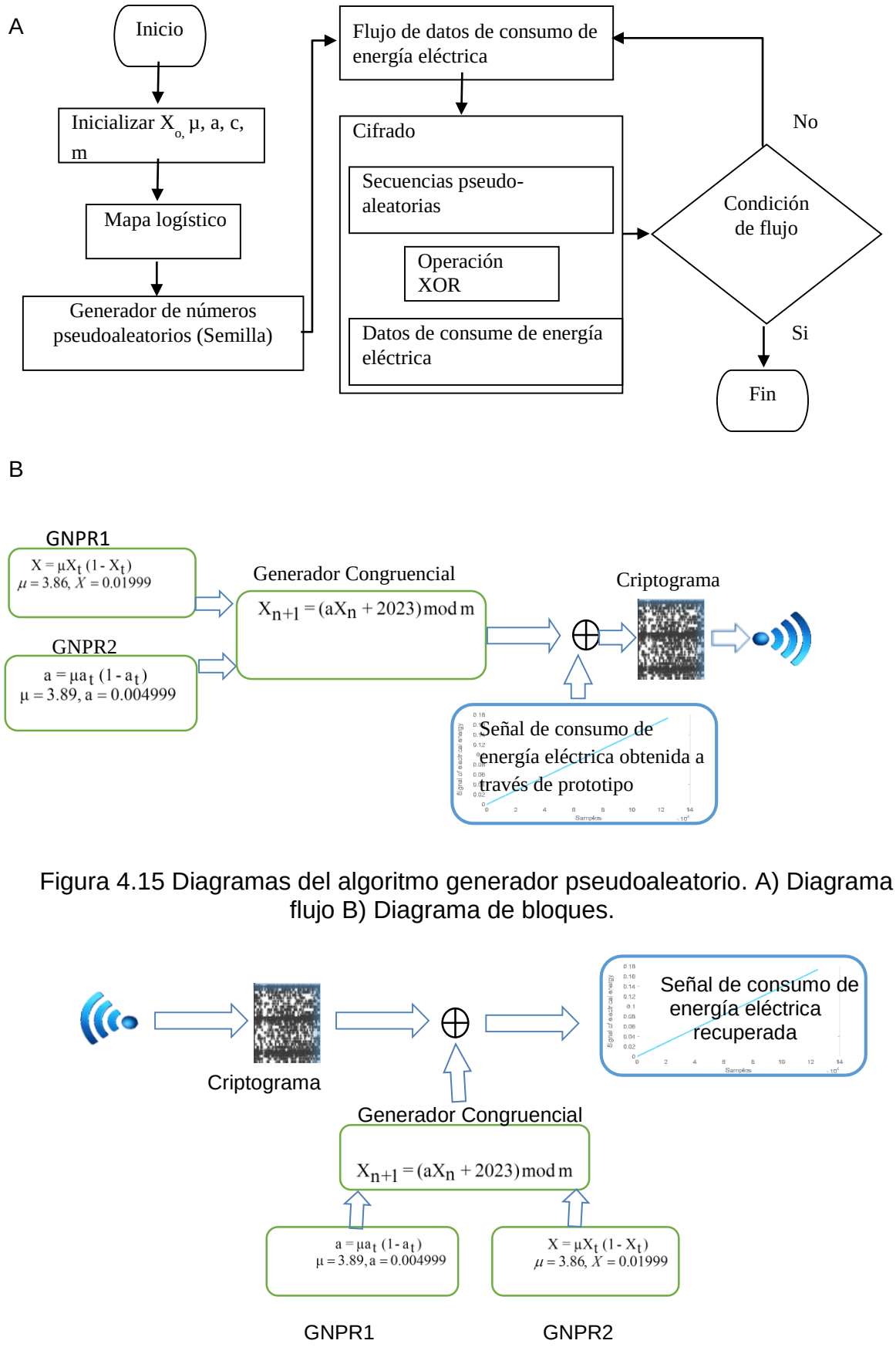


Figura 4.15 Diagramas del algoritmo generador pseudoaleatorio. A) Diagrama flujo B) Diagrama de bloques.

Figura 4.16 Diagrama de bloques: Algoritmo de recuperación de señal cifrada.

4.3 Mapa caótico Skew-Bernoulli

La función skew-Bernoulli es un sistema dinámico definido por la siguiente expresión:

$$\tau(\mu, x) = \begin{cases} \frac{x}{\mu}, & 0 < x \leq \mu \\ \\ \frac{-1+x}{1-\mu} + 1, & \mu < x \leq 1 \end{cases}, \qquad (8)$$

Donde μ es el parámetro de control, x en [0, 1]. La versión iterada de esta función es el mapa caótico Skew-Bernoulli [21], [22].

$$Xn = \tau^n(\mu, x_0) = \begin{cases} \frac{x_{n-1}}{\mu}, & 0 < x_{n-1} \leq \mu \\ \\ \frac{-1+x_{n-1}}{1-\mu} + 1, & \mu < x_{n-1} \leq 1 \end{cases}, \qquad (9)$$

donde x_n en [0,1], n = 0,1, ..., N-1 y x_0 es la condición inicial en el sistema dinámico; τ^n es la aplicación iterada de τ, n veces, a x_0. Usando la ecuación 9, se produce una secuencia de números reales con cardinalidad N: X (μ) = {x_0, x_1, x_2, x_3,... x_N}.

Observe que el mapa de Bernoulli de la figura 4.6, tiene un comportamiento caótico si 0 <μ <1 y no tiene una región estable. Este diagrama es una herramienta que muestra el comportamiento de todas las secuencias posibles que puede generar un mapa caótico específico en función de su parámetro de control, y no considera el transitorio de las secuencias. El diagrama de bifurcación representa un resumen de las funciones de distribución estadística de las secuencias numéricas generadas por el mapa caótico en función de μ. Ahora, para construir un diagrama de bifurcación, el mapa caótico se itera de acuerdo con la ecuación 2 considerando diferentes valores de μ [0, 1] con un paso incremental específico δμ. Un procedimiento simple que explica cómo construir un diagrama de bifurcación, evitando la transición de la secuencia generada, es el siguiente: (a) definir μ = 0.0,

(b) seleccionar aleatoriamente una condición inicial $x_0 \in [0, 1]$. El mapa caótico debe ser iterado N veces (por ejemplo, N = 1000) para calcular la secuencia $X(\mu) = \{x_0, x_1, x_2, \ldots, x_N\}$, (c) Los primeros 100 valores de la secuencia se descartan para garantizar que se ha excedido el transitorio, (d) se representan los valores restantes de las secuencias $\{x_1, x_2, x_3, \ldots, x_N\}$, (e) aumentar el valor de μ, es decir, $\mu = \mu + \delta\mu$ y el procedimiento se repetirá desde (b) hasta μ = 1.0 [23].

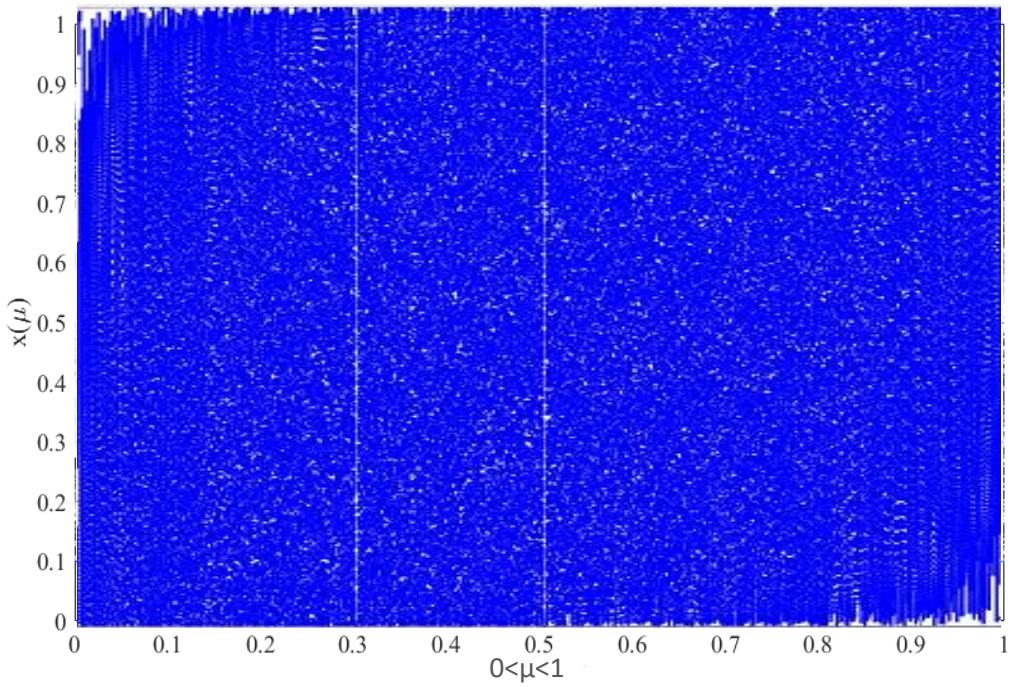


Figura 4.17 Diagrama de bifurcación producido por la ecuación 9 considerando μ [0, 1].

Si se utiliza un sistema caótico como generador de números pseudoaleatorios, debe evitarse el comportamiento periódico, ya que las propiedades estadísticas requeridas en el criptográfico se verán afectadas. En [24] se pueden discutir dos condiciones de captura en funciones caóticas que se encuentran en condiciones iniciales específicas: una de ellas colapsa el proceso caótico y se ha llamado trampa de anulación de caos (CAT), y la otra produce el mismo resultado y ha sido llamado caos de trampa fija (CFT). Estas condiciones de captura deben evitarse cuando se está diseñando un generador de números pseudoaleatorios. En este sentido, la característica determinante de cada punto fijo en el mapa caótico de Bernoulli debe especificarse tratando de establecer sus condiciones de captura.

De esta manera, se establece | ηn | = | τ n (μ, x0 + η0) - τ n (μ, x0) | la diferencia relativa entre dos secuencias producidas por el mapa de skew-Bernoulli usando x0 + η0 y x0 como dos condiciones iniciales, considerando que η0 es un número arbitrariamente pequeño y μ el parámetro de control del mapa de skew tend. Si | ηn + 1 | < |nn |, entonces τ converge para todos n. A la inversa, si | ηn + 1 | < |nn | entonces τ diverge n. Ahora, si estos casos se analizan cuando x0 es un punto fijo, las condiciones de captura pueden estimarse. Sea x0 = x* un punto fijo, y considerando que τ n (μ x *) = x* < n, la diferencia relativa ηn + 1 se puede escribir como,

$$|n_n + 1| = |\tau^n(\mu, x^* + n_0) - \tau^n\ (\mu, x^*)|$$

$$|\tau^n(\mu, x^* + n_0) - x^*)| \qquad (10)$$

Por la serie de Taylor,

$$|n_n + 1| = \left|\tau^n\left(\mu, x^* - n_n \frac{d\tau(\mu, x)}{dx}\Big|_{x^*} \quad | - x^*\right)\right|,$$

$\left|n_n \frac{d\tau(\mu,x)}{dx}\Big|_{x^*} \quad |, \right|,$

$$|n_n \tau'(\mu, x^*)| \qquad (11)$$

Por lo tanto, ηn + 1 <ηn se produce cuando τ '(μ, x*) <1 y x* es un punto fijo atractor, y ηn + 1> se produce cuando τ ' (μ, x *)> 1 y x * es un punto fijo repelente. Suponiendo que τ n (μ, x*) = x* se pueden calcular los puntos fijos del mapa de tienda. Estos puntos son x* = 0 y x* = 1 / (2 μ), y ambos son repelentes o puntos inestables en el sistema dinámico. Si se realizan algunas operaciones algebraicas, entonces se pueden calcular las condiciones para alcanzar los puntos fijos en el mapa de Bernoulli. Estas condiciones son x0 = 0, x0 = 1, x0 = μ, x0 = μ / (2- μ) y x0 = 1 / (2- μ). Además, si x0 = μ cuando k = 2, 3, 4. Se puede alcanzar el punto fijo x* = 0 después de algunas iteraciones en el mapa de Bernoulli. Así entonces, para cualquier valor de x0, donde μ = 1/2 también después de algunas iteraciones se alcanza el punto fijo x * = 0. En la figura 4.16 se muestra la ausencia de comportamiento caótico o bits en la región de caos que anula la trampa es evidente cuando x0 = μ, x0 = 1 / (2-μ) y cuando μ = 1/2. Esta condición se ratifica a diferentes

valores de x_0 cuando $\mu = 1/2$ [25]. Cada secuencia utilizada satisface la condición de no caer en un punto fijo y posibilita la obtención secuencias pseudoaleatorias.

En los sistemas criptográficos usados actualmente se hace necesario optar por generar números pseudoaleatorios, que sean criptográficamente fuertes y que no puedan ser previstos por un atacante. Estos números se usan generalmente para generar llaves de sesiones y su fortaleza es crítica para la calidad de los sistemas que dependan de ellos. Las secuencias generadas por mapas caóticos son candidatas para reemplazar a los generadores de números pseudoaleatorios, ya que su implementación en hardware es más sencilla porque se basan en ecuaciones simples con alguna no linealidad. Motivo por el cual en esta investigación se hace uso del modelo de mapeo caótico de Bernoulli.

En esta sección se plantea un algoritmo de generación de secuencias pseudoaleatorias a través de un sistema de ecuaciones que resultan de un proceso determinista de retroalimentación basado en el modelo de mapa de Bernoulli, con el propósito de utilizarlo en el proceso de difusión y confusión para cifrado y descifrado de señales de consumo de energía eléctrica, obtenidas mediante un modelo de simulación de medición del consumo energía eléctrica. El modelo de mapa de Bernoulli, ha sido elegido por sus propiedades criptográficas, que incluyen una alta sensibilidad a las condiciones iniciales y ergodicidad del sistema.

El criptograma propuesto es un sistema alimentado con tres funciones caóticas independientes con alta sensibilidad a las condiciones iniciales, cumple con los requisitos fundamentales criptográficos de confusión, difusión, y aleatoriedad. El modelo de mapa de Bernoulli, representado por las ecuaciones (8) y (9), se utiliza para generar secuencias que simulan comportamiento caótico, puede comprobarse que se aumenta las propiedades de aleatoriedad al llenar todo el plano en el diagrama de bifurcación (figura 4.16) a excepción de las condiciones detectadas donde ocurre el estado de equilibrio existiendo puntos atractores que anulan el comportamiento pseudoaleatorio, mostrando ventanas que aparecen en el mapa iterado posibilitando estabilidad en esas zonas.

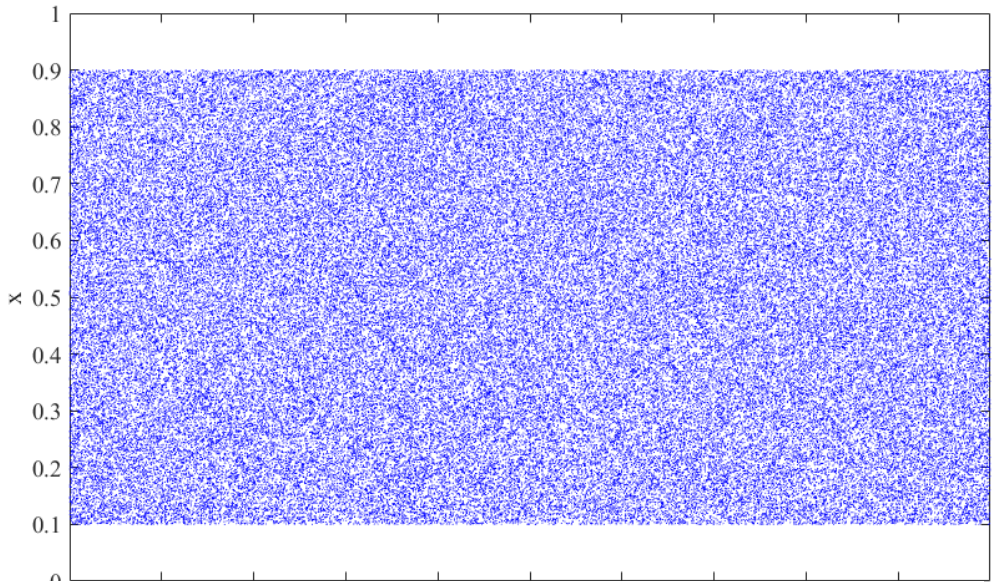
Bajo el manifiesto previo se hace uso de la versión iterativa (ecuación 8), para generar secuencias pseudoaleatorias exceptuando las condiciones de estabilidad,

primeramente se toma el parámetro μ>x_0 , para x_0=x_0/μ y posteriormente μ<x_0 , para x_0= ((x_0-1)/(1-μ))+1; con el propósito de obtener tres generadores de secuencias pseudoaleatorias. Los parámetros y valores de las condiciones iniciales que son utilizados para la ecuación son: $\mu = 0.596 \;\; y \;\; x_0 = 0.234$, $\mu = 0.369 \, y \, x_0 = 0.708$ y $\mu = 0.659 \, y \;\; x_0 = 0.123$. Dichos valores son elegidos teniendo en cuenta que manifiestan comportamiento aperiódico como se observa en la figura 4.17 (A, B y C) donde se muestran los mapas generados con 100,000 iteraciones evitando las condiciones donde se anula el comportamiento pseudoaleatorio.

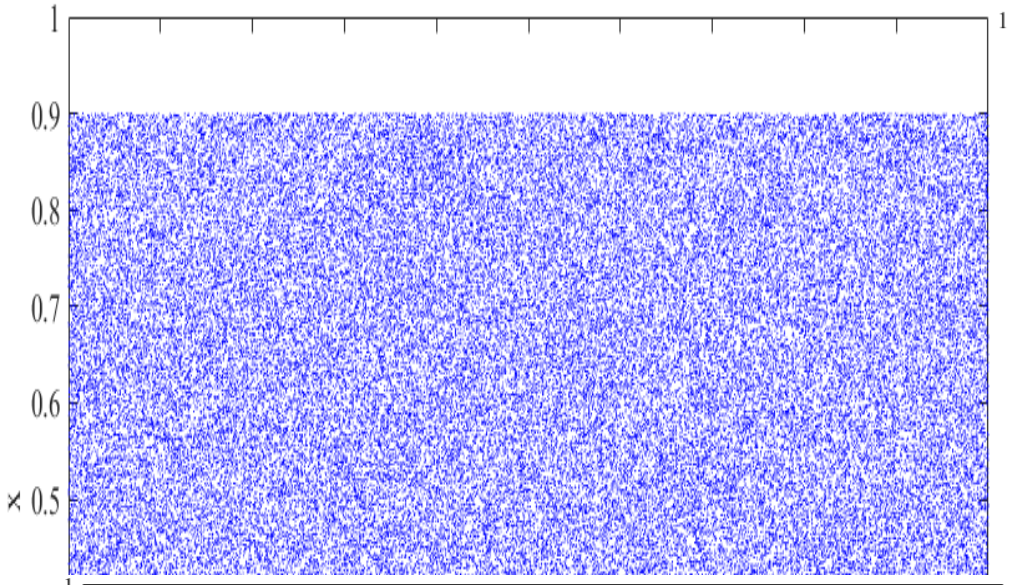
Con las características y cualidades que muestra los mapas son ideales para ser utilizadas en la criptografía ya que puede conseguirse una señal con características de aleatoriedad altas, al combinar los tres generadores de secuencias bajo la función de disyunción exclusiva Xor con el fin de que esta mezcla generada sea útil para cifrar una señal de consumo de energía eléctrica.

A continuación, se muestra el diagrama a bloques en la figura 4.18, que ilustra la mezcla de las ecuaciones generadoras de secuencias pseudoaleatorias para formar la señal de interés con características altas de aleatoriedad que cifrara la información de la señal de consumo de energía eléctrica. Inspirado por el procedimiento que se lleva a cabo en el algoritmo de cifrado de señal telefónica A5 (GSM), que funciona como cifrador de flujo de datos, y el flujo cifrado se consigue por medio de la operación Xor de tres registros usado para proporcionar privacidad en la comunicación al aire libre los registros utilizados en A5/1 usa 3 registros lineales de desplazamiento con retroalimentación (LFSR).

A


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
x

B


1
0.9
0.8
0.7
0.6
0.5
x

C

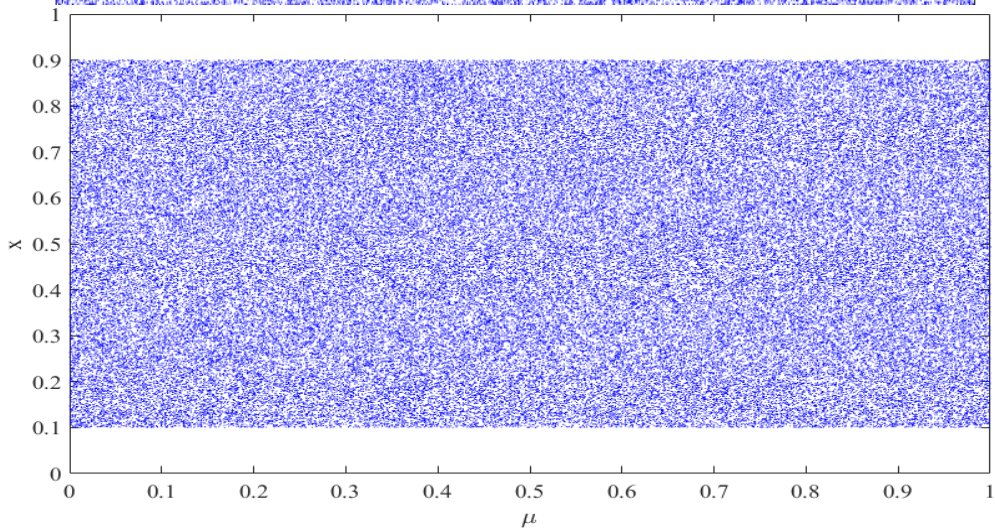

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
x
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
μ

Figura 4.18 Parámetros y condiciones iniciales $(A)\mu = 0.596\ y\ x_0 = 0.234$; $(B)\mu = 0.369\ y\ x_0 = 0.708 \quad (C)\mu = 0.659\ y\ \ x_0 = 0.123$

En este caso de investigación se reemplaza el uso de registros de desplazamiento con retroalimentación lineal (LFSR) por las ecuaciones generadoras secuencias pseudoaleatorias de Skew-Bernoulli Map.

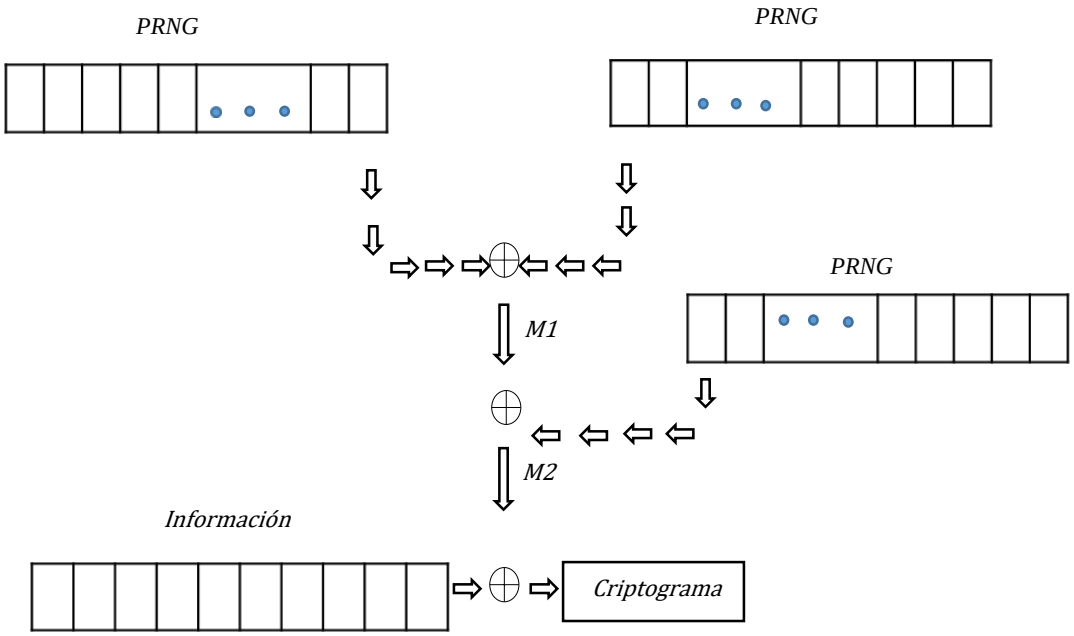


Figura 4.19 Diagrama a bloques del algoritmo de cifrado.

En el algoritmo que muestra la figura 4.19, se combinan dos generadores de secuencias pseudoaleatorias PGRN1 y PGRN2 mezclando bit a bit cada secuencia por medio de la función de disyunción exclusiva Xor, posteriormente la secuencia resultante M1 es combinada a su vez con un tercer generador de secuencias pseudoaleatorias PGRN3 bajo la misma operación lógica; la secuencia obtenida finalmente M2 es mezclada con la señal de consumo de energía eléctrica a cifrar. Cada uno de los registros es alimentado en respuesta a cada iteración de los generadores de secuencias pseudoaleatorias.

Representado algebraicamente dicho proceso bajo la siguiente expresión:

Criptograma=$[(PRNG1'PRNG2 + PRNG1PRNG2') + (M1'PRNG3 + PRNG3M') + (M2'Información + Información'M2)]$

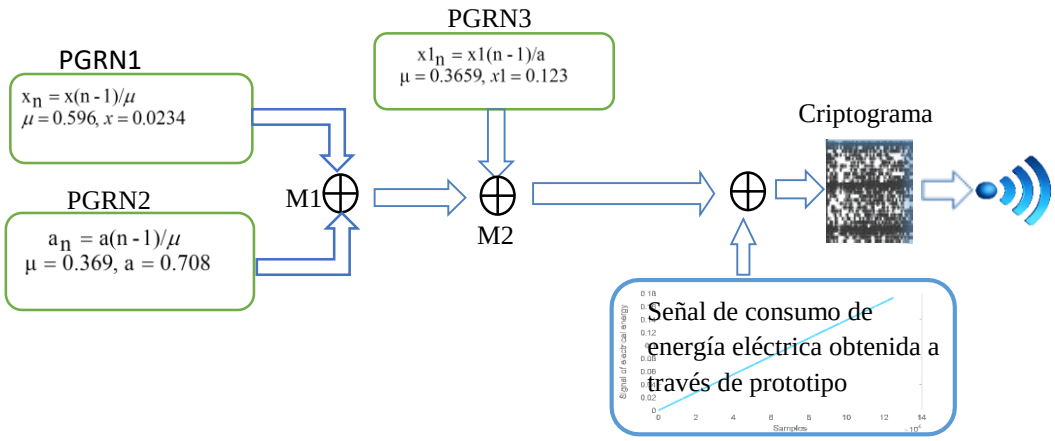


Figura 4. 20 Diagrama de bloques: Algoritmo cifrado de señal con Bernoulli.

El proceso de descifrado es muy similar al mostrado en la figura 4.19, no obstante, en este caso la señal cifrada es utilizada para realizar la mezcla con la secuencia de los generadores pseudoaleatorios a través de la operación lógica Xor recuperando nuevamente la señal original. Vale la pena señalar que el sistema de generadores pseudoaleatorios utilizado para el descifrado, debe estar perfectamente sincronizado con las condiciones iniciales mencionadas anteriormente, para lograr el descifrado sin pérdida de datos.

4.4 Referencias

[1]. Zhen Qin, Erqiang Zhou, Yi Ding, Yang Zhao, Fuhu Deng and Hu Xiong. Data Service Outsourcing and Privacy Protection in Mobile Internet, Data Service Outsourcing and Privacy Protection in Mobile Internet, IntechOpen, DOI: 10.5772/intechopen.79903, 2018.

[2]. B. Rajan and PA. Saumitr. Novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system. IEEE Transactions on circuits and system (4) pp. I- 53, 2006.

[3]. D. Xiao, X. Liao and P. Wei. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons & Fractals, 40 (5) (2009), pp. 2191-2199, 2009.

[4]. D. Xiao and F. Shih. Using the self-synchronizing method to improve security of the multi chaotic systems-based image encryption. Optics Communications Optar. Commun., 283 (15) pp. 3.030 a 3036, 2010.

[5]. Y. Zhang and D. Xiao. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Optar. Los láseres Eng., 51 (4), pp. 472-480, 2013.

[6]. M. Jiménez, F. Flores, and G. González. System for Information Encryption Implementing Several Chaotic Orbits.Ingeniería, Investigación y Tecnología, 16(3), 335-343, 2015.

[7]. A. Radwan, S. AbdElHaleem and S. Abd-El-Hafiz . Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. Journal of Advanced Research. 7(2), 193–208, 2016.

[8]. E. Yavuz, R. Yazıcı, M. Kasapbaşı & E. Yamaç. A chaos-based image encryption algorithm with simple logical functions. August 2016, Pages 471–483, 2017.

[9]. R. Ye. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications, 284(22), pp.5290-5298, 2011

[10]. R. Martínez-González, J. Díaz-Méndez, L. Palacios-Luengas, J. López-Hernández, and R. Vázquez-Medina. A steganographic method using Bernoulli's chaotic maps. Computers & Electrical Engineering. Vol 54, pp. 435-449, 2015.

[11]. G.A. Sathishkumar and D.N. Sriraam. Image encryption based on diffusion and multiple chaotic maps. arXiv preprint arXiv:1103.3792, 2011.

[12]. C. Liew, R. Shaw, L. Li and Y. Yang. Survey on Biometric Data Security and Chaotic Encryption Strategy with Bernoulli Mapping. 2014 International Conference on Medical Biometrics, pp. 174-180, 2014.

[13]. López-Hernández, J. Vázquez-Medina, R., Ortiz-Moctezuma, M. Digital Implementation of a Pseudo-Random Noise Generator using Chaotic Maps. IFAC Proceedings Volumes 45 (12), pp. 209–214, 2012.

[14]. Miyazaki, Y., Tsuneda, A., and Inoue, T. Spreading Sequences with Negative Auto-correlations Generated by LFSRs Based on Chaos Theory of Modulo-2 Added Sequences.In ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications, pp. 541-544, 2008.

[15]. López-Hernández, J., Díaz-Méndez, A., Del-Río-Correa, J., Cruz-Irisson, M. and Vázquez-Medina, R. A current mode CMOS noise generator using multiple Bernoulli maps. Microelectronic Engineering, 90, pp.163-167, 2012.

[16]. Zia. Ur Rahman. GSM Technology: Architecture, Security and Future Challenges. International Journal of Science Engineering and Advance Technology, vol. 5, pp. 70-74, 2017.

[17]. E. Barkan, E. Biham and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, CRYPTO 2003, pp.600–616, 2003.

[18]. National Institute of Standards and Technology. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" Revision 1, Special Publication 800-22. Revised Enero 2016.

[19]. A. Rezk, A. Madian, A. Radwan and A. Soliman, "Reconfigurable Chaotic Pseudo Random Number Generator based on FPGA," AEU - International Journal of Electronics and Communications, 2018.

[20]. C. Robinson, "Dynamical Systems," Boca Raton, Fla.CRC Press, 2009.

[21]. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, and I. Pitas, Statistical analysis of a watermarking system based on Bernoulli chaotic sequences, Signal Processing, vol. 81, pp. 1273-1293, 2001.

[22]. Alexander JC, Zagier D: The entropy of a certain infinitely convolved Bernoulli measure, J. London Math. Soc., (2) 44, pp.121-134,1991

[23]. S.H. Strogatz, Nonlinear δynamics and ψhaos: With αpplications to physics, biology, chemistry and engineering, Perseus Books Group, 2001.

[24]. S.V. Kartalopouols, Next Generation Intelligent Optical: Networks: From Acces to Backbone, Springer, 2008

[25]. C. Shashikala, & A. Jadhav. Steganography an Art of Hiding Data. International Journal on Computer Science and Engineering, Vol.1 (3) pp.137-141, 2009

CAPÍTULO V

SISTEMA DE MEDICIÓN

En esta sección se desarrolla el prototipo de medición de consumo de energía eléctrica que debe satisfacer requerimientos como: bajo costo, fácil instalación, proporcionar mediciones exactas de corriente, voltaje y potencia, además de medir y procesar los valores de consumo de energía eléctrica y capacidad de enviar la información de forma remota.

5.1 Diseño de prototipo

Para medir el consumo de energía de un usuario debe sensarse y procesarse variables físicas mediante sistemas embebidos, para ser enviados de forma inalámbrica a través de servidores que permitan visualizar los datos a través de plataformas móviles; permitiendo este sistema de monitoreo de energía eléctrica ser conscientes del consumo en periodos muy cortos de tiempo, así como corroborar que la facturación tiene la precisión requerida, además, de poder proporcionar servicios adicionales como: notificación de alarmas y consejos, utilizando mensajes de texto y de correo electrónico y alertas instantáneas basadas en parámetros definidos por el usuario; fortaleciendo la seguridad y privacidad que son dos temas clave para este tipo de sistemas [1].

Mediante un dispositivo de medición de energía eléctrica se calcula la cantidad de energía consumida para luego comunicar esta información a otro dispositivo que, a su vez, permita a los consumidores en periodos muy cortos de tiempo visualizar la

cantidad de energía que están utilizando, ser conscientes del consumo y administrar sus cargas además de reducir costos de facturación. El prototipo se desarrolla en dos etapas, la primera constituye la adquisición y procesamiento de señales de voltaje, corriente y potencia a través de simulación y la segunda procesa toda la información adquirida por la etapa anterior por medio de la plataforma Arduino.

Al ser SIMULINK, una herramienta que facilita la visualización en forma gráfica y numérica al emular el sistema de medición; se desarrolla un circuito de prueba de corriente alterna a 60 Hz, en el que se mide el voltaje y la corriente para calcular la potencia, y con esto la energía que consume una carga resistiva simulado en Matlab simulink (figura 5.1). En las figuras 5.2, 5.3, 5.4 y 5.5 se presenta la corriente, voltaje, potencia y la curva de consumo de energía eléctrica obtenida, cuando la carga resistiva es de 144Ω. Para este caso demostrativo, solo se presenta el consumo de energía en el trascurso de un tiempo de 10 segundos.

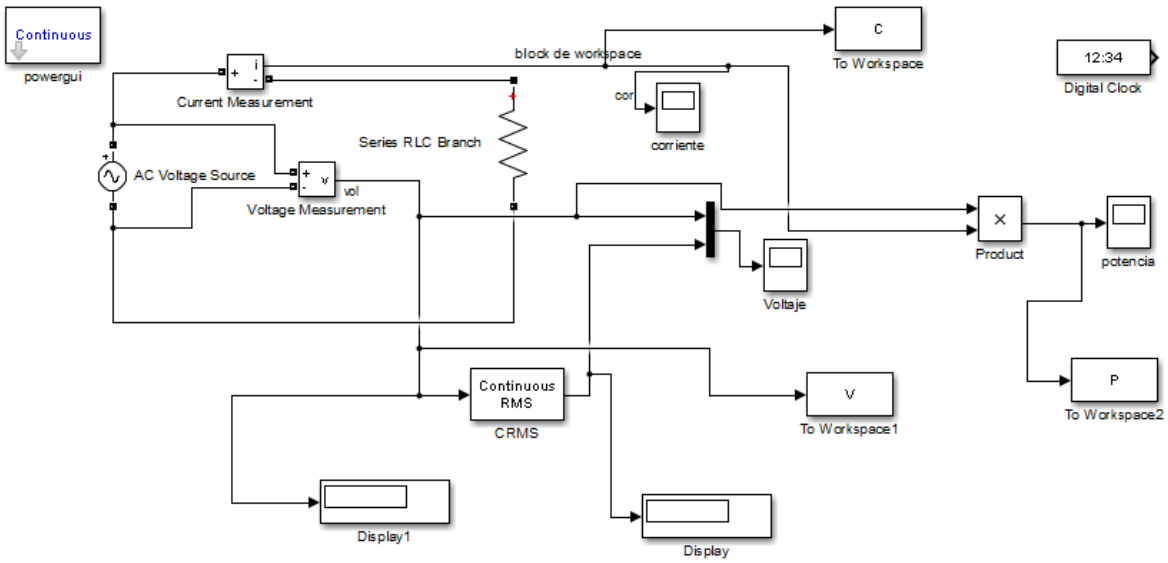


Figura 5.1 Diagrama a bloques del algoritmo de cifrado realizado en matlab/Simulink.

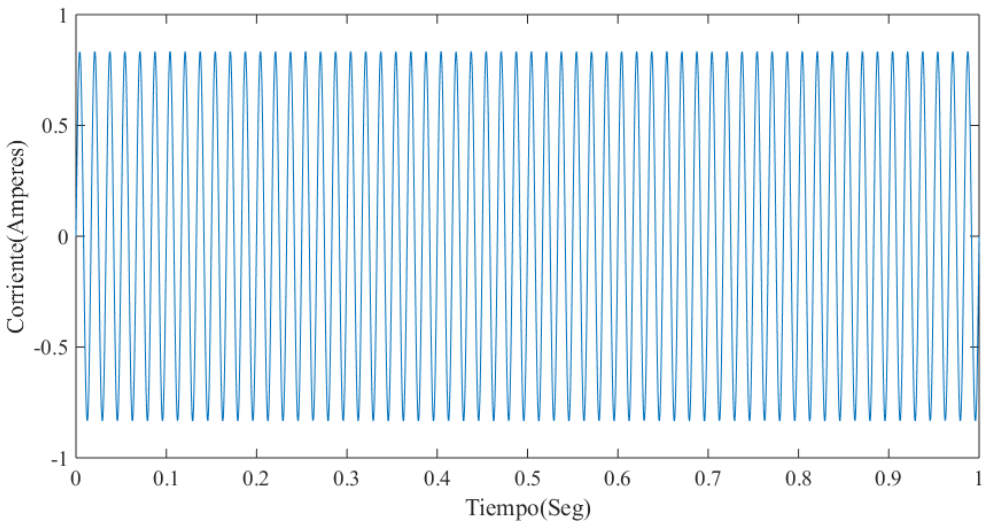


Figura 5.2 Señal de corriente matlab/Simulink.

En la figura 5.2, se presenta la señal de corriente simulada a través del circuito. Para este caso demostrativo, solo se presenta el consumo de energía en el trascurso de un tiempo de 1 segundo.

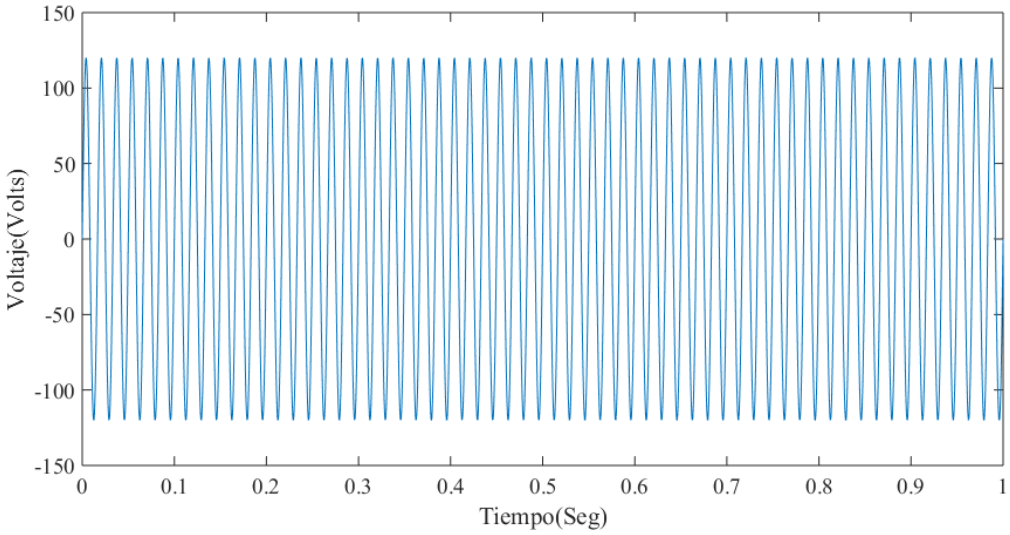


Figura 5.3 Señal de voltaje matlab/Simulink.

En la figura 5.3, se presenta la señal de voltaje simulada a través del circuito durante el trascurso de un tiempo de 1 segundo.

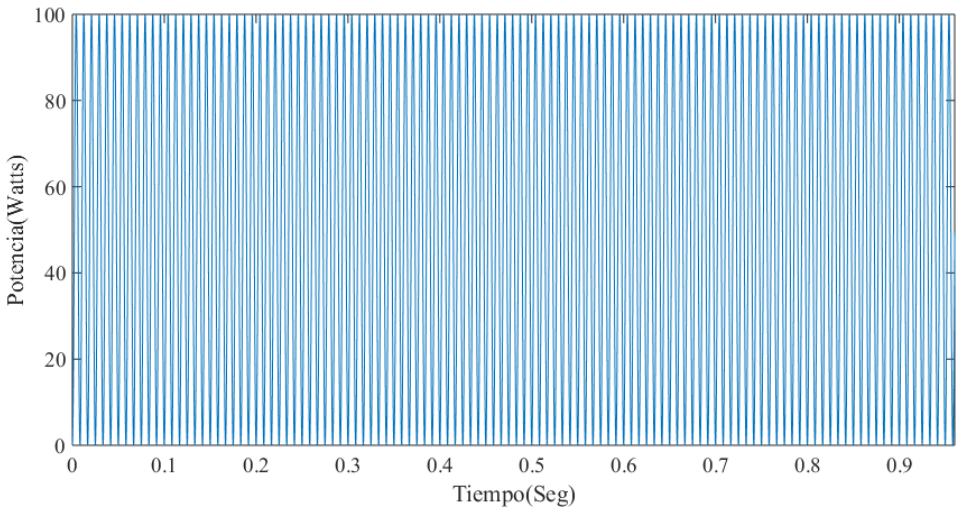


Figura 5.4 Señal de potencia matlab/Simulink.

En la figura 5.4, se muestra la señal de potencia calculada, observando que se aumenta al doble la frecuencia y solo muestra valores positivos.

En la figura 5.5, se muestra la señal de consumo de energía eléctrica calculada por la ecuación: $\int_0^t P(t)dt$.

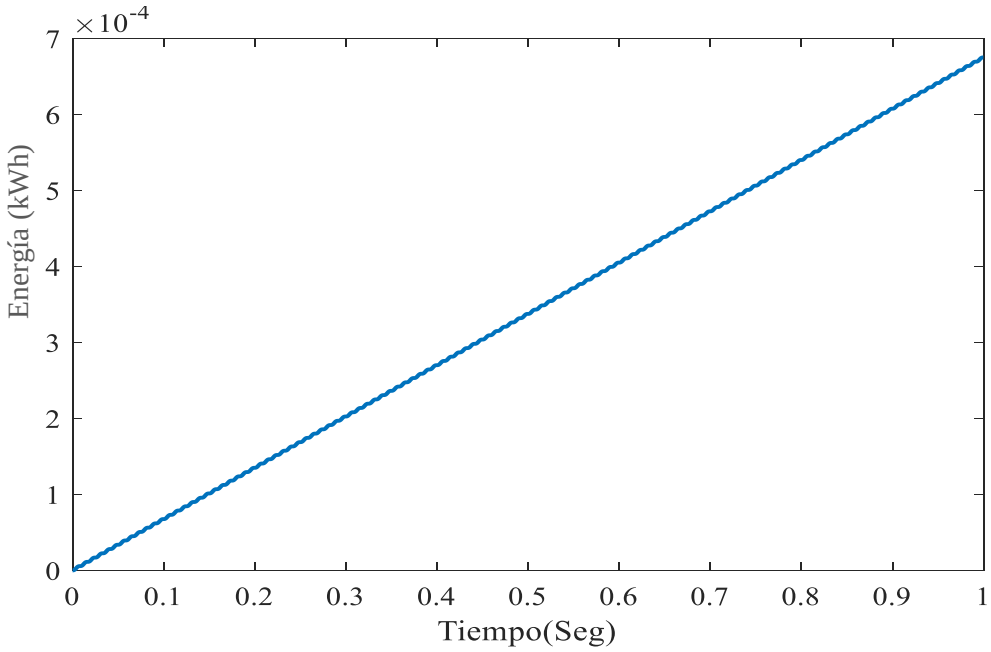


Figura 5.5 Esquema de la señal de energía matlab/Simulink.

Hoy día no solo se están utilizando sistemas de vigilancia y control de la energía para reducir el consumo de electricidad en la industria, sino que se están aplicando cada vez más en oficinas, edificios comerciales y de servicios, e incluso en los hogares para lograr los mismos objetivos. Para medir el consumo de energía debe

sensarse y procesar variables físicas y determinar valores para ser enviados a los usuarios a través de las tecnologías de información y comunicación [2].

Dado que las tecnologías de la comunicación son susceptibles a ataques intencionados y debe proponerse la solución más adecuada en cada caso. Una forma de fortalecer la confidencialidad e integridad de la información es a través del cifrado o encriptación, siendo la columna vertebral en la protección de datos altamente sensibles, pero la selección de un cripto-algoritmo afectará el rendimiento de un dispositivo en términos de memoria, latencia de cálculo y ancho de banda en la comunicación [3].

Para atender la seguridad y fiabilidad de los datos resulta imprescindible analizar la seguridad de las redes de energía inteligentes; enfocándose al sistema de medición, describiendo los requisitos de seguridad y considerando las posibles amenazas y vulnerabilidades, con la finalidad de que se comprenda cómo los atacantes maliciosos pueden comprometer la seguridad, refiriendo las vulnerabilidades, así como los ataques más sofisticados y su impacto [4].

Para la implementación del sistema de medición de consumo monofásico se propone el diagrama de bloques que se puede observar en la figura 5.6. Se procede a implementar las funciones de cada bloque para después ser ensamblados entre si

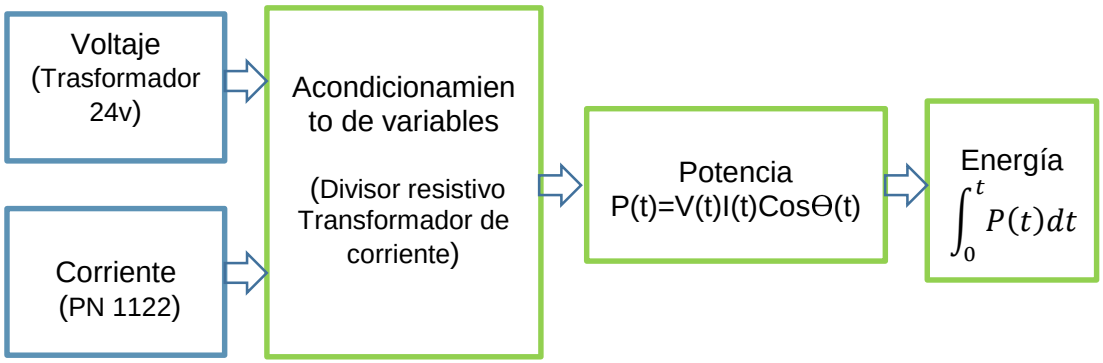


Figura 5. 6 Diagrama de bloques que ilustra el proceso de adquisición de variables físicas a través de los sensores de I y v.

La implementación del sistema para procesar los datos y generar un prototipo se realiza bajo plataforma Arduino, por las características técnicas de esta placa donde destacan su bajo costo, su tamaño reducido, las interfaces de comunicación que

maneja, y además posee un conversor análogo digital y puertos con salida de PWM por hardware, manejo de interrupciones externas e internas y una gran cantidad de librerías para el manejo de diferentes dispositivos.

La adquisición con los sensores para el acondicionamiento de la señal se lleva a cabo en tres etapas, dos de las cuales corresponden a un proceso electrónico que incluye la amplificación de la señal y su desplazamiento, este último se conoce comúnmente como “DC offset”, y puede apreciarse en el diagrama de circuito figura 5.7 y figura 5.8. La tercera etapa es el código necesario en la plataforma Arduino UNO para la captura de la señal análoga. Para la adquisición del dato de corriente se multiplica el valor que entrega el sensor por (0.04204); para medir el voltaje se utiliza un trasformador de 24 voltios y se utiliza solo una fase con la tierra del mismo, para obtener 12 voltios.

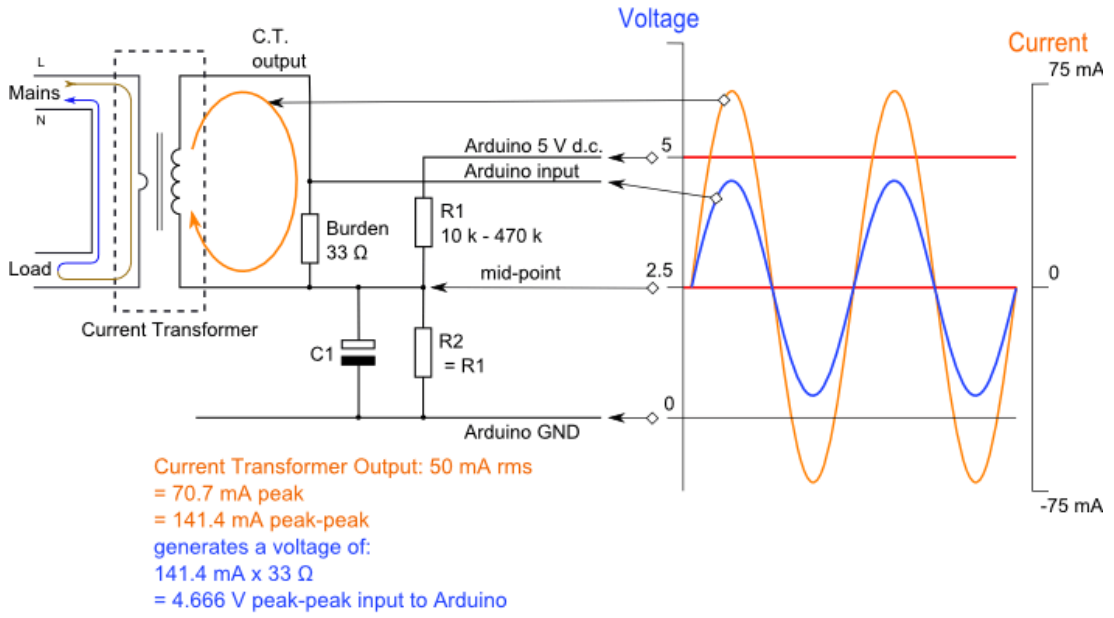


Figura 5.7 Diagrama de circuito de acoplamiento de la corriente [5].

El objetivo principal para la electrónica de acondicionamiento de señal que se detalla a continuación es disponer la salida del adaptador de alimentación de CA para que cumpla con los requisitos de las entradas analógicas Arduino: un voltaje positivo entre 0V y el voltaje de referencia de ADC (por lo general 5V o 3.3V). Las resistencias R1 y R2 forman un divisor de voltaje que reduce el voltaje de CA, las resistencias R3 y R4 proporcionan la polarización de voltaje.

El condensador C1 proporciona una ruta de baja impedancia a tierra para la señal de CA. El valor no es crítico, entre 1 µF y 10 µF será satisfactorio.

La polarización de voltaje proporcionada por R3 y R4 debe ser la mitad de la tensión de alimentación de Arduino. Como tal, R3 y R4 necesitan ser de igual resistencia. Una mayor resistencia reduce el consumo de energía. Si el Arduino está funcionando a 5V, la forma de onda resultante tiene un pico positivo de 2.5V + 1.15V = 3.65V y un pico negativo de 1.35V que satisface los requisitos de voltaje de entrada analógica de Arduino. Esto también deja algo de espacio libre para minimizar el riesgo de alto voltaje. La combinación de 10k y 100k R1 y R2 funciona bien.

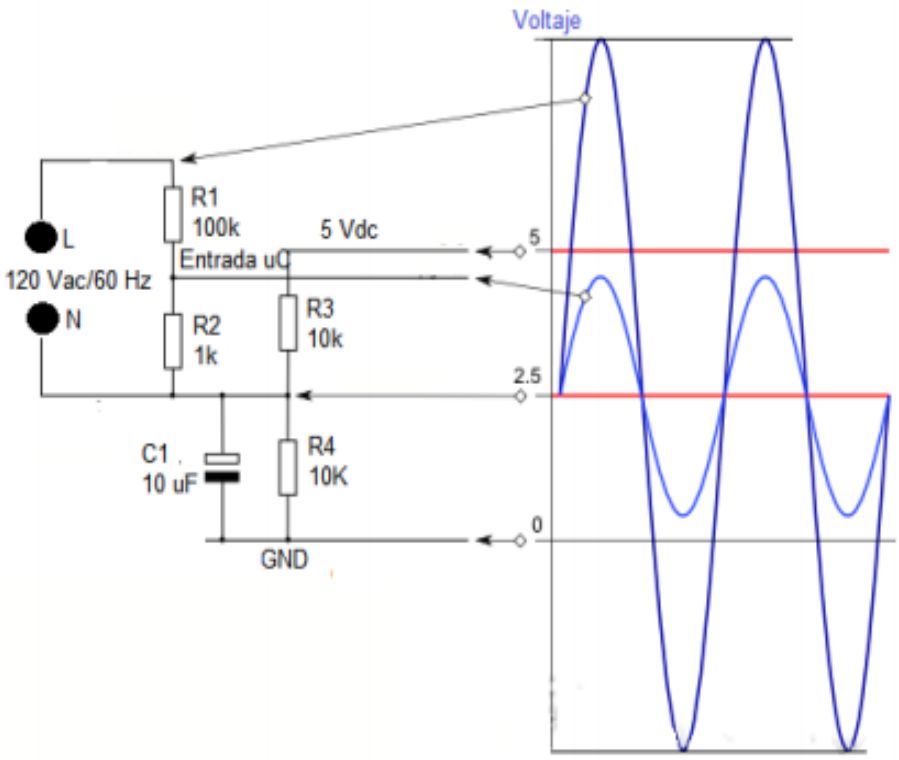


Figura 5. 8 Circuito de acoplamiento del voltaje [5]

Para maximizar la resolución de la medición, el voltaje a través de la resistencia de carga en la corriente máxima debe ser igual a la mitad del voltaje de referencia analógico de Arduino. Se procedió a integrar los dispositivos necesarios para ensamblar el prototipo obteniendo como resultado el dispositivo que se muestra en la figura 5.9.

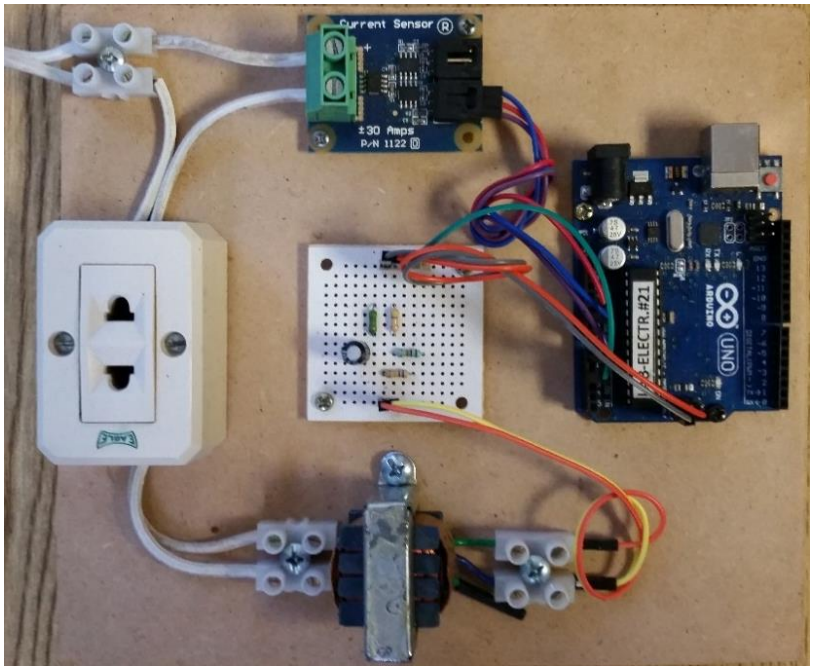


Figura 5.9 Circuito de cálculo de energía eléctrica

5.2 Implementación

Se acondiciona la señal teniendo una variación aproximada entre 0 y 5 voltios, Esta es la señal que recibe la entrada analógica de Arduino ya sin pasar a la parte negativa de la sinusoidal. En este punto ya obtuvo el valor de la corriente y voltaje, lo siguiente es calcular la potencia, para lo cual se utiliza la siguiente formula.

$$P(\mathrm{t}) = \mathrm{V(t)I(t)Cos\Theta(t)} \tag{1}$$

Donde la variable p representa la potencia (watts) que es dada por el producto del Voltaje y la Corriente (intensidad). La energía eléctrica que consume un aparato eléctrico se calcula integrando la potencia eléctrica por la diferencial del tiempo que se encuentra funcionando.

$$E = \int_0^t P(t)dt \tag{2}$$

Donde E corresponde a la energía, p a la potencia con respecto de t, tiempo. Se plantea realizar un muestreo cada 50 milisegundos, donde se divide entre 20 para representar en milisegundos.

Posteriormente se realizan distintas pruebas con diferentes aparatos eléctricos conectados al prototipo de medición de consumo de corriente eléctrica con el fin de

obtener los diferentes consumos, por ejemplo de una lámpara incandescente de 100 watts como se observa en la figura 5.10.

Figura 5.10 Medición de energía de una lámpara incandescente.

Se muestra el consumo de energía de una lámpara incandescente de 100 watts utilizando el prototipo de cálculo figura 5.11.

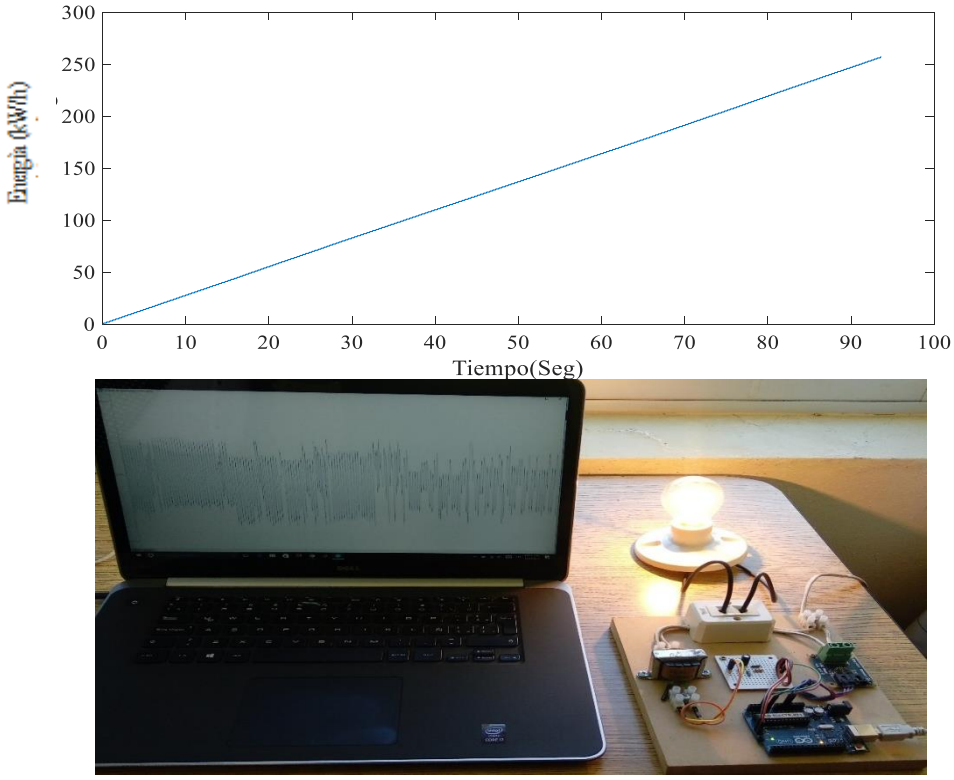


Figura 5. 11 Prototipo de cálculo de consumo de energía eléctrica.

5.3 Propuesta de reporte y monitoreo de mediciones de consumo de energía eléctrica de forma remota.

En la actualidad, no se cuenta con dispositivos comerciales de bajo costo enfocados al uso particular que permitan hacer medición [6], almacenamiento y reporte de la información propia de los consumidores como es el consumo de energía eléctrica. La recolección de esta información es importante porque permite, por ejemplo, conocer en tiempo real el consumo de energía eléctrica, lo que facilitaría que la ciudadanía identificara cuáles son sus hábitos de consumo, lo que a su vez favorecería acciones como el ahorro de energía [7] y con ello concientizar sobre el uso óptimo de los recursos y el impacto en los recursos naturales. Así mismo, es claro observar que con base en la información obtenida a través del desarrollo de ciertas aplicaciones tecnológicas [7] se puede realizar por ejemplo una alerta al móvil de un usuario cuando el consumo de energía se dispare en un momento y con ello generar la ejecución de acciones preventivas o correctivas.

Según Cisco [8], se espera que para 2020 se cuente con 50 billones de dispositivos conectados a internet, lo cual se ve evidenciado en la creciente producción de sensores [9] y dispositivos de comunicación de bajo costo que permiten hacer reportes periódicos de datos siguiendo determinados protocolos [10]. Representa una gran ventaja poder conocer en tiempo cuasi-real si el consumo de energía eléctrica es muy elevado en determinado momento ya sea que haya o no presencia humana en el hogar [11] para concientizar en cuanto al uso eficiente de los recursos. Por tanto, se identifica claramente la necesidad latente de diseñar y desarrollar de manera rápida y con tecnología local aplicaciones orientadas al favorecimiento de la calidad de vida de la ciudadanía y garantizando una accesibilidad económica y de calidad.

Para el diseño y desarrollo de un sistema de medición y monitoreo de consumo de energía eléctrica, actualmente en el mercado existen aplicaciones, que permiten hacer una medición periódica de algunas variables y reportar estas mediciones utilizando diferentes protocolos, aunque en una gran mayoría de estas aplicaciones está enfocadas a un mercado muy reducido. El desarrollo de un sistema de medición y monitoreo remoto enfocado al consumidor exige el conocimiento de temas

relevantes como el funcionamiento de algunos sensores para medición de variables físicas de consumo de energía eléctrica; el funcionamiento de las diversas redes de comunicación; el hardware existente para instrumentar, procesar y comunicar datos por medio de las redes existentes y las tecnologías WEB que permiten interactuar de manera favorable con usuarios.

En menos de 10 años, la WEB ha transformado los sistemas informáticos, ha roto barreras físicas, mostrando un horizonte lleno de posibilidades [12]. Las aplicaciones WEB combinan diferentes lenguajes de programación, dentro de los más comunes se encuentran HTML, PHP, MySQL y JAVASCRIPT; permiten la interacción del usuario con la información que circula por internet [13], [14].

Dentro de las tecnologías disponibles en software se hace necesario separar las disponibles en software para programación de hardware y software para programación de aplicaciones WEB. Matlab es un potente lenguaje diseñado para la computación de alto nivel. Una de las grandes ventajas de utilizar Matlab es que incorpora una serie de librerías específicas [15], que contienen funciones especializadas y diseñadas para resolver problemas muy particulares.

Debido a las características del sistema, se hace necesario identificar el hardware apropiado que pueda suplir las necesidades de procesamiento, confiabilidad y costos. Al analizar los requerimientos principales del sistema que incluyen entre otras cosas adquisición, manipulación y en ocasiones filtrado de señales; procesamiento, agrupación y caracterización de datos. El IDE de Arduino puede descargarse de manera libre desde el sitio web [16]. La gran variedad de placas, la economía, la accesibilidad y la abundante documentación que genera la enorme comunidad, hacen a esta plataforma ideal para ser utilizada en el desarrollo de este proyecto.

Para la página WEB se decidió utilizar el administrador de contenidos JOOMLA, debido a la necesidad de una página de llamada única que cuente solo con un formulario de validación de entrada por medio del cual los usuarios puedan ingresar a un panel de control desde el que puedan generar las gráficas de los reportes del consumo y monitoreo y que les permita enviar órdenes a los dispositivos que posean. Cabe señalar que dentro del diseño de la página WEB se contempla que

esta responda a los dispositivos móviles y adapte su contenido a los diferentes tipos y tamaños de pantalla de estos.

Se diseñó una base de datos en el gestor de bases de datos phpMyAdmin que permite almacenar y relacionar los datos de los usuarios, de los diferentes tipos de dispositivos que hay y que le pertenecen a algún usuario, los datos de los reportes hechos por los diferentes dispositivos y las órdenes enviadas por cada usuario a cada uno de sus dispositivos. La implementación de una base de datos permite almacenar, consultar y relacionar la información de esta manera facilita enormemente la escalabilidad del sistema.

Se concluye el tratamiento electrónico que se le debe dar a la señal, ahora es necesario capturar procesar y enviar la señal resultante, para hacer esto se deben tener algunas consideraciones con respecto a la señal, la calidad de esta y la capacidad de procesamiento del Arduino. Después de construir el prototipo para hacer mediciones de consumo de energía eléctrica y reportar las mediciones, se consideró además enviarlas vía inalámbrica.

Se desarrolla una interfaz WEB que permite interactuar con la información reportada por un prototipo que hace mediciones y envía la información de forma inalámbrica. Con la decisión de construir la página WEB apoyada en el gestor de contenidos JOOMLA, se procede a obtener recursos necesarios para el desarrollo del sitio, se requiere alojamiento WEB y un dominio. Después de adquirir y configurar el alojamiento y el dominio, se procede a instalar el gestor de contenidos JOMMLA.

Cumpliendo con los requerimientos, en la figura 5.12, puede observarse el formulario de validación de usuarios desarrollada sobre el gestor de contenidos JOOMLA.

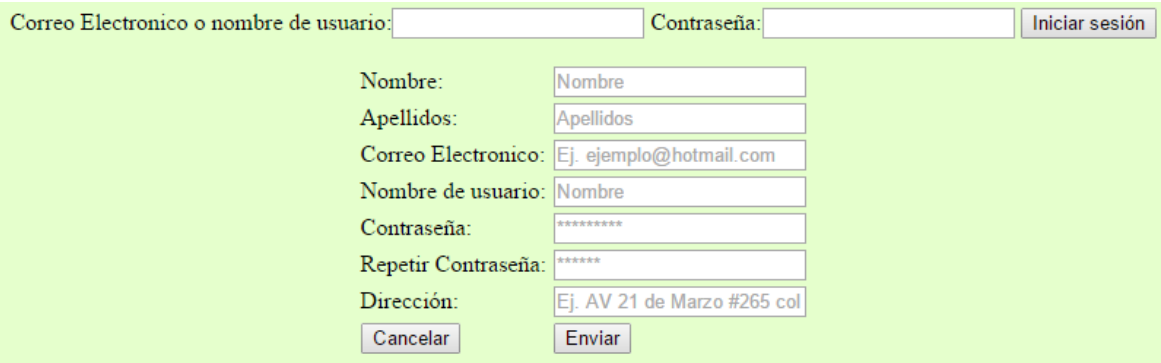


Figura 5.12 Formulario de validación de usuarios

Cómo puede observarse en la figura 5.12, en la parte superior del formulario se muestran dos opciones para solicitar la contraseña y usuario, con lo que permite la accesibilidad de la página WEB.

Aprovechando la implementación de la base de datos para administrar los datos, se decide escalar el proyecto construyendo una aplicación para dispositivos móviles Android desde el cual se pudiera monitorear y enviar reporte sobre consumo a los interesados.

El gestor de contenidos JOOMLA brinda la facilidad de separar de manera modular todas las partes que actúan en la página WEB, esto quiere decir que los artículos y el contenido pueden generarse de manera independiente a la construcción del resto de la página. JOOMLA permite desligar la parte visual del contenido generado y publicado. Aprovechando esta ventaja, se desarrolló el módulo de gráficas como un artículo de manera independiente. Inicialmente se desarrolló un formulario HTML que permitiera seleccionar la variable que se desea graficar y el rango de fechas entre los cuales se quiere generar la gráfica. Además, se agregó un calendario que hiciera más amigable la función de selección de las fechas entre las que se quería graficar.

Se define que el lapso de tiempo a utilizarse entre reportes de consumo de energía eléctrica sería de entre 6 y 12hrs debido a que en un lapso de tiempo más grande sería más difícil identificar los dispositivos que contribuyen al consumo de energía eléctrica. Además, esta frecuencia en los reportes permite identificar de manera precisa entre otras cosas las horas pico y las horas valle en el consumo de energía de un hogar o empresa pequeña.

Como resultado se crea una página WEB funcional y segura con un módulo de gestión de usuarios que permite resguardar los datos de los hogares o las empresas, con un sistema de generación de diversos gráficos que permiten analizar los datos de los reportes y con una interfaz que les permite a los usuarios, monitoreo y control sus consumos de energía eléctrica. Se obtiene una aplicación para dispositivos móviles con sistema operativo Android que permite validar los usuarios que la utilizan garantizando así la seguridad de los datos de los hogares o las empresas pequeñas, conocer el estado actual de los dispositivos que se poseen, y monitorear los valores de las variables que reportan los dispositivos de manera remota.

Finalmente, el resultado obtenido puede apreciarse en la figura 5.13, que corresponde a las gráficas que representan el consumo de energía eléctrica simulada de un hogar en un periodo de tiempo establecido.

Figura 5.13 Representación gráfica del consumo de energía eléctrica para móviles.

5.4 Referencias

[1]. Bader M. O. A, Design and Implementation of a Reliable Wireless Real-Time Home Automation System Based on Arduino Uno Single-Board Microcontroller. Vol 3(3), pp. 11-15, 2014.

[2]. Lu Tan; Neng Wang "Future internet: The Internet of Things" Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on Digital pp. V5-376 - V5-380, 2010.

[3]. Q. Al-Haija, M. Tarayrah, H. Al-Qadeeb and A. Al-Lwaimi, "A Tiny RSA Cryptosystem based on Arduino Microcontroller Useful for Small Scale Networks", Procedia Computer Science, vol. 34, pp. 639-646, 2014.

[4]. M., Zapateiro, D. Hoz, L., Acho, Y. Vidal. An Experimental Realization of a Chaos-Based Secure Communication Using Arduino Microcontrollers", The Scientific World Journal, vol. 2, pp. 1-10, 2015.

[5]. J. D & # 39; Ambra y E. Logger, Energy Data Logger, Hackster.io, 2018. [En línea]. Disponible: https://www.hackster.io/javidambra/energy-data-logger-3e2dba. [Accedido: 31 de mayo de 2018].

[6]. S. Pokric, Krco, D. Drajic, M. Pokric, I. Jokic, and M. Stojanovic, ekonet environmental monitoring using low-cost sensors for detecting gases, particulate matter, and meteorological parameters, in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Eighth International Conference pp. 421_426, 2014.

[7]. J. D. Hobby and G. H. Tucci, “Analysis of the residential, commercial and industrial electricity consumption, in Innovative Smart Grid Technologies Asia (ISGT), IEEE PES, pp. 17, IEEE, 2011.

[8]. I. Simonis and M. Van Der Merw. Earth observation and environmental modelling for the mitigation of health risks such as cholera, cardio-vascular and respiratory diseases, in IST-Africa Conference Proceedings, IEEE, pp. 1-8, 2011.

[9]. D. Evans, The internet of things: How the next evolution of the internet is changing everything,CISCO white paper, vol. 1, 2011.

[10]. F. Zhang, R. Wang, S. Gao, S. Yu, J. Hu, and Y. Jin, _Design and implementation of wireless bridge health monitoring system, 2011.

[11]. R. Petrolo, N. Mitton, J. Soldatos, M. Hauswirth, and G. Schiele, Integrating wireless sensor networks within a city cloud, in Sensing, Communication, and Networking Workshops (SECON Workshops), Eleventh Annual IEEE International Conference on, pp. 24_27, IEEE, 2014.

[12]. B. Izneid, A. Abdulrahman and T. Al-kharazi, "Development of remote monitoring (CO) measurement instrument based microcontroller and electro-optic technique", 2013 IEEE International RF and Microwave Conference (RFM), 2013.

[13]. A. Tanenbaum and D. Wetherall, Redes de computadoras. México: Pearson Educación, 2012.

[14]. S. L. Mora. Programación de aplicaciones web: historia, principios básicos y clientes web. Editorial Club Universitario, 2002.

[15]. Ó. T. Artero, Arduino: curso práctico de formación. RC Libros, 2013.

[16]. L. Herger and M. Bodarky, Engaging students with open source technologies and arduino, inIntegrated STEM Education Conference (ISEC), 2015 IEEE, pp. 27_32, 2015.

CAPÍTULO VI

EVALUACIÓN DEL CIFRADO

En este capítulo se evalúa el algoritmo utilizando los métodos: Mapeo Logístico sobre datos simulados, datos fuera de línea e implementación en prototipo y Bernoulli sobre datos fuera de línea. Se muestran los criterios de evaluación para el criptosistema de acuerdo a los principios de Shannon; como la teoría de la información, entropía del mensaje de entrada y de salida e información mutua, y su distribución estadística; con el principal objetivo de evaluar la aleatoriedad en la distribución estadística se hace uso de pruebas estándares de valoración de aleatoriedad planteadas en la suite NIST, con el propósito de obtener métricas del grado de seguridad, fortaleza de clave, diseño de cifrado, rendimiento y resistencia de cada uno de ellos. Posteriormente, los algoritmos son sometidos a pruebas para evaluar su desempeño y eficiencia sobre la imagen Lena [1], [2].

Finalmente, se compara el desempeño del algoritmo propuesto midiendo el grado de seguridad, fortaleza de clave, diseño, modo de cifrado, rendimiento (Software y Hardware) y resistencia de cada; uno de ellos e idoneidad en entornos de recursos restringidos con el objetivo de evidenciar su capacidad para asegurar los datos protegidos contra ataques y su velocidad y eficiencia en hacerlo y proporcionar mayor seguridad de la información, bajo un contexto ideal.

6.1 Criterios de Evaluación

Para llevar a cabo una buena evaluación de todo proceso criptográfico, es necesario tener en cuenta los fundamentos teóricos de la criptografía, dando una serie de nociones básicas sobre Teoría de la Información, introducida por Claude

E. Shannon. Sin duda, esta disciplina permite efectuar una aproximación teórica al estudio de la seguridad de cualquier algoritmo criptográfico [3].

La cantidad de información, se puede observar como una medida de disminución de incertidumbre acerca de un suceso. Con el objeto de simplificar la notación, se emplea una variable aleatoria x para representar los posibles sucesos que se pueden encontrar. Considerando que la entropía mide la incertidumbre de una fuente de información calculando la aleatoriedad de los datos, lo que permite evitar cualquier previsibilidad. La entropía está dada por la ecuación siguiente:

$$H = \sum_{i=1}^{2^8} P(S_i)\log_2 P(S_i) \quad (1)$$

Donde H, representa (entropía de Shannon) la sorpresa de un evento o su nivel de incertidumbre, S un símbolo, carácter o mensaje y P la probabilidad de aparición de éste. Se considera que, entre más alto es el valor de H, más inesperado se hace la ocurrencia de dicho evento, en otras palabras, se torna más aleatorio e impredecible [3].

La Teoría de la Información de Shannon permitió la caracterización estadística de fuentes deterministas caóticas. Estos esfuerzos para describir la impredescibilidad de sistemas dinámicos condujeron a la definición de cantidades tales como la entropía métrica y los exponentes de Lyapunov que pueden emplearse para detectar la presencia de caos y para cuantificar el comportamiento caótico determinista. Y sumando ponderadamente las cantidades de información de todos los posibles estados de una variable aleatoria, obtenemos la ecuación:

$$\lambda = \lim_{n\to\infty} \{\frac{1}{2}\sum_{i=0}^{n-1} \ln | f'(x_i) | \} \quad (2)$$

Para evaluar el algoritmo de cifrado propuesto previamente, el cual está aplicado sobre un sistema de medición de datos de energía eléctrica en el marco de las redes inteligentes; se desarrolla un circuito de prueba de corriente alterna a 60 Hz, en el que se mide el voltaje y la corriente para calcular la potencia, y con ello la energía que consume una carga resistiva. En la figura 6.1A, se muestra la señal de los datos de consumo de energía eléctrica antes de aplicar el algoritmo de cifrado, y en la misma figura se sobrepone la señal recuperada (descifrada) después del proceso de cifrado.

En la figura 6.1B, se presenta la señal cifrada usando el algoritmo propuesto sobre mapeo logístico en este trabajo de investigación; utilizando como parámetros de entrada: $\mu = 3.89$ y $x_0 = 0.00499$ para la primera secuencia y $\mu = 3.86$ y $x_0 = 0.01999$ para la segunda; que son semilla generadora de la clave de

cifrado (simétrico), dadas sus características de impredecibilidad que muestran las pruebas en el caso simulado.

En las figuras 6.1A y 6.1B, puede apreciarse el comportamiento de la señal que representa el consumo de energía eléctrica, y su equivalente cifrada, respectivamente, esta última presenta un comportamiento con variación en la señal una vez que es afectada por el algoritmo de cifrado, en sus propiedades básicas (frecuencia, amplitud), tendiendo a parecerse a una señal de ruido.

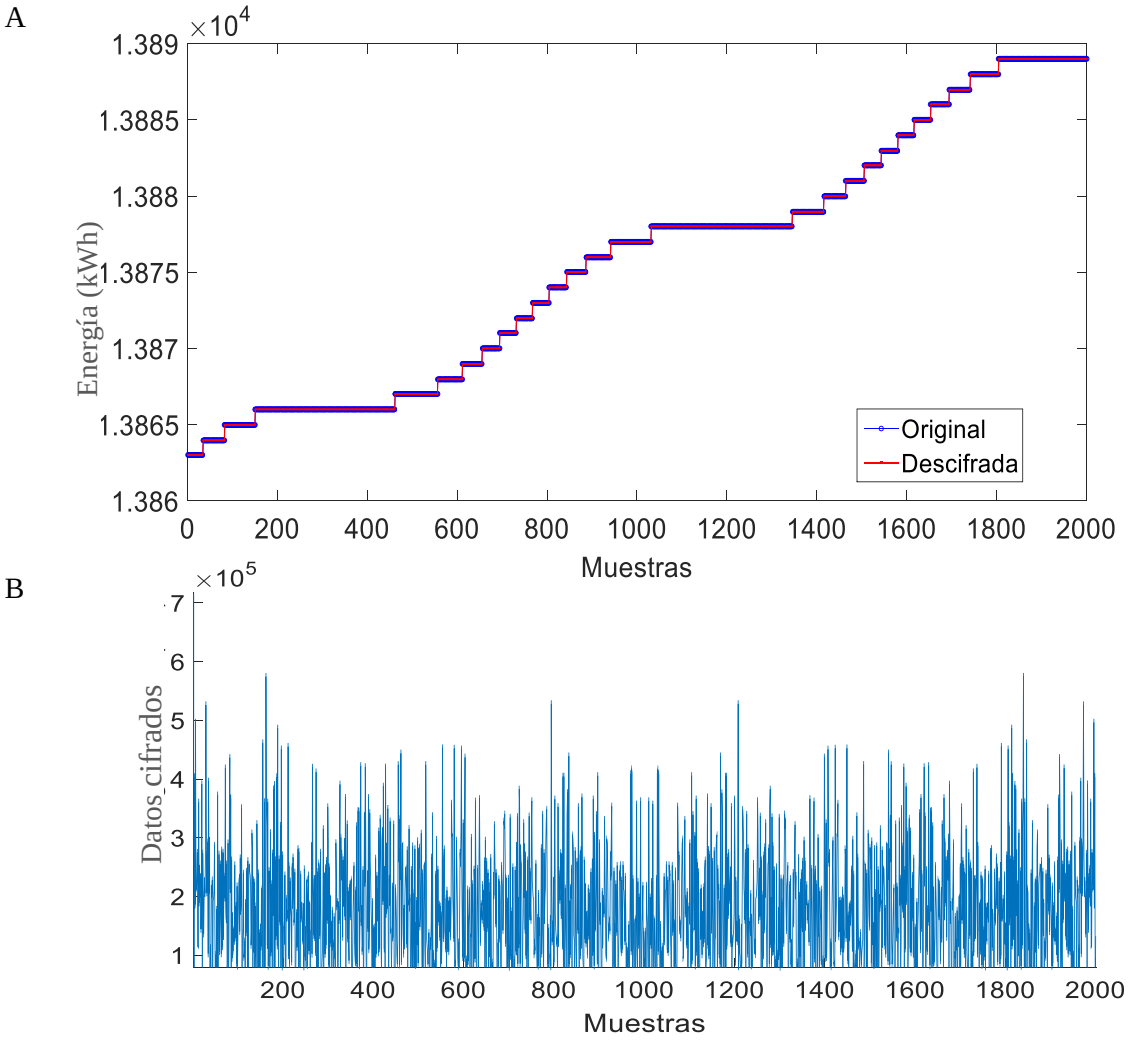


Figura 6.1 Señal de consumo de energía eléctrica. (A)Señal original y señal recuperada superpuesta (B) Señal cifrada con el algoritmo propuesto.

6.2 Evaluación de cifrado

Para valorar características de independencia, distribución y correlación entre la sucesión datos cifrados se lleva a cabo la evaluación de cifrado, donde se presenta que los resultados simulados demuestran viabilidad y seguridad del

algoritmo propuesto, se emplean pruebas estadísticas de distribución, dispersión, correlación, histogramas y entropía.

La información obtenida a partir de las medidas de posición (centralización), dispersión y forma se pueden apreciar en el diagrama de caja que visualmente proporciona información de cómo están distribuidos los datos. En la figura 6.2A, se muestra la distribución de datos cifrados, señalando donde cae la mayoría de ellos y los que difieren considerablemente de la norma, indicando la mediana por la línea que atraviesa la caja con un valor de 8,803, delimitada por la posición de los cuartiles primero con 4,876 y tercero con 12,427 y, la extensión del conjunto de valores, siendo el máximo de 16,378 y mínimo 14, respectivamente. Debido a la posición que se presentan los datos con respecto a la media, indica que los valores se encuentran uniformemente distribuidos.

A través de un diagrama de dispersión se puede visualizar el comportamiento de los datos, para determinar si existe un patrón. En la figura 6.2B, se muestra el diagrama de los datos de la señal de consumo de energía eléctrica contra los mismos datos pero cifrados, se traza un punto central y sobre este las líneas de división por regiones, que permite distinguir la distribución de los puntos predominantes dentro de estas, sin embargo los puntos, se encuentran muy dispersos mostrando poca o nula asociación entre los valores originales y los valores cifrados ya que la distribución es uniforme; esto indica que no hay relación (correlación) entre las variables de estudio. Ambas variables son independientes entre sí; lo que indica que la variación de una de ellas no influye para nada en la otra.

Se realiza un análisis de correlación donde se mide la asociación lineal entre los datos originales y los datos cifrados, posteriormente se realiza la correlación con los datos cifrado y los descifrados, con la finalidad de determinar si existe alguna perdida de información al utilizar el algoritmo.

Con el fin de obtener medidas numéricas se calcula el coeficiente de correlación con la siguiente ecuación:

$$c = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad (3)$$

Donde, n es el número de elementos en los dos vectores adyacentes x e y. Para datos fuertemente encriptados, los coeficientes de correlación se deben aproximar a cero [4], [5].

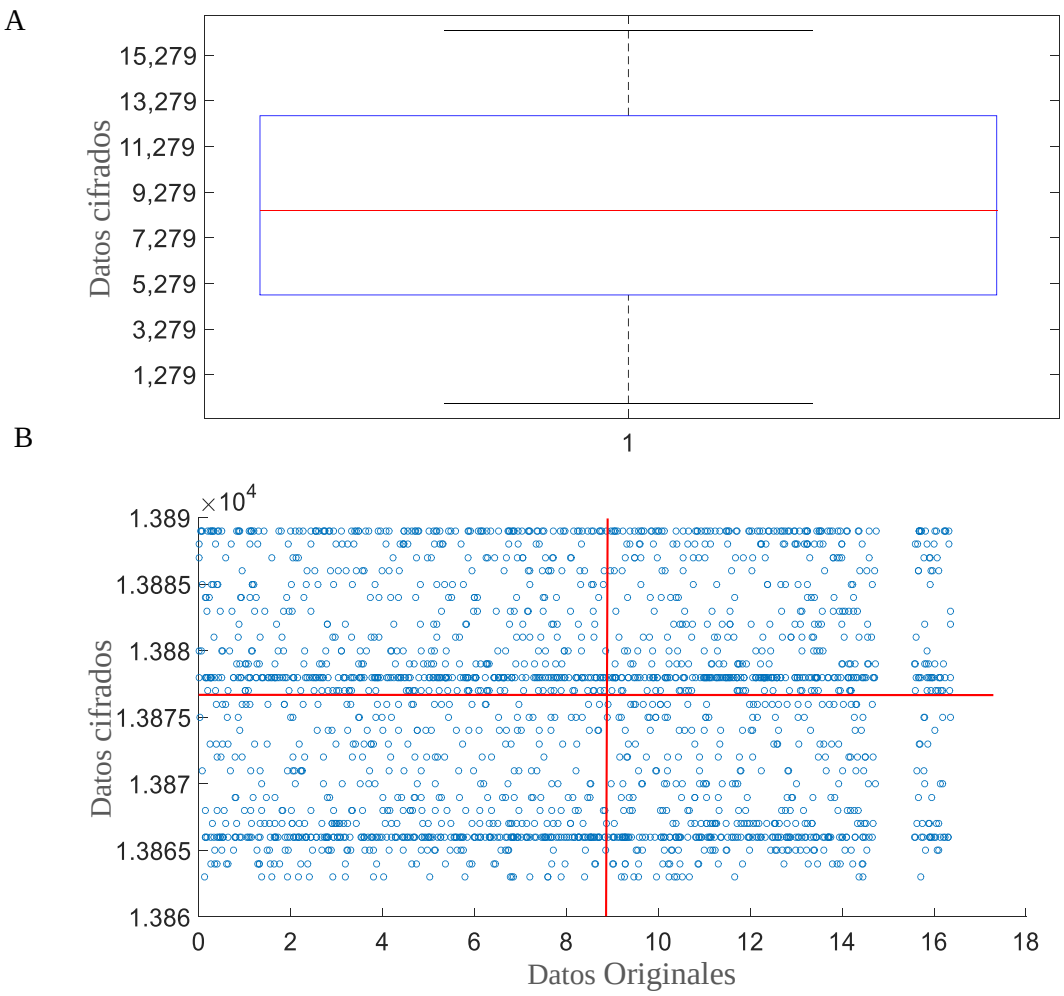


Figura 6. 2 Distribución de datos cifrados. (A)Diagrama de caja, (B) Diagrama de dispersión de datos cifrados.

Si los puntos están repartidos equitativamente en las cuatro regiones, entonces el coeficiente de correlación entre los valores es cero o muy cercano a cero [2].

Los histogramas permiten representar de forma gráfica cómo se distribuyen los datos. En las figuras 6.3A y 6.3B, se muestra la distribución de los valores tanto en la señal original como en la señal cifrada, respectivamente. En el primer caso el histograma exhibe en el eje horizontal los valores de la señal en el rango de 13865 a 13890, donde, las barras más altas indican los valores que se repiten con mayor frecuencia. Por otra parte, en el segundo caso, el histograma de la señal cifrada, con el algoritmo propuesto, en el eje horizontal presenta valores de 0 a 16000.

Al comparar los histogramas de las figuras 6.3A y 6.3B, se puede observar que tienen diferente distribución en las frecuencias de la señal original respecto a la señal cifrada, mostrando rangos diferentes en el eje horizontal, lo cual, aumenta la dificultad al posible atacante para analizar y descifrar los datos codificados.

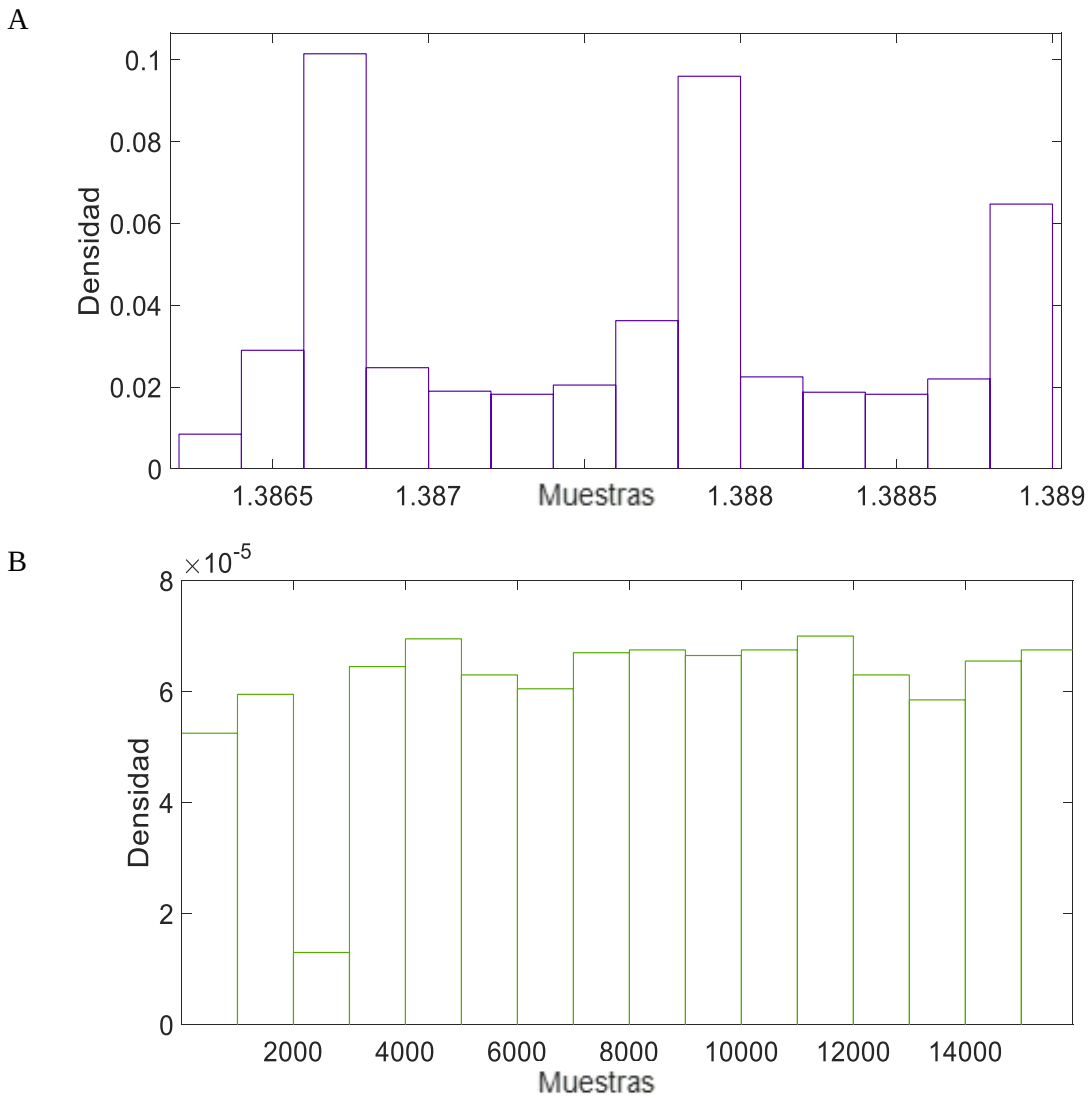


Figura 6.3 Histograma. A) Señal original. B) señal cifrada.

Existen muchos métodos adecuados para detectar estructuras, pero ninguno ha logrado tener una aplicabilidad tan amplia como la de la entropía para indicar aleatoriedad. La entropía mide la incertidumbre de una fuente de información calculando la aleatoriedad de los datos, lo que permite evitar cualquier previsibilidad. La entropía está dada por la ecuación siguiente:

$$H = \sum_{i=1}^{2^8} P(S_i) \log_2 P(S_i) \quad (4)$$

Donde H, representa (entropía de Shannon) la sorpresa de un evento o su nivel de incertidumbre; S un símbolo, número o mensaje y P la probabilidad de aparición de éste. Se considera que, entre más alto es el valor de H con respecto a los datos digitalizados, más inesperado se hace la ocurrencia de dicho evento, en otras palabras, se torna más aleatorio e impredecible [5]. Si se trabaja en caracteres ASCII, queda simbolizado cada uno con 8 bits, y permite representar hasta 256

caracteres, suficientes para contener información referente. Tabla 6.1, se muestra el comportamiento de la señal resultante después del proceso de cifrado y los valores esperados en base a la evaluación aplicada donde las propiedades importantes esperadas son uniformidad e independencia en los datos cifrados.

Tabla 6.1. Concentrado de evaluaciones estadísticas al criptograma.

Métricas estadísticas	
Coeficientes de correlación	-0.0251
Entropía	7.9936
Desviación estándar	4728.7
Media	8526.4
Mediana	8803.5
Varianza	2.2360
Corrida ascendente y descendente	0
Información mutua	0.000202

6.3 Suite de pruebas estadísticas del NIST

Debido a que existen muchas pruebas estadísticas que se aplican para determinar si una secuencia es o no aleatoria y teniendo como objetivo el de evaluar la aleatoriedad de las secuencias obtenidas en el proceso de cifrado, en esta tesis se hace uso de la suite de pruebas estadísticas NIST, arquitectura conformada de cinco etapas figura 6.4, involucradas en la evaluación estadística de un generador de secuencias aleatorias.

En la selección de un generador para evaluarse, éste debe producir una secuencia binaria de 0’s y 1’s de una longitud *n* determinada. Se construye un conjunto de *m* secuencias binarias que posteriormente se guardan en un archivo. Durante la ejecución de la suite de pruebas estadísticas del NIST usando el archivo generado en la etapa dos y la secuencia de la longitud deseada se seleccionan las pruebas estadísticas y los parámetros de entrada que deben aplicarse.

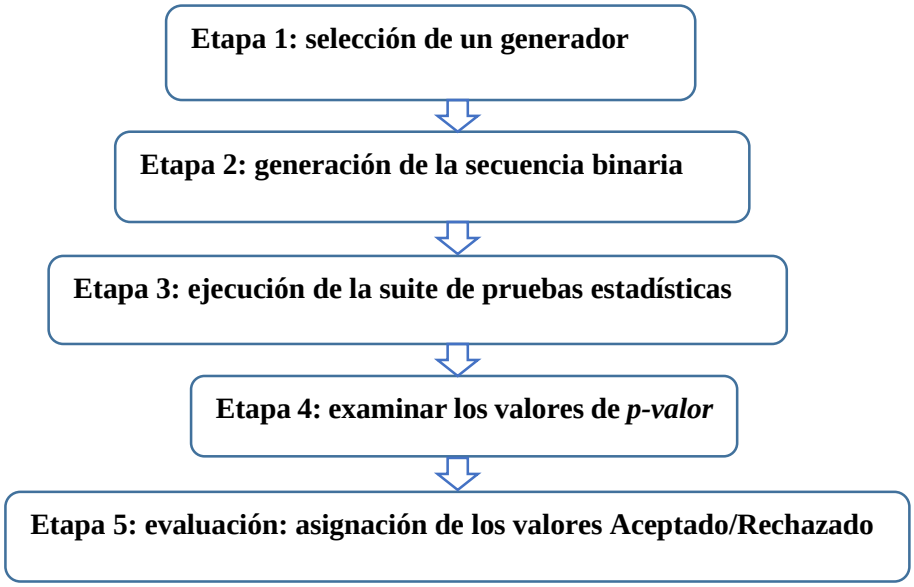


Figura 6.4 Etapas de evaluación estadística de un generador de secuencias aleatorias.

La suite de pruebas estadísticas genera un archivo de salida con los valores relevantes, como las pruebas estadísticas y los valores de *P* para cada prueba. Basándose en los valores de *P*, se pueden hacer conclusiones respecto a la calidad de la secuencia, donde se evalúa la asignación de los valores aceptando o rechazado en base al nivel de significancia.

Por ejemplo, si el nivel de significancia es 0.01 (α = 0.01), entonces se espera que aproximadamente el 1% de las secuencias fracasen. Una secuencia certifica una prueba estadística siempre y cuando el valor de $P > \alpha$, de lo contrario falla. En consecuencia, por cada prueba estadística, la proporción de secuencias que aprueban se calcula y analiza. Dada la interpretación de los resultados obtenidos existen escenarios que representan eventos que pueden ocurrir debido a las pruebas efectuadas.

La suite NIST ha adoptado dos enfoques que incluyen el examen de la proporción de las secuencias que aprueban un test estadístico y la distribución de los valores-P para comprobar la uniformidad. En caso de que cualquiera de estos dos enfoques falle (la hipótesis nula correspondiente debe ser rechazada). La Suite cuenta con 15 pruebas estadísticas. Estas pruebas evalúan la presencia de un patrón, el cual, si es detectado indicaría que la secuencia no es aleatoria. En cada prueba para el criptograma con mapeo Logístico sobre datos de consumo de energía eléctrica obtenidos por simulación, se calcula un P-valor con una significancia de α = 0.01, los resultados obtenidos se observan en la tabla 6.2.

- El nivel de significancia α para todas las pruebas de la suite se establece en 1%.
- Un P-valor de cero indicaría que la secuencia no es aleatoria en absoluto.

- Un P-valor menor que α significaría que la secuencia no es aleatoria con una certeza de un 99%.
- Si el P-valor es mayor que α, concluimos que la secuencia es aleatoria con una certeza del 99%.

Tabla 6.2. Resultado de la suite NIST para criptograma con mapeo Logístico

Pruebas	Valor P Obtenido	Estado
APPROXIMATE ENTROPY	0.809791	OK
BLOCK FREQUENCY	0.491789	OK
CUMULATIVE SUMS	0.412876	OK
CUMULATIVE SUMS	0.312923	OK
FFT	0.804313	OK
FRECUENCY	0.406539	OK
LINEAR COMPLEXITY	0.750305	OK
LONGEST RUNS OF ONES	0.504821	OK
NONOVERLAPPING TEMPLATE	0.5094025	OK
OVERLAPPING TEMPLATE	0.313653	OK
RANK	0.885113	OK
RUNS	0.436975	OK
NONPERIODIC TEMPLATES	0.5094025	OK
SERIAL	0.381633	OK
UNIVERSAL STATISTICAL	0.877240	OK

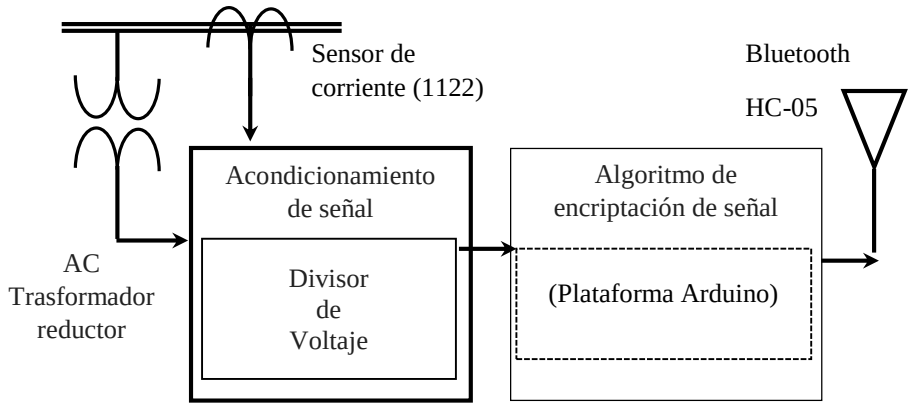
La tabla 6.2, muestra los resultados obtenidos por la suite de pruebas estadísticas del NIST. En ella se puede observar el P-valor arrojado para cada prueba, siendo dichos resultados congruentes con los valores α definidos en la suite. Se evaluó el rendimiento estático del criptosistema utilizando un conjunto de pruebas estadísticas con datos de 1 Mbit arrojando métricas aceptables en cada prueba específica.

6.4 Implementación de Algoritmo en prototipo (física)

El algoritmo pseudoaleatorio son el método logístico, presentado en este documento se implementa en un prototipo para experimentar con datos reales y evaluar las propiedades de aleatoriedad para el criptograma propuesto. De esta forma, se confirma un comportamiento apropiado y apto para cubrir las necesidades de fortalecimiento a la seguridad de los datos.

El esquema del sistema integrado para la creación del prototipo se muestra en la figura 6.5A, donde la corriente y la tensión se miden mediante un sensor de corriente (1122-30 Amperes) y un transformador de CA respectivamente. El acondicionamiento de la señal se aplicó a estas señales para escalar la señal a la plataforma Arduino-UNO. Dentro del sistema Arduino, la conversión analógica a digital (A / D) se desarrolló utilizando un muestreo cada 50 milisegundos. Después de la adquisición, se procesa la señal de energía, antes de la aplicación de encriptación. Una vez que los datos están encriptados, se establece la comunicación con otros dispositivos a través de Bluetooth (transmisor HC-05) incorporado. La figura 6.5B muestra la imagen del prototipo.

A



B

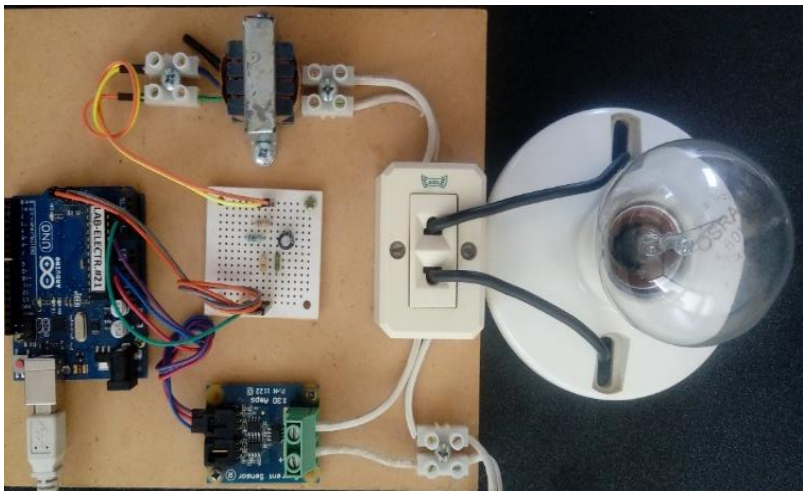


Figura 6.5 Esquema de prototipo. A) Diagrama de bloque de Sistema embebido. B) Imagen de prototipo.

La etapa de adquisición de datos se subdivide en dos subetapas; uno para el acondicionamiento de la señal y el otro para la adquisición de datos. El rendimiento estadístico del criptosistema se evaluó mediante un conjunto de pruebas estadísticas, utilizando 125000 muestras de datos como se muestra en la figura 6.6A y estableciendo el intervalo de parámetros μ (3.86 - 4), y x_t (0,1). La señal cifrada figura 6.6B, evidencia una media de 1.8173^{03} y métricas de varianza de 1.0860^{06} para la señal original, mientras que, para la señal cifrada, la media y la varianza se calcularon como 4.4981^{05} y 6.7240^{10} respectivamente. Cada valor_P correspondiente a una prueba en particular se presenta en la tabla 4 e indica las secuencias producidas por el algoritmo propuesto.

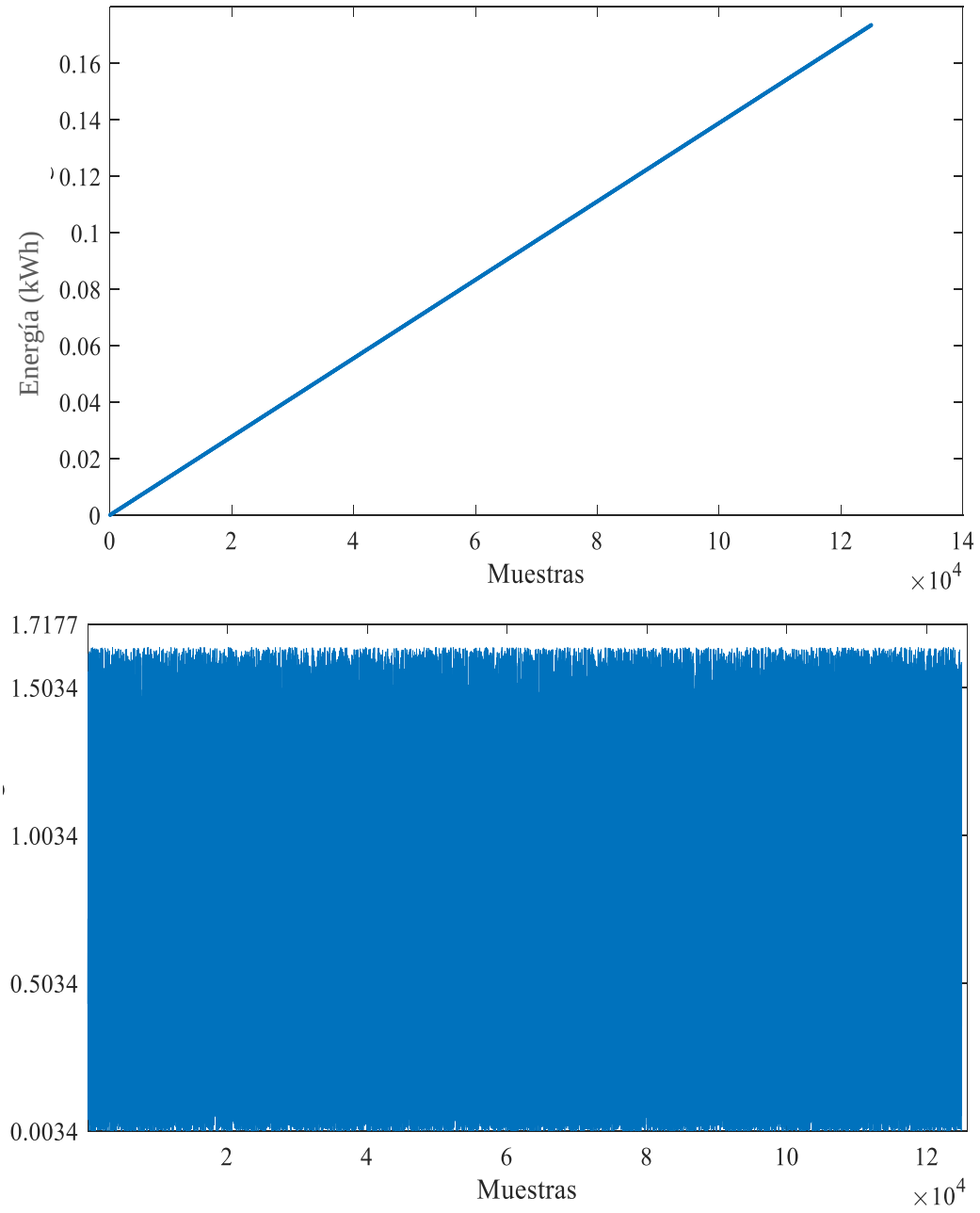


Figura 6. 6 Señal original de consumo de energía eléctrica con 125000 muestras. A) Original. B) Cifrada

Después de la representación gráfica los resultados de cifrado, éstos son evaluados bajo las pruebas estadísticas de aleatoriedad de 15 ensayos NIST como se muestra en la tabla 6.3 [6]. A partir de estos resultados se demuestra que al utilizar solo los métodos (generador congruencial y mapeo logístico) las secuencias no tienen las características estadísticas suficientes para pasar todas las pruebas. Sin embargo, realizando una disyunción exclusiva de ambos métodos las pruebas resultan todas satisfactorias con respecto al valor de significancia. El rendimiento estadístico del criptosistema se evaluó utilizando un conjunto de pruebas estadísticas, utilizando 125000 muestras de datos y configurando el intervalo de parámetro μ en (3.86-4) y condición inicial de x_t (0,1).

Tabla 6.3. Pruebas Nist de los métodos utilizados para el algoritmo

Pruebas	Métodos utilizados				Algoritmo Propuesto			
	Generador Congruencial		Mapeo Logístico		Simulado		Implementado	
	Valor_P	Estado	P-value	Estado	Valor_P	Estado	Valor_P	Estado
Approximate entropy	0	×	0	×	0.8097	✓	0.3679	✓
Block frequency	0.0190	✓	0	×	0.4917	✓	0.8712	✓
Cumulative sums(Forward)	0.0024	✓	0	×	0.4128	✓	0.2456	✓
Cumulative sums(Reverse)	0.0028	✓	0	×	0.3129	✓	0.5297	✓
FFT	0	×	0.0259	✓	0.8043	✓	0.0067	×
Frequency	0	×	0.0379	✓	0.4065	✓	0.3200	✓
Linear complexity	0.6282	✓	0	×	0.7503	✓	0.3372	✓
Longest run	0.3041	✓	0	×	0.5048	✓	0.0470	✓
Non overlapping template	0.3026	✓	0.1060	✓	0.5094	✓	0.3896	✓
Overlapping template	0.2157	✓	0	×	0.3136	✓	0.1526	✓
Rank	0.9352	✓	0.4691	✓	0.8851	✓	0.0712	✓
Runs	0	×	0	×	0.4369	✓	0.6248	✓
Non periodic templates	0	×	0	×	0.5094	✓	0.7154	✓
serial	0	×	0	×	0.3816	✓	0.9645	✓
Universal	0.3954	✓	0	×	0.8772	✓	0.2589	✓

De estos resultados se desprende que los métodos, generador congruencial y mapa logístico, no son suficientes para pasar todas las pruebas de forma independiente; sin embargo, mezclando los métodos tienen éxito en todas las pruebas. Los resultados obtenidos demuestran que todas las métricas NIST se logran bajo simulación utilizando el algoritmo de cifrado propuesto; mientras en el prototipo, la prueba FFT muestra un valor_P bajo, que supone como resultado de una interferencia eléctrica en el circuito.

6.5 Comparativa con otros procesos de cifrado

En esta sección, la fortaleza del algoritmo propuesto se evaluó mediante la versión en color de la imagen de Lena y comparado con el coeficiente de correlación con [1] [7] y [8]. El tamaño de la imagen de Lena seleccionado es de 512 × 512 píxeles y, para mantener el procedimiento descrito en la Sección 6.2, se determinó el grado de entropía y distorsión de la imagen cifrada. Se comparó el coeficiente de correlación ya que en el análisis de seguridad de un proceso criptográfico es esencial para garantizar la fortaleza de la técnica criptográfica. Un histograma de imagen representa la frecuencia de cada píxel y un cifrado adecuado presenta un histograma con una distribución de frecuencia uniforme de los valores de píxeles [9].

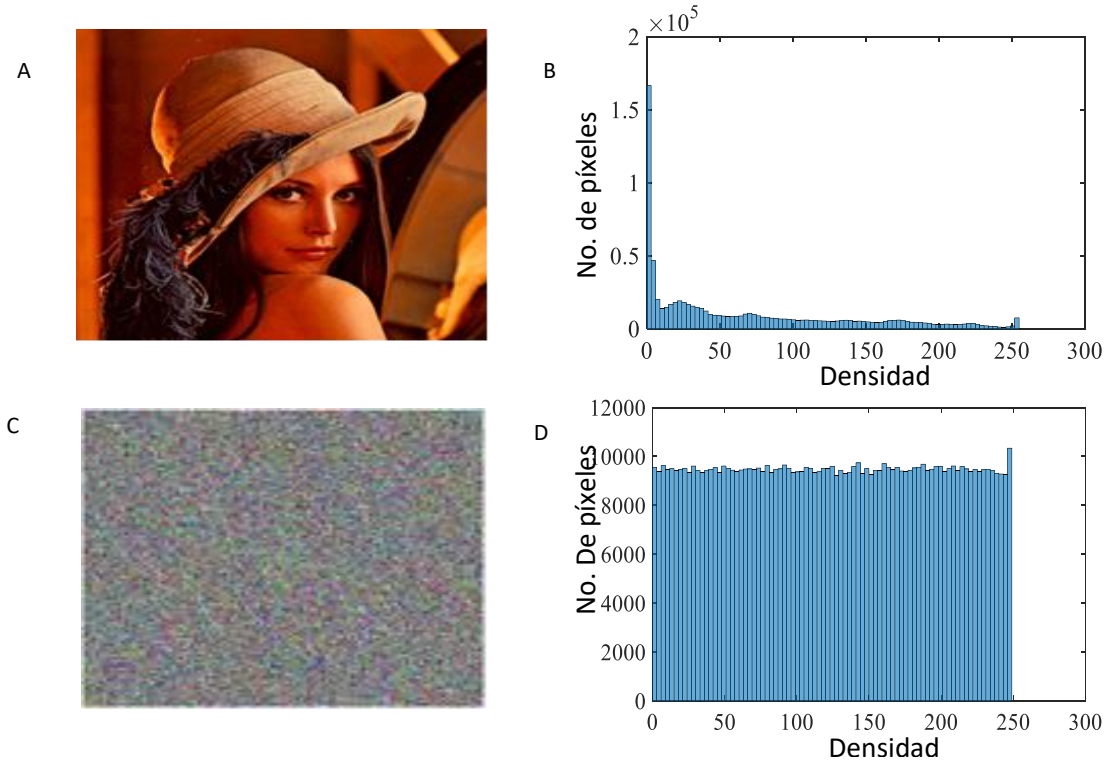


Figura 6.7 Imagen de Lena. A) imagen Original. B) Histograma de imagen original. C) imagen cifrada. D) Histograma de imagen cifrada.

La Figura 6.7A muestra la imagen original, y la Figura 6.7C muestra la imagen cifrada. Del mismo modo, las Figuras 6.7B y 6.7D muestran los histogramas de la imagen original y la imagen cifrada respectivamente.

En la Figura 6.7, se puede apreciar cómo la distribución de frecuencia de los píxeles en el histograma de la imagen cifrada se distribuye de manera uniforme, como se espera en el algoritmo propuesto. Para determinar el nivel de entropía y desorden de la imagen cifrada, se analizó la correlación de 1,000 puntos seleccionados al azar. La Tabla 6.4, presenta los resultados de la correlación horizontal, vertical y diagonal de píxeles adyacentes. Esta tabla también muestra que el algoritmo propuesto genera un coeficiente de correlación más cercano a cero que las otras dos referencias.

Tabla 6.4 Comparación del coeficiente de correlación del algoritmo propuesto con los de otras referencias.

Imagen Cifrada (coeficiente de Correlación)				
Dirección	**algoritmo Propuesto** [Elizalde et al., 2019 [11]	Hossam et al., 2007 [7]	(Chong et al., 2011) [8]	(Jiménez et al., 2015) [1]
Horizontal	0.0074	0.0308	0.0368	0.0270
Vertical	-0.0089	0.0304	-0.0392	-0.0009
Diagonal	-0.0032	0.0317	0.0068	0.0020

Dato que la implementación fue uno de los principales objetivos, la comparación del tiempo de procesamiento se probó por primera vez en una computadora personal bajo Matlab R2015a, con un procesador Intel (R) Celeron 2 Core a 2.16 GHz de frecuencia, 4GB en RAM, ejecutando Windows 10 Home O.S. El tiempo de procesamiento resultante fue de 0,5263 segundos, cifrando 125,000 muestras de datos de consumo de energía eléctrica.

Finalmente, en la Tabla 6.5, se muestra el tiempo de cifrado promedio comparativo tomado de algunas imágenes de Lena con diferentes tamaños. El tiempo de ejecución del algoritmo criptográfico aumenta a una tasa menor que la observada en Li et al. [10], [11]. El análisis de tiempo se realizó en una CPU Core 2 Duo de 2.26 GHz con una notebook de 4 GB de RAM usando Matlab; las mismas características que Li et al. [10].

Tabla 6.5 Tiempo comparativo de cifrado

Tamaño de la imagen (pixeles)	**Tiempo de cifrado(s)**	
	Algoritmo propuesto (Elizalde et al., 2019 [11]	(Li et al., 2016)[10]
256 x 256	0.84	0.90
512 x 512	1.79	1.82
1024 x 1024	8.46	13.08
2048 x 2048	33.45	76.38

6.6 Cifrado con método de Mapeo Bernoulli

El otro algoritmo propuesto es bajo el método de Bernoulli generando estructuras cifradoras que simulan caos utilizados para fortalecer la seguridad de los datos de medición de energía eléctrica, presentando buenas características estadísticas, y refiriendo condiciones de seguridad contra diferentes ataques. El método criptográfico propuesto se basa en los mapas caóticos de Bernoulli que no tiene islas de estabilidad dentro de su región caótica, por lo tanto, su parámetro de control puede ser modificado en un intervalo específico en (0,1) de los números reales. Este mapa puede generar secuencias pseudoaleatorias con distribuciones estadísticas muy cercanas a la distribución uniforme.

Se realizan pruebas experimentales utilizando una señal de energía eléctrica fuera de línea, los resultados obtenidos demuestran que el proceso de cifrado/descifrado no afectará la eficiencia de codificación, manteniendo una tasa de bits y un bajo consumo de recursos computacionales. Para validar el algoritmo se somete a un análisis de seguridad basado en valoración estadística de la suite NIST, pruebas que son superadas, lo que indica, que la información o los datos quedan criptográficamente protegidos.

Para la validación del criptosistema se utiliza la teoría estadística que prueba la aleatoriedad evaluada a través de la suite NIST que se compone de 15 pruebas estadísticas para la aprobación de generadores de números aleatorios y generadores de secuencias aleatorias para aplicaciones criptográficas, que se ejecutan de forma sucesiva sobre la secuencia de bits.

Para evaluar el algoritmo de cifrado propuesto previamente, el cual está enfocado para trabajar con señales de energía eléctrica y datos, de un medidor digital de energía eléctrica en el marco de las redes inteligentes; al igual que la

prueba anterior, se desarrolla un circuito de prueba de corriente alterna a 60 Hz, en el que se mide el voltaje y la corriente para calcular la potencia, y con ello la energía que consume una carga resistiva. En la figura 6.8A, se presenta la curva de consumo de energía eléctrica obtenida, cuando la carga resistiva es de 144Ω.

Esta sección tiene como objetivo examinar la eficacia del algoritmo de cifrado haciendo uso de criterios que permitan validar sus fortalezas y debilidades, mediante el análisis visual y estadístico. Mediante la comparación de la figura 6.8A con la figura 6.8B, se puede ver que no hay similitudes perceptibles entre la señal de consumo de energía eléctrica original y la cifrada. No hay información visual que se pueda observar en la versión procesada por el algoritmo de cifrado propuesto basado en el modelo de Bernoulli.

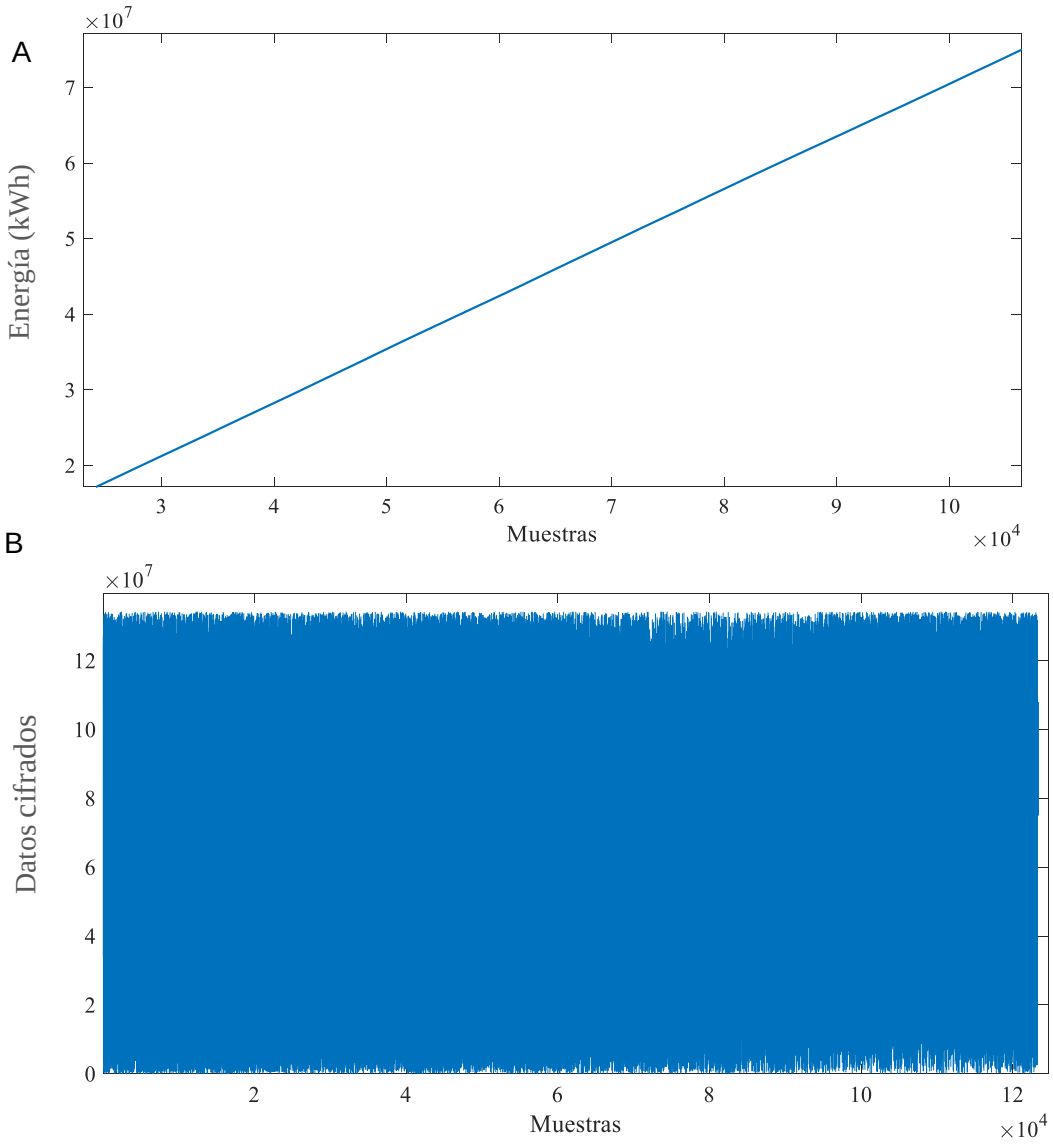


Figura 6.8 Señal de consumo de energía eléctrica. A) Señal original. B) Señal cifrada.

La evaluación de confusión implica el análisis de histograma para la señal original y cifrada. En la figura 6.9, se presenta el histograma de la señal cifrada frente a la señal original, donde éstas siguen una distribución uniforme.

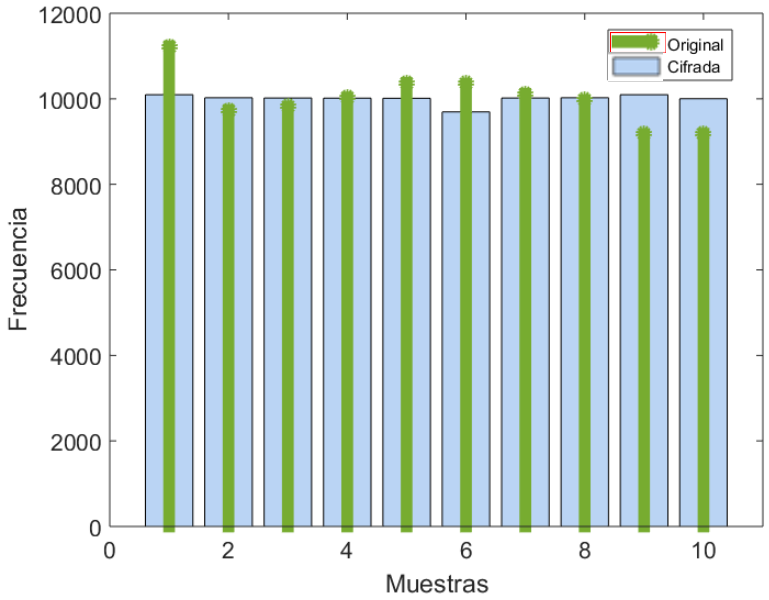


Figura 6.9 Histograma de señal original y cifrada

Para evaluar la independencia en las variables implicadas se analiza el diagrama de dispersión que muestra la figura 6.10, con la relación de correlación entre la señal original y la señal cifrada, en este caso revelan independencia entre sí.

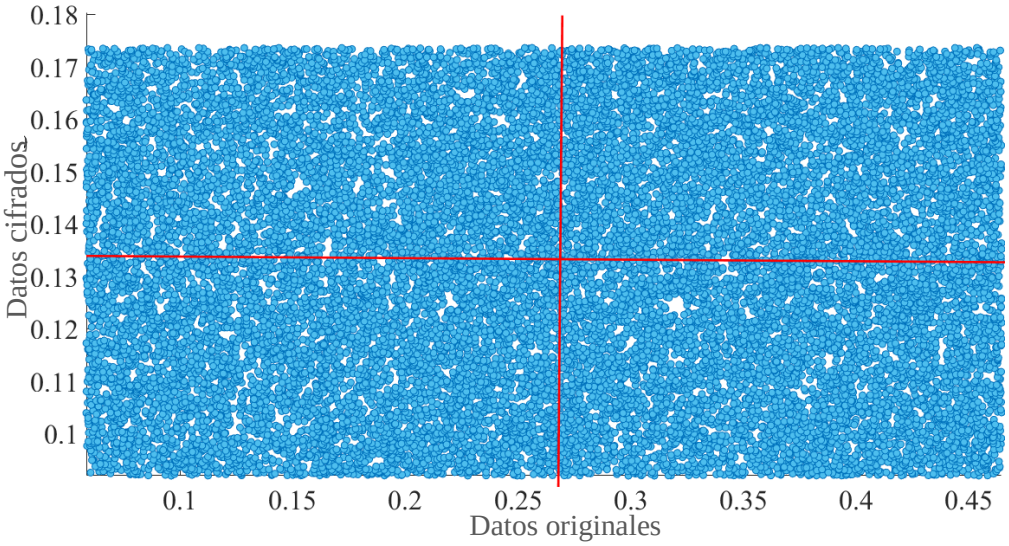


Figura 6.10 Diagrama de dispersión

Con ello se puede afirmar que no existe correspondencia o ésta es muy baja como puede mostrarse numéricamente a través del coeficiente de correlación (ver tabla 6.6), y se demuestra numéricamente a través del coeficiente de correlación. La

información mutua resultante de la comparativa de dos vectores (datos originales vs datos cifrados) de 3200 muestras cada uno, es de 0.000202.

Para medir la correlación, se utiliza el coeficiente de correlación de Pearson. El coeficiente varía de -1 a 1. Una correlación de 1 muestra una correlación positiva perfecta, mientras que -1 muestra una correlación negativa perfecta. Una correlación de 0 no muestra ninguna relación.

Tabla 6.6 Correlación entre señal original y la señal cifrada

	Señal Original	Señal Cifrada
Señal original	1.0000	-0.0001
Señal Cifrada	-0.0001	1.0000

Después de haber evaluado la señal cifrada se procede al descifrado de ésta, en donde la señal original es recuperada cuasi al 100% como puede apreciarse en la figura 6.11, usando el algoritmo de descifrado propuesto a través del modelo de Bernoulli, teniendo en cuenta los parámetros y condiciones iniciales.

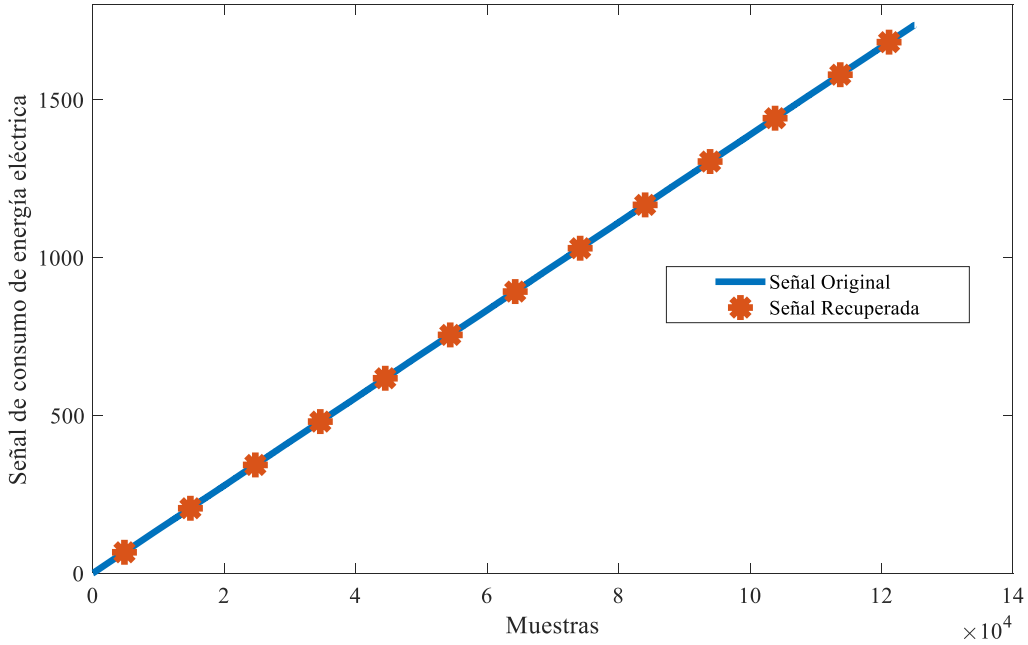


Figura 6.11 Señal original y sobrepuesta la señal recuperada.

Se muestra el resultado de error cuadrado medio en tabla 6.7, que demuestra total similitud entre los valores de la señal original y la recuperada después de aplicar el algoritmo de descifrado. Además, se agregan resultados de la matriz de coeficientes de correlación, que evidencian la total similitud entre los valores de la

señal original y la recuperada después de aplicar el algoritmo de descifrado. La tabla 6.8 evidencia la concentración de métricas.

Tabla 6.7. Correlación entre señal original y la señal recuperada

	Señal Original	Señal recuperada
Señal original	1.0000	0.9999
Señal Recuperada	0.9999	1.0000

Tabla 6.8. Concentración de métricas

Estadísticas	**Obtenidas**	**Esperadas**
coeficiente de Correlación	0.0007	0
Entropía	7.9617	8
Error cuadrático medio	0	0

Para verificar la eficacia del criptosistema antes mencionado, algunos experimentos se han llevado a cabo como cambiar algún valor de los parámetros y/o condiciones iniciales; como en este caso en x_o=.0708 μ=.396, se cambió la última cifra del valor de μ= 0.360. Cabe señalar que el sistema de ecuaciones caóticas que se utilizan en el cifrado; tanto los parámetros y condiciones iniciales que sirven de semilla en la generación de la señal caótica deben ser perfectamente sincronizados al momento de obtener el descifrado dado que una pequeña variación de las mismos da como resultado que no se recupere la señal original como se muestra en la figura 6.12. Para corroborar la correlación se mide el coeficiente evidenciando en la tabla 6.7 que existe muy poca correlación entre la señal original y recuperada.

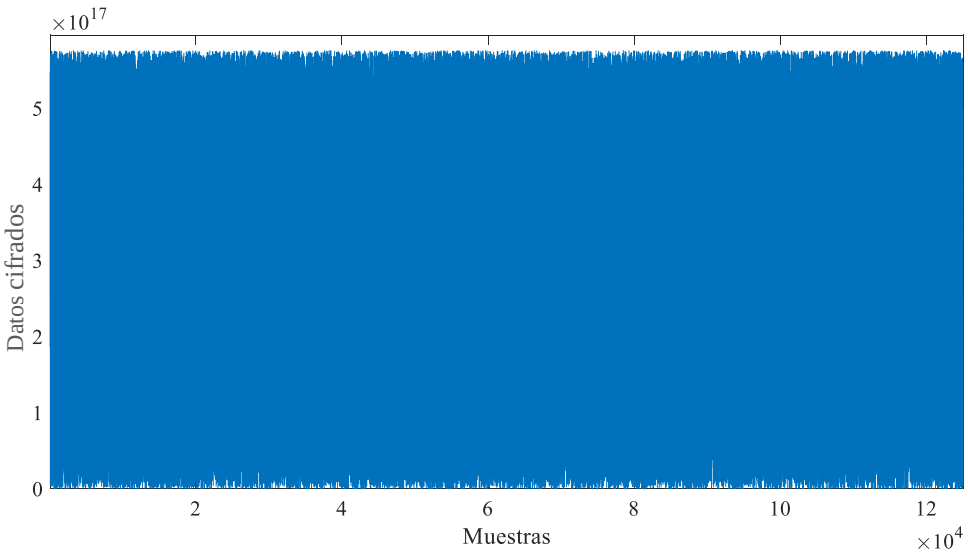


Figura 6.12 Señal recuperada con un cambio de bit en condición inicial de una función Bernoulli Map.

Tabla 6.7. Correlación entre señal original y la señal recuperada

	Señal Original	Señal recuperada con un cambio en el parámetro
Señal original	1.0000	-0.0020
Señal Recuperada con un cambio en el parámetro	-0.0020	1.0000

El criptograma debe ser invulnerable a los ataques estadísticos en aplicaciones criptográficas. La aleatoriedad es importante para pseudo-generadores de números aleatorios [2]. Por esta razón, la aleatoriedad de la señal cifrada resultante se evaluó utilizando el NIST (Instituto Nacional de Estándares y Tecnología) conjunto de pruebas de aleatoriedad estadística[6].

Obteniendo un nivel de significancia por encima de 0,01 para cada prueba con el fin de aceptar la aleatoriedad de secuencias de bits. En cada prueba se calcula un P-valor, con un nivel de significancia α =1%. Un P-valor mayor que α significa que la secuencia es aleatoria con una certeza del 99%. Los resultados de las pruebas de aleatoriedad se dan en la Tabla 6.9.

Al ser inspirado el criptosistema en el algoritmo A5 que es un algoritmo cifrador usado para proporcionar privacidad en la comunicación bajo el estándar GSM, se realiza el cifrado de la señal de consumo de energía eléctrica bajo este algoritmo y se obtienen los resultados siguientes que pueden observarse en la tabla 6.9 donde se muestra la comparativa de los dos algoritmos.

Tabla 6.2. Pruebas comparativas A5 Vs Criptosistema propuesto de Bernoulli

Pruebas NIST	Algoritmo A5		Algoritmo Bernoulli	
	Valor –P	Conclusión	Valor -P	Conclusión
APPROXIMATE ENTROPY	0.999380	**Aceptada**	0.817922	**Aceptada**
BLOCK FREQUENCY	0.381565	**Aceptada**	0.682126	**Aceptada**
CUMULATIVE SUMS (FORWARD)	0.539032	**Aceptada**	0.902442	**Aceptada**
CUMULATIVE SUMS (REVERSE)	0.222317	**Aceptada**	0.937951	**Aceptada**
FFT	0.000000	**Rechazada**	0.919596	**Aceptada**
FRECUENCY	0.421397	**Aceptada**	0.919596	**Aceptada**
LINEAR COMPLEXITY	0.000000	**Rechazada**	0.270578	**Aceptada**
LONGEST RUNS OF ONES	0.175339	**Aceptada**	0.932668	**Aceptada**
OVER TEMPLATE OF ALL ONES	0.313231	**Aceptada**	0.151471	**Aceptada**
RANDOMEXCURSIONS VARIANT	0.000000	**Rechazada**	0.543940	**Aceptada**
RANDOM EXCURSIONS	0.000000	**Rechazada**	0.390738	**Aceptada**
RANK	0.487872	**Aceptada**	0.487872	**Aceptada**
RUNS	0.000000	**Rechazada**	0.988839	**Aceptada**
NONPERIODIC TEMPLATES	0.000000	**Rechazada**	0.521226	**Aceptada**
SERIAL	1.000000	**Aceptada**	0.544026	**Aceptada**
UNIVERSAL STATICAL	0.216652	**Aceptada**	0.892742	**Aceptada**

Como puede observarse solo 10 de las 16 pruebas propuestas en la suite NIST para evaluar la aleatoriedad fueron exitosas al cifrar con el algoritmo A5.

La fuerza del algoritmo propuesto se evaluó mediante el cifrado de la versión en color de la imagen de Lena con tamaño de 512 × 512 píxeles y se compara con el coeficiente de correlación con [1], [7], [8] y [11]. Se determinó el grado de entropía y distorsión de la imagen cifrada y el coeficiente de correlación. Una buena imagen de cifrado tiene una distribución de frecuencia uniforme de los valores de píxeles [9]. La Figura 6.12A muestra la imagen original, y la Figura 6.12C muestra la imagen cifrada. Del mismo modo, las Figuras 6.12B y 6.12D muestran los histogramas de la imagen original y la imagen cifrada respectivamente. Se espera que el diseño del desarrollo de cifrado sea de peso ligero y exista la posibilidad de implementarse en un diseño de hardware de bajos recursos y limitado de energía.

La tabla 6.10, presenta los resultados de la correlación horizontal, vertical y diagonal de píxeles adyacentes. Esta tabla también muestra que el algoritmo propuesto genera un coeficiente de correlación más cercano a cero que las otras dos referencias.

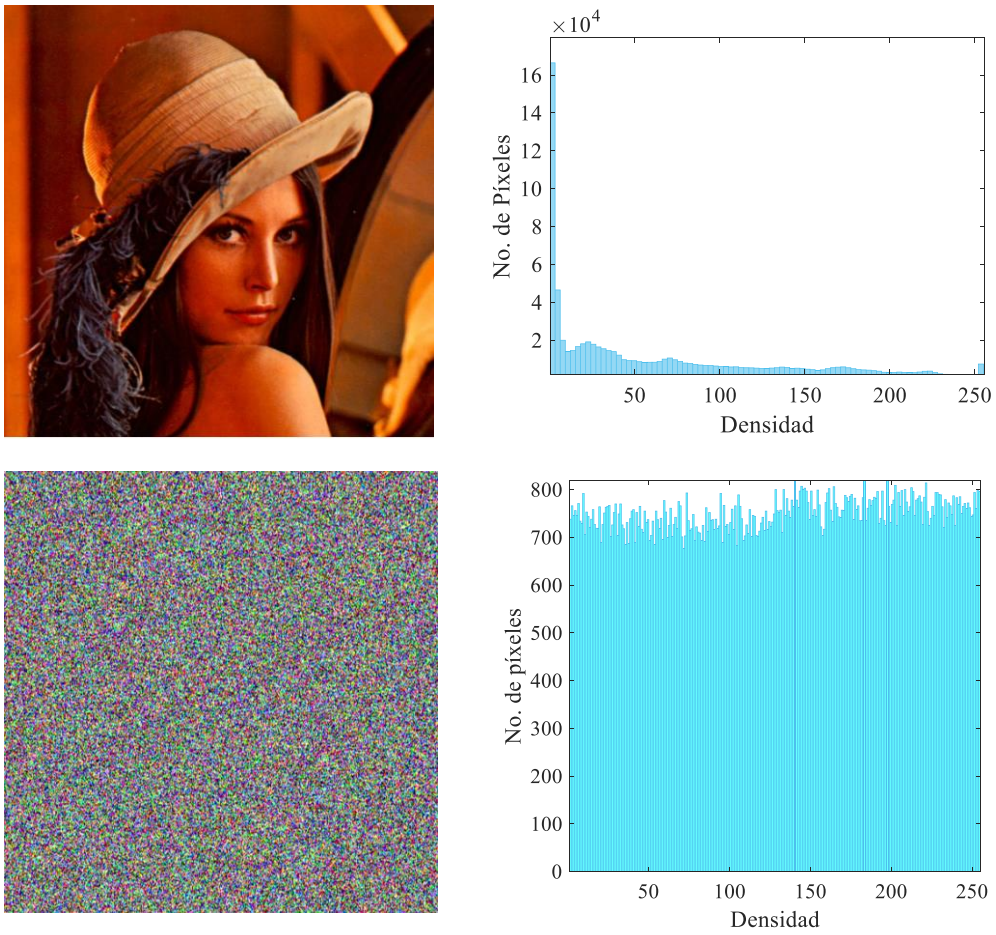


Figura 6.13 Imagen Lena. (A) Imagen Original. (B) Histograma de imagen original. (C) Imagen cifradas. (D) Histograma de imagen cifrada.

Tabla 6.10. Comparación de coeficiente de correlación algoritmo propuesto con otras referencias.

Imagen Cifrada(coeficiente de Correlación)					
Dirección	**Algoritmo Propuesto [Elizalde et al., 2019[11]**	Algoritmo Propuesto Bernoulli	Hossam et al., 2007 [7]	(Chong et al., 2011) [8]	(Jiménez et al., 2015) [1]
Horizontal	0.0074	-0.0066	0.0308	0.0368	0.0270
Vertical	-0.0089	0.0079	0.0304	-0.0392	-0.0009
Diagonal	-0.0032	-0.0089	0.0317	0.0068	0.0020

Los resultados de la evaluación en la Suite del NIST se presentan en la tabla 6.11 que evalúan la presencia de un patrón, el cual, si es detectado indicaría que la secuencia no es aleatoria. El nivel de significancia α para todas las pruebas de la suite se establece en 1%.

Tabla 6.11. NIST Bernoulli (Datos fuera de Línea)

Suite de pruebas Nist	Valor P Obtenido	Estado
Approximate Entropy	0.365391	OK
Block Frequency	0.799751	OK
Cumulative Sums	0.905318	OK
Cumulative Sums	0.972564	OK
Fft	0.941477	OK
Frecuency	0.902899	OK
Linear Complexity	0.539939	OK
Longest Runs of Ones	0.847100	OK
Nonoverlapping Template	0.782516	OK
Overlapping Template	0.618325	OK
Rank	0.032083	OK
Runs	0.282816	OK
Nonperiodic Templates	0.634300	OK
Serial	0.381633	OK

Las pruebas estadísticas aplicadas al criptograma dan como resultado que los datos cifrados provienen de secuencias con alto grado de aleatoriedad, lo que se traduce en un alto nivel de seguridad, dado que el proceso de manipulación conserva su entropía natural, por tanto, la hace poco vulnerable a posibles ataques externos. Con ello se comprueba que efectivamente los datos que se obtienen provienen de secuencias con alto grado de aleatoriedad; con lo cual se dificulta para un atacante determinar algún orden en los datos, por lo que el cifrado se puede considerar válido y confiable.

6.7 Referencias

[1]. M. Jiménez-Rodríguez, et al., “Sistema Para Codificar Información Implementando Varias Órbitas Caóticas,” Ingeniería, Investigación y Tecnología, vol 16(3), pp. 335-343, 2015.

[2]. A. Radwan, et al., "Symmetric Encryption Algorithms Using Chaotic and Non-Chaotic Generators: A review," Journal of Advanced Research, vol. 7(2), pp. 193-208, 2016.

[3]. C. Shannon, “Communication Theory of Secrecy Systems,” Bell System Technical Journal, vol.28, pp. 656-715, 1949.

[4]. A. Kerckhoffs, “La Cryptographie Militaire,” Journal des sciences militaires, vol 9, pp. 161-191, 1883

[5]. D. Pavanello, et al., "Statistical Functions and Relevant Correlation Coefficients of Clearness Index," Journal of Atmospheric and Solar-Terrestrial Physics, vol. 130-131, pp. 142-150, 2015.

[6]. L. Bassham, et al.,"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST, 2018. [Online]. Available: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic. [Accessed: 25- Jan- 2016].

[7]. E.A. Hossam, et al., “An efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption,” Informatica, vol 31, pp. 121–129, 2007.

[8]. C. Fu, et al., "A Novel Chaos-Based Bit-level Permutation Scheme for Digital Image Encryption," Optics Communications, vol. 284(23), pp. 5415-5423, 2011.

[9]. R. Parvaz and M. Zarebnia,"A Combination Chaotic System and Application in Color Image Encryption," Optics & Laser Technology, vol. 101, pp. 30-41, 2018.

[10]. C. Li, G. Luo, K. Qin and C. Li, "An Image Encryption Scheme Based on Chaotic Tent Map," Nonlinear Dynamics, vol. 87, no. 1, pp. 127-133, 2016.

[11]. Elizalde-Canales, F. Rivas-Cambero, I. Rebolledo-Herrera, L. and Camacho-Bello C.”Pseudo-Random Bit Generator Using Chaotic Seed for Cryptographic Algorithm in Data Protection of Electric Power Consumption”. International Journal of Electrical and Computer Engineering. Vol. 9, No. 2, pp. 1399-1409, 2019.

CONCLUSIONES

Se presenta el diseño y evaluación de dos algoritmos generadores de bits seudoaleatorios con cifrado caóticos, basado en secuencias dinámicas. Estas secuencias se generan a partir de funciones unidimensionales de mapeo logístico acoplado a un generador lineal congruencial y a través de Bernoulli; cuyos parámetros constituyen la clave secreta para el sistema de codificación. Los algoritmos de cifrado, se proponen para su implementación en hardware integrado de bajo costo centrado en la mejora de las funciones de seguridad, considerando bajos recursos computacionales sin descuidar la velocidad de ejecución.

El generador de cifrado caótico se aplica para cifrar la información del consumo de energía eléctrica, obtenida por simulación y por un prototipo de medición de energía, y luego las pruebas de cifrado y descifrado se llevan a cabo en un entorno ideal, recuperando así la señal original. Los algoritmos se evalúan con las funciones estadísticas principales y se validan bajo las pruebas NIST además de la aplicación en la imagen de Lena como base de comparación. Durante las pruebas experimentales, todas las métricas del NIST se lograron bajo la simulación, excepto la prueba FFT bajo prototipo. Se estima que esto es una consecuencia de la interferencia eléctrica en el circuito de prototipo, por lo tanto, la mejora del circuito de PCB se realizará en trabajos futuros.

Los algoritmos presentados en esta investigación ofrecen un alto grado de confidencialidad, ya que la información solo se puede recuperar utilizando la misma clave para generar el sistema criptográfico. En este caso, tiene un error cuadrático medio de 3.469111 en las pruebas de sensibilidad, que indica qué tan lejos están los datos descifrados relacionados con los datos originales. Se observó un tiempo de procesamiento de 0,5263 segundos en un procesador Intel Celeron de 2.16 GHz.

La evaluación estadística muestra una correlación significativamente decreciente entre los valores cifrados y los originales del orden de 10-3. Se confirma que el criptograma muestra un alto grado de imprevisibilidad también evidencia una entropía muy cercana a 8, lo que significa que el criptograma ofrece la confidencialidad esperada para la información y, por lo tanto, disminuye la vulnerabilidad a los ataques cibernéticos. Además, se realizan pruebas para medir el tiempo de procesamiento, la entropía y el grado de trastorno utilizando la imagen de Lena, obteniendo métricas comparables a las reportadas en la literatura revisada. En futuras investigaciones, será necesario optimizar el algoritmo, para que este pueda ser aplicado para el cifrado de flujo.

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 2, April 2019, pp. 1399~1409
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i2.pp1399-1409

Pseudo-random bit generator using chaotic seed for cryptographic algorithm in data protection of electric power consumption

Francisca Elizalde-Canales, Iván Rivas-Cambero, Lucio Rebolledo-Herrera, Cesar Camacho-Bello
Faculty of Engineering Universidad Politécnica de Tulancingo, México

Article Info

Article history:

Received May 9, 2018
Revised Nov 2, 2018
Accepted Nov 20, 2018

Keywords:

Cryptography
Decryption
Encryption algorithm
Statistical tests

ABSTRACT

Cryptographic algorithms have played an important role in information security for protecting privacy. The literature provides evidence that many types of chaotic cryptosystems have been proposed. These chaotic systems encode information to obviate its orbital instability and ergodicity. In this work, a pseudo pseudo-random cryptographic generator algorithm with a symmetric key, based on chaotic functions, is proposed. Moreover, the algorithm exploits dynamic simplicity and synchronization to generate encryption sub-keys using unpredictable seeds, extracted from a chaotic zone, in order to increase their level of randomness. Also, it is applied to a simulated electrical energy consumption signal and implemented on a prototype, using low hardware resources, to measure physical variables; hence, the unpredictability degree was statistically analyzed using the resulting cryptogram. It is shown that the pseudo-random sequences produced by the cryptographic key generator have acceptable properties with respect to randomness, which are validated in this paper using National Institute of Standards and Technology (NIST) statistical tests. To complement the evaluation of the encrypted data, the Lena image is coded and its metrics are compared with those reported in the literature, yielding some useful results.

Corresponding Author:

Francisca Elizalde-Canales,
Department of Automation and Control,
Universidad Politecnica de Tulancingo,
Calle Ingenierías # 100. Col. Huapalcalco, Tulancingo, Hidalgo, C.P. 43629, México.
Email: francisca.elizalde@upt.edu.mx

1. INTRODUCTION

The electric power industry has become increasingly vulnerable because of smart grid growth used for interconnection of consumers with power generation, transmission, and distribution trought information technologies based on communication systems. In this sense, smart meters could inadvertently provide unauthorized access to consumer data, which is a concern in the management of information for the adoption of intelligent networks in the face of the increasing possibility of cyber-attacks, since security has not traditionally been considered a requirement in design of integrated systems and the application of security techniques specific to these devices is still incipient [1]-[4].

Cryptographic algorithms are the backbone of the protection of highly sensitive data. The selection of a suitable crypto-algorithm will dynamically affect the lifespan and performance of a device in terms of battery-life, hardware memory, computation latency, and communication bandwidth. In the current developments of resource-constrained environments, the trend is shifting towards lightweight algorithmic designs [5], [6].

VULNERABILIDAD EN LOS SISTEMAS DE MEDICIÓN INTELIGENTE

F. A. Elizalde Canales[a], I.J. Rivas Cambero[b], A.M. Godinez Jarillo[c], E. Cortes Palma[d]

Universidad Politécnica de Tulancingo
francisca.elizalde@upt.edu.mx[a], ivan.rivas@upt.edu.mx[b]
alicia.godinez@upt.edu.mx[c], elizabeth.cortes@upt.edu.mx[d]

RESUMEN

La red inteligente (Smart Grid) es una modernización de la red eléctrica, para supervisar, inspeccionar, proteger y optimizar automáticamente el control y la fiabilidad de las operaciones de la red eléctrica a través de sistemas de monitoreo y control distribuido. A la red inteligente se integran las de Tecnologías de Información y Comunicación (TIC) que permiten el monitoreo y control remoto, sin embargo, la integración expone a los sistemas de energía inteligentes a las amenazas de seguridad y vulnerabilidad, que podrían verse comprometidos por usuarios maliciosos y atacantes, debido al aumento de la conectividad y la apertura de Internet.

En este trabajo se realiza un análisis de los requisitos de seguridad, amenazas y vulnerabilidades en los sistemas de medición inteligente para que facilite la comprensión y visualización de los principales riesgos cibernéticos a fin de que fortalezca la seguridad y establezca contramedidas. El caso específico que se aborda en este artículo es el de los medidores inteligentes (Smart Meter), los que se encargan de registrar la información de cada consumidor para que sea recolectada y procesada para el cálculo de la factura de consumo, sin embargo esta información puede ser usada con fines diferentes.

La finalidad de este artículo es que se comprenda cómo los atacantes maliciosos pueden comprometer la seguridad de los sistemas de medición inteligente refiriendo ataques sofisticados y vulnerabilidades así como su impacto.

1. INTRODUCCIÓN

Uno de los principales objetivos de la red inteligente es que los usuarios finales tengan información sobre sus consumos y dispongan de herramientas que favorezcan el control eficiente de sus cargas, generando así eficiencia energética [1].

Las comunicaciones para las aplicaciones de redes inteligentes manejan datos sensibles, la seguridad física como la seguridad cibernética y la privacidad constituyen factores clave para su amplio despliegue y adopción. Para determinar las vulnerabilidades dentro de estas aplicaciones se examina la metodología de ataque, debido a que los métodos exactos pueden variar. La

Pistas Educativas, No. 120, noviembre 2016. México, Tecnológico Nacional de México/Instituto Tecnológico de Celaya.

ALGORITMO DE CIFRADO SIMÉTRICO BASADO EN MAPEO LOGÍSTICO Y TRANSFORMADA RÁPIDA DE FOURIER

Francisca Angélica Elizalde Canales
Universidad politécnica de Tulancingo
Francisca.elizalde@upt.edu.mx

Iván de Jesús Rivas Cambero
Universidad politécnica de Tulancingo
Ivan.rivas@upt.edu.mx

Resumen

Las herramientas estadísticas utilizadas en la criptografía desde la antigüedad hasta nuestros días, son muy útiles en el criptoanálisis de sistemas de cifrado dado que ofrecen un buen instrumento para la identificación del sistema de cifrado utilizado en un criptograma. Los algoritmos criptográficos son cada vez más necesarios para garantizar la confidencialidad de los datos en la transmisión de forma segura a través de canales de comunicación inseguros.

En éste trabajo se presenta un algoritmo de cifrado simétrico, cuya implementación está basada en el acoplamiento de mapeo logístico, un generador congruencial lineal, y la trasformada rápida de Fourier. Como parte del proceso se generan subclaves de cifrado a través de una semilla extraída de una zona caótica para aumentar su nivel de aleatoriedad. Se realiza un análisis al criptograma, en particular, con pruebas estadísticas sobre datos cifrados, con el fin de determinar su impredecibilidad en secuencias generadas, evaluando las propiedades de independencia y aleatoriedad. Se obtienen resultados en simulación que muestran una notable distorsión en los datos cifrados con respecto a los originales, que, en términos de seguridad, disminuye su vulnerabilidad ante ataques externos.

Palabra(s) Clave(s): Algoritmo de cifrado, criptograma, descifrado, pruebas estadísticas.

Artículo

Revista de Cómputo Aplicado

Septiembre 2017 Vol.1 No.3 38-49

Algoritmo criptográfico con semilla caótica y generador congruencial para fortalecer la seguridad de los datos transmitidos de forma inalámbrica

ELIZALDE-CANALES, Francisca Angélica*†, RIVAS-CAMBERO, Iván de Jesús, ARROYO-NÚÑEZ, José Humberto y RUEDA-GERMÁN, Clementina

Recibido Julio 13, 2017; Aceptado Septimebre 15, 2017

Resumen

Los algoritmos criptográficos juegan un papel importante en la seguridad de la información, principalmente en el fortalecimiento de la privacidad de los datos. Los sistemas caóticos pueden ser empleados en la codificación de la información, debido a su inestabilidad orbital y ergodicidad. En este trabajo se propone la aplicación de un algoritmo de cifrado de clave simétrica basado en funciones caóticas de mapeo logístico para generar subclaves de cifrado a través semillas impredecibles extraídas de las zonas caóticas para aumentar su nivel de aleatoriedad. El algoritmo es aplicado sobre una señal simulada de consumo de energía eléctrica. Se genera un criptograma, el cual es analizado estadísticamente para determinar el grado de impredecibilidad; se obtienen propiedades adecuadas en términos de calidad de la aleatoriedad, mismos que son validados con las pruebas estadísticas que establece El Instituto Nacional de Estándares y Tecnología (NIST).

Algoritmo de cifrado, pruebas estadísticas, criptograma, descifrado

Abstract

The cryptographic algorithms play an important role in the security of the information for the strengthening of the privacy. Chaotic systems can be used in the coding of information, due to their orbital instability and ergodicity. This work proposes the application of a symmetric key cryptographic algorithm based on chaotic logistical mapping functions to generate encryption subkeys through unpredictable seeds extracted from the chaotic zones to increase their level of randomness. The algorithm is applied on a simulated electrical energy consumption signal. A cryptogram is generated, which is statistically analyzed to determine the degree of unpredictability; appropriate properties are obtained in terms of quality of randomness, which are validated with the statistical tests established by the National Institute of Standards and Technology (NIST). Application of seed Congruential to strengthen the security of the data transmitted wirelessly.

Encryption algorithm, statistical tests, cryptogram, decryption

Citación: ELIZALDE-CANALES, Francisca Angélica, RIVAS-CAMBERO, Iván de Jesús, ARROYO-NÚÑEZ, José Humberto y RUEDA-GERMÁN, Clementina. Algoritmo criptográfico con semilla caótica y generador congruencial para fortalecer la seguridad de los datos transmitidos de forma inalámbrica. Revista de Cómputo Aplicado 2017, 1-3: 38-49

* Correspondencia al Autor (Correo Electrónico: francisca.elizalde@upt.edu.mx)
† Investigador contribuyendo como primer autor.

Artículo

Revista de Ingeniería Innovativa

Junio 2017 Vol.1 No.2 9-16

Modulación-Demodulación en amplitud para el proceso de sincronía eléctrica

RUEDA-GERMÁN, Clementina†*, RIVAS-CAMBERO, Iván de Jesús, ARROYO-NÚÑEZ, José Humberto y ELIZALDE-CANALES, Francisca Angélica

Departamento de Energías Renovables, Universidad Politécnica de Tulancingo

Recibido 24 de Abril, 2017; Aceptado 19 de Junio, 2017

Resumen

Los requisitos para la interconexión entre una fuente de generación de energía distribuida a pequeña escala y el sistema eléctrico nacional, van ligados con la sincronía eléctrica; un proceso en el que una señal de referencia interna formada por un algoritmo de control, permite que la señal de salida de un convertidor de potencia opere en sincronismo con la componente fundamental de la red. La señal conformada mediante el convertidor deberá permanecer en un rango de frecuencia entre 59.5 a 60.5 Hz sintonizada en fase. La transformada de Hilbert es una herramienta matemática que sirve para detectar la envolvente compleja de una señal modulada por una portadora, empleada en sistemas de telecomunicaciones. En este trabajo se adapta un demodulador de amplitud basado en la transformada de Hilbert, una señal de referencia es modulada empleando una senoidal de mayor frecuencia, para después demodularla y obtener su envolvente, esta contiene información de fase y frecuencia con el fin de fortalecer el proceso de enganche de un PLL (Phase Locked Loop), siendo este modelo de fácil implementación e idóneo ante cambios abruptos de amplitud, frecuencia y fase, evitando la perdida de sintonía con la señal de referencia.

Amplitud, modulación, Transformada de Hilbert, envolvente, PLL

Abstract

The requirements for the interconnection between a small-scale distributed power generation source and the national electricity system are associated to the electrical synchrony that is a process in which an internal reference signal formed by a control algorithm generates an output signal in a power converter in synchrony with the fundamental component of the electrical grid. The signal generated by the power converter must remain in a frequency range between 59.5 to 60.5 Hz, tuned in phase. The Hilbert transform is a mathematical tool that is used to detect the complex envelope of a signal modulated by a carrier; it is used in telecommunications systems. In this work, an amplitude demodulator based on the Hilbert transform is adjusted, a reference signal is modulated using a higher frequency sine signal, then use a demodulator to obtain the envelope, this contains the phase and frequency information in order to strengthen the PLL (Phase Locked Loop) tune in process, this model is easy to implement and also suitable for abrupt changes in amplitude, frequency and phase, avoiding the loss of tuning with the reference signal.

Amplitude, modulation, Hilbert Transform, envelope, PLL

Citación: RUEDA-GERMÁN, Clementina, RIVAS-CAMBERO, Iván de Jesús, ARROYO-NÚÑEZ, José Humberto y ELIZALDE-CANALES, Francisca Angélica. Modulación-Demodulación en amplitud para el proceso de sincronía eléctrica. Revista de Ingeniería Innovativa 2017. 1-2:9-16

1

Artículo Revista de Ciencias Naturales y Agropecuarias

Septiembre, 2017 Vol.4 No.12, 1-4

Techado de Andador con Paneles Solares en la Universidad Politécnica De Tulancingo

FLORES-GARCIA, Francisco Armando†*, COYOTL-MIXCOATL, Felipe, ELIZALDE-CANALES, Francisca Angélica, CASTILLO-MIMILA, Diego Fernando

Universidad Politecnica de Tulancingo

Recibido 15 de Mayo, 2017; Aceptado 04 de Julio, 2017

Resumen

En el ser humano, una exposición prolongada a la radiación UV solar puede producir efectos agudos y crónicos en la salud de la piel, los ojos y el sistema inmunitario. Los niveles de radiación UV registrados durante 5 años en el campus de la universidad Politécnica de Tulancingo presentan una media de 12 IUV con picos hasta de 15 IUV a las 14 horas. Este trabajo propone el techado de andadores con paneles solares que producirán 20,000 KWh. para abastecer del 50% de la electricidad que consume la universidad, Colocados estos, sobre una estructura metálica en los andadores que conectan los edificios del campus. Beneficio social: Se protege de la radiación solar extrema a toda la comunidad universitaria que transita de edificio a edificio. Beneficio ecológico: Al generar energía eléctrica por medios fotovoltaicos se disminuyen las emisiones de CO2. Para la vida útil de este proyecto se dejan de emitir 2,700 toneladas de CO2. Beneficio económico: El sistema fotovoltaico se interconectara con la red eléctrica. Obteniendo ahorros e incentivos por utilización de energías renovables.

Techado, Andador, Paneles, Solares

Abstract

In humans, prolonged exposure to solar UV radiation may result in acute and chronic health effects on the skin, eyes and immune system. The levels of UV radiation recorded during the last 5 years on the university campus of the polytechnic university of Tulancingo have an average of 12 IUV with peaks of up to 15 IUV at 14 hours. This work proposes walkway roofing with solar panels that will produce 20,000 kWh. To supply 50% of the electricity consumed by the university, these panels are placed on a metallic structure along the walkways that connect the campus buildings. Social benefit: the roofing will decrease extreme solar radiation exposure of those traversing the university campus. Ecological benefit: when generating electricity using photovoltaic technology, co2 emissions decline. For the life of this project, CO2 emissions will be reduced by as much as 2,700 tons. Economic benefit: as part of the electrical grid, the photovoltaic system will generate savings and provide incentives for use of renewable energy.

Roofing, Walkway, Panels, Solar

Citacion: FLORES-GARCIA, Francisco Armando, COYOTL-MIXCOATL, Felipe, ELIZALDE-CANALES, Francisca Angélica, CASTILLO-MIMILA, Diego Fernando. Techado de Andador con Paneles Solares en la Universidad Politécnica De Tulancingo.Revista de Ciencias Naturales y Agropecuarias. 2017, 4-12: 1-4.

* Correspondencia del Autor (Correo Electrónico: francisco.flores@upt.edu.mx)
†Investigador contribuyendo como primer autor.

Programa base que genera las secuencias binarias con 32 bits

```
clear all;

clc;
SECUENCIA = 31250; %Tamaño de la
secuencia 125,000
X0  = 0.0001;
Miu = 0.7196;
[seqr] =
SBM2(X0,Miu,SECUENCIA,100,1,0.1,0.9);
[seqd] = (RtoD(seqr,0,1,32));
Binario = dec2bin(seqd,32); %Se
transforman en 0's y 1's
BinarioConcatenado = Binario(1,:);
%Se concatena el primer valor
cont = 2;
while cont < (SECUENCIA+1)
    %Se van concatenando todos los
valores binarios
    BinarioConcatenado =
strcat(BinarioConcatenado,
Binario(cont,:));
    %despliega(cont) =
Binario(cont,:);
    cont = cont + 1;
end

%Se escribe en un archivo
fileID =
fopen('B32_1_9_001_m7196.txt','w');
nbytes =
fprintf(fileID,BinarioConcatenado);
fclose(fileID);
length(BinarioConcatenado) %Tamaño
de la cadena binarizada
```

Realizamos tres funciones con pocos datos(1000) la secuencia para tomar solo 3200 datos en Binario y Calcular la información mutua.

```
Funtion 1
clear all;
clc;
SECUENCIA = 1000; %Tamaño de la
secuencia 125,000
X0  = 0.49997;
Miu = 0.000989;
 [seqr] =
SBM2(X0,Miu,SECUENCIA,100,1,0.1,0.9);
[seqd] = (RtoD(seqr,0,1,32));
Binario = dec2bin(seqd,32); %Se
transforman en 0's y 1's
BinarioConcatenado = Binario(1,:);
%Se concatena el primer valor
cont = 2;
while cont < (SECUENCIA+1)
    %Se van concatenando todos los
valores binarios
    BinarioConcatenado =
strcat(BinarioConcatenado,
Binario(cont,:));
    %despliega(cont) =
Binario(cont,:);
    cont = cont + 1;
    save seqr_1;
end


%Se escribe en un archivo
fileID = fopen('uno.txt','w');
nbytes =
fprintf(fileID,BinarioConcatenado);
fclose(fileID);
length(BinarioConcatenado) %Tamaño
de la cadena binarizada

Funtion 2
clear all;
clc;
SECUENCIA = 1000; %Tamaño de la
secuencia 125,000
X0  = 0.49997;
Miu = 0.0989;
 [seqr] =
SBM2(X0,Miu,SECUENCIA,100,1,0.1,0.9);
%Secuencia en Skew Bernoulli Map en
reales
 [seqd] = (RtoD(seqr,0,1,32));
Binario = dec2bin(seqd,32); %Se
transforman los 8 bits en 0's y 1's
BinarioConcatenado = Binario(1,:);
%Se concatena el primer valor
cont = 2;
while cont < (SECUENCIA+1)
    %Se van concatenando todos los
valores binarios
  BinarioConcatenado =
strcat(BinarioConcatenado,
Binario(cont,:));
    %despliega(cont) =
Binario(cont,:);
   cont = cont + 1;

end


%Se escribe en un archivo
fileID = fopen('dos.txt','w');
nbytes =
fprintf(fileID,BinarioConcatenado);
fclose(fileID);
length(BinarioConcatenado) %Tamaño
de la cadena binarizada

Function 3
clear all;
clc;
SECUENCIA = 1000; %Tamaño de la
secuencia 125,000 por tamaño 8 = 1
millon
X0  = 0.123;
Miu = 0.798;
 [seqr] =
SBM2(X0,Miu,SECUENCIA,100,1,0.1,0.9);
%Secuencia en Skew Bernoulli Map en
reales
```

```
   %[seqd] = (RtoD(seqr,0,1,8));
%Secuencia decimal de tamaño de 8
bits
   [seqd] = (RtoD(seqr,0,1,32));
   Binario = dec2bin(seqd,32); %Se
transforman los 8 bits en 0's y 1's
   BinarioConcatenado = Binario(1,:);
%Se concatena el primer valor
   cont = 2;
   while cont < (SECUENCIA+1)
       %Se van concatenando todos los
valores binarios
     BinarioConcatenado =
strcat(BinarioConcatenado,
Binario(cont,:));
       %despliega(cont) =
Binario(cont,:);
   cont = cont + 1;
       %save seqr_3;
   end

   %entropy(seqr_3)
   %Se escribe en un archivo
   fileID = fopen('tres.txt','w');
   nbytes =
fprintf(fileID,BinarioConcatenado);
   fclose(fileID);
   length(BinarioConcatenado) %Tamaño
de la cadena binarizada


   Luego cifre usando los archivos
creados en skewbernoulli con
Prueba3200.m
   load S;
   fid=fopen('uno.txt','r');
   AM1=fread(fid);
   %AM1=fopen('c:\Users\angelica\Docum
ents\Doctorado7\MiArchivo.txt')
   fid=fopen('dos.txt','r');
   AM2=fread(fid);
   fid=fopen('tres.txt','r');
   AM3=fread(fid);
   fid=fopen('pruebabin.txt','w');

   for c=1:3200

     R11(c)=bitxor(AM1(c),AM2(c));
     T(c)=mat2str(R11(c));
     R111(c)=double(T(c));
   r123a(c)=bitxor(R111(c),AM3(c));


    X1(c)=(bitxor(S(c),r123a(c)));

   end
   save X1;

   #include "EmonLib.h"
   EnergyMonitor emon1;
   Int long i=0;

   void setup()
   {
   Serial.begin(115200);
   emon1.voltage(2, 110, 1.7);
   }
   void loop()
   {

   float supplyVoltage   =
emon1.Vrms;
   while(i<100) {
   float sensorCorriente =
analogRead (A0);
   double Irms = sensorCorriente *
(0.0524);
   emon1.calcVI(20,50);
   float supplyVoltage   =
emon1.Vrms ;
   float watts = supplyVoltage *
Irms;
   int long WattPor50Mili = watts
+ WattPor50Mili;
   int long Ws=  WattPor50Mili /
20;
   Serial.print("Energia (W/s):
");
   Serial.println(Ws);

   i=i+1;
   }
   }
```