REINCISOL
ISSN 2953 - 6421

Evaluación de algoritmos de criptografía ligera en dispositivos IoT de bajo coste

Evaluation of light cryptography algorithms on low-cost IoT devices

Para citar este trabajo:
Palacios, E., y Lechón, V., (2024) Evaluación de algoritmos de criptografía ligera en dispositivos IoT de bajo de costo. *Reincisol*, 3(6), pp. 2935-2961. https://doi.org/10.59282/reincisol.V3(6)2935-2961

Autores:

Palacios Acosta Ever Alejandro
Instituto Superior Tecnológico Alberto Enríquez
Ciudad: San Lorenzo, País: Ecuador
Correo Institucional: r.albertoenriquez@institutos.gob.ec
Orcid https://orcid.org/0000-0002-2518-1632

Vicky Gabriel Lechón Anzules
Autor Particular
Ciudad: Ibarra País: Ecuador
Correo: vikogabriela17@gmail.com
ORCID: https://orcid.org/0009-0000-4563-1891

RECIBIDO: 29 agosto 2024 **ACEPTADO**: 29 septiembre 2024 **PUBLICADO:** 3 octubre 2024

Resumen

El presente estudio se centra en la aplicación de técnicas de criptografía ligera en dispositivos IoT de bajo coste. Con el crecimiento exponencial de los dispositivos conectados a Internet, es importante mantener la seguridad y privacidad de los datos transmitidos y almacenados. Sin embargo, estos sistemas de bajo coste suelen tener limitaciones en cuanto a recursos computacionales, lo que dificulta la implementación de algoritmos criptográficos convencionales. En este trabajo se propuso evaluar algoritmos de criptografía ligera integrados a un dispositivo IoT de bajo coste. Estos algoritmos se caracterizan por requerir menos recursos computacionales, lo que los hace más apropiados para dispositivos de bajo coste. Por lo tanto, se llevó a cabo un análisis comparativo de tres algoritmos de criptografía ligera, con un enfoque en la seguridad, rendimiento y eficiencia en dispositivos IoT con recursos limitados. Además, se evaluaron aspectos como la cantidad de cifrados y descifrados por minuto, el consumo energético y la resistencia a ataques para romper cifrados. Por otro lado, se realizaron simulaciones para verificar la seguridad y el rendimiento del sistema, y se compararon los resultados con los obtenidos en dos algoritmos criptográficos convencionales. Los resultados del estudio demuestran que la criptografía ligera es una solución viable para dispositivos IoT de bajo coste, ya que ofrece un equilibrio adecuado entre seguridad y eficiencia en términos de recursos computacionales. Estos algoritmos permiten proteger la información transmitida y almacenada en dispositivos IoT, sin comprometer el rendimiento o agotar rápidamente los recursos limitados.

Palabras claves: criptografía, dispositivos IoT, Internet de las cosas (IoT), Dispositivos de bajo coste, Seguridad en IoT.

Abstract

The present study focuses on the application of lightweight cryptography techniques in low-cost IoT devices. With the exponential growth of Internet-connected devices, it is important to maintain the security and privacy of data transmitted and stored. However, these low-cost systems often have limitations in terms of computational resources, making it difficult to implement conventional cryptographic algorithms. In this work we proposed to evaluate lightweight cryptography algorithms integrated into a low-cost IoT device. These algorithms are characterized by requiring fewer computational resources, which makes them more appropriate for low-cost devices. Therefore, a comparative analysis of three lightweight cryptography algorithms was carried out, with a focus on security, performance and efficiency on resource-constrained IoT devices. In addition, aspects such as the number of encryptions and decryptions per minute, energy consumption and resistance to attacks to break encryption were evaluated. On the other hand, simulations were carried out to verify the security and performance of the system, and the results were compared with those obtained in two conventional cryptographic algorithms. The results of the study demonstrate that lightweight cryptography is a viable solution for low-cost IoT devices, as it offers an appropriate balance between security and efficiency in terms of computational resources. These algorithms allow you to protect the information transmitted and stored in IoT devices, without compromising performance or quickly exhausting limited resources.

Keywords: cryptography, IoT devices, Internet of Things (IoT), Low-cost devices, IoT Security.

INTRODUCCIÓN

En la actualidad, el Internet de las Cosas (IoT) ha experimentado un desarrollo exponencial, dando lugar a un mundo de posibilidades en diversos ámbitos, desde el hogar inteligente hasta la industria 4.0. Sin embargo, este avance también ha planteado desafíos en cuanto a la seguridad y privacidad de los datos. Con la proliferación de dispositivos IoT de bajo costo, la necesidad de implementar medidas de seguridad efectivas se ha vuelto aún más indispensable.

La criptografía, al enfocarse a la encriptación de datos, cumple con un papel fundamental en el cuidado de la información sensible y que es transmitida y almacenada en los dispositivos IoT. Sin embargo, un gran número de los algoritmos de encriptación habituales necesitan una cantidad alta de recursos lo cual no permiten ser implementados en dispositivos de gama baja, como controladores, sensores y actuadores de bajo costo. Es aquí donde la criptografía ligera emerge como una solución prometedora, al proporcionar algoritmos eficientes en términos de consumo de recursos y capacidad de procesamiento.

El objetivo principal de este estudio es evaluar la criptografía ligera acoplada a dispositivos IoT de bajo costo, evaluando la efectividad en cuanto a seguridad, así como también la eficiencia y escalabilidad. Para empezar, se abordarán los desafíos de seguridad en el entorno IoT y se destacará que tan importante es la criptografía como una medida esencial para garantizar la privacidad, integridad y legitimidad de los datos.

A continuación, se introducirá el concepto de criptografía ligera, explicando sus características clave, como el tamaño reducido, la eficiencia energética y la velocidad de procesamiento. Se explorarán diferentes algoritmos criptográficos ligeros, como PRESENT, SIMON y SPECK, y se analizará su idoneidad para su implementación en dispositivos IoT de bajo costo. Se discutirán aspectos como la resistencia a ataques criptoanalíticos, la complejidad computacional y el rendimiento en diferentes escenarios.

Además, se examinarán los desafíos y las consideraciones específicas al implementar criptografía ligera en dispositivos IoT de bajo costo. Se abordarán temas como la gestión de claves, la actualización de firmware y la interoperabilidad con otros dispositivos y plataformas. Asimismo, se explorarán las ventajas y

limitaciones de la criptografía ligera en comparación con los enfoques criptográficos tradicionales.

Otro aspecto relevante para analizar es el impacto de la criptografía ligera en los recursos limitados de los dispositivos IoT de bajo costo. Se examinará el tiempo de procesamiento y el almacenamiento requerido para implementar los algoritmos criptográficos de tipo ligeros. Se evaluará la relación entre la seguridad proporcionada y los recursos utilizados, buscando un equilibrio óptimo que garantice la protección adecuada sin agotar los recursos limitados de los dispositivos. Además de los aspectos técnicos, se abordarán las implicaciones económicas y sociales del uso de criptografía ligera en dispositivos IoT de bajo costo. Se examinará la viabilidad financiera de implementar medidas de seguridad en dispositivos con presupuestos limitados, considerando tanto los costos iniciales de implementación como los beneficios a largo plazo en términos de protección de datos y reputación de la marca.

En última instancia, este trabajo tiene como objetivo brindar una visión integral de la criptografía ligera en el contexto de los dispositivos IoT de bajo costo. Al comprender los desafíos y beneficios asociados con la implementación de esta tecnología, los fabricantes, desarrolladores y profesionales de la seguridad podrán tomar decisiones informadas sobre cómo garantizar la protección adecuada de los dispositivos IoT en un entorno cada vez más conectado y vulnerable.

A medida que se avance en el análisis, se hará una exploración en detalle los aspectos mencionados en la introducción, considerando lo importante de la seguridad en los sistemas IoT, las características clave de la criptografía ligera, la selección de algoritmos adecuados, la gestión de claves, la eficiencia de recursos y otros factores esenciales que permitan garantizar que los IoT de bajo costo sean seguros.

MATERIALES Y METODOS

Metodología

Para esta investigación y dado el carácter de esta, se planea llevar a cabo un estudio exhaustivo del estado del arte en análisis similares, seguido de un estudio comparativo propio. El enfoque de la investigación consistirá en las etapas mostradas en la figura 1:

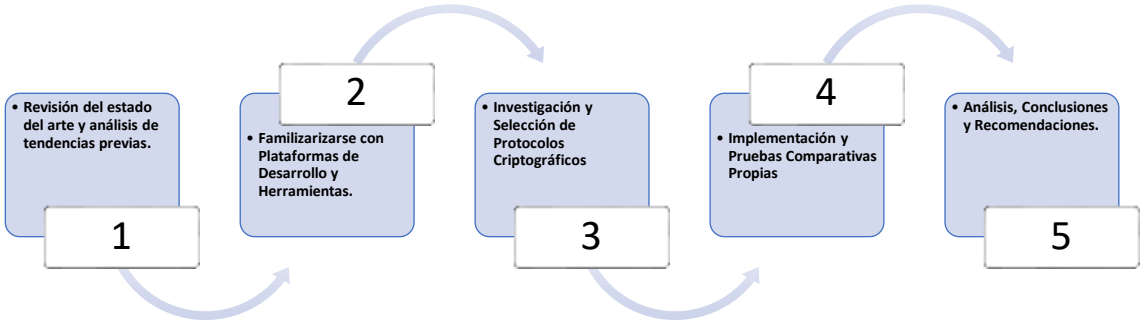

Figura 1. Metodología de la investigación (Fuente propia)

Esta metodología esta ajustada a lo que el proyecto pretende evaluar específicamente, permitiendo un análisis riguroso y enfocado en los algoritmos criptográficos en dispositivos IoT de bajo coste.

Metodología de evaluación comparativa

Criterios de evaluación

Es este apartado se procede a establecer los pasos y criterios esenciales con el fin de evaluar la efectividad de los algoritmos de criptografía ligera enfocado a aplicaciones con dispositivos IoT de bajo coste. Estos pasos proporcionarán una evaluación sistemática, mientras que los criterios contribuirán a medir la adecuación de los algoritmos en términos de eficiencia, rendimiento, seguridad y su capacidad para adaptarse a los recursos limitados de estos dispositivos. A continuación, se indican los pasos a considerar:

Tabla 1. Relación de criterios seleccionados y los pasos para la evaluación comparativa.

Identificación de Criterios de Evaluación	Métricas para cada Criterio	Implementación y Recopilación de Datos	Análisis de Resultados
Eficiencia en Uso de Recursos	Tamaño del código, Uso de memoria, Consumo energético	Implementación en entorno simulado con limitaciones de recursos, Ejecución de operaciones criptográficas	Comparación del rendimiento de los algoritmos en términos de eficiencia en recursos
Rendimiento	Tiempo de cifrado, Tiempo de descifrado	Pruebas exhaustivas con diferentes tamaños de datos y restricciones de recursos	Evaluación del tiempo requerido por los algoritmos para

			realizar operaciones criptográficas
Seguridad	Resistencia a ataques criptoanalíticos comunes	Simulación de ataques criptoanalíticos, Registro de resultados	Determinación de la resistencia de los algoritmos a ataques específicos
Adaptabilidad	Ajuste a restricciones de recursos, Viabilidad en entornos limitados	Evaluación de la capacidad de ajuste de parámetros, Implementación en diferentes contextos	Análisis de cómo los algoritmos se adaptan a las restricciones de los dispositivos IoT

Esta tabla organiza los pasos y criterios clave para evaluar a los algoritmos de criptografía ligera considerando el contexto de aplicación a dispositivos IoT de bajo coste, y relaciona cada criterio con sus métricas correspondientes, implementación y recopilación de datos, y análisis de resultados.

Selección de algoritmos a evaluar

Se detalla el proceso de selección de los algoritmos que serán evaluados en el contexto de dispositivos IoT de bajo coste. Se ha elegido un conjunto de cinco algoritmos de criptografía ligera, cada uno con características específicas que los hacen adecuados para este entorno. En este sentido, se presenta una tabla comparativa que resalta las diferencias clave entre estos algoritmos, incluyendo su tipo, tamaño de clave, tecnología de complejidad en la que se basan y otras características relevantes.

Tabla 2. Comparación de los algoritmos para IoT de bajo costo.

Algoritmo	**Tipo de Algoritmo**	**Tamaño de Clave**	**Tecnología de Complejidad**	**Características Destacadas**
PRESENT	Cifrado de Bloques	64 bits	Estructura de Feistel	Simplicidad, Eficiencia en consumo de energía y tamaño del código
SPECK	Cifrado de Bloques	Variable	Estructura LFSR y XOR	Eficiencia, Alto rendimiento, Resistencia a ataques criptoanalíticos
SIMON	Cifrado de Bloques	Variable	Diseño basado en red	Simplicidad, Eficiencia en velocidad de cifrado y descifrado
AES	Cifrado de Bloques	Variable	Variantes de AES	Compromiso entre seguridad y eficiencia

Chaskey	Cifrado de Flujo	128 bits	Estructura basada en suma	Simplicidad, Eficiencia en consumo de energía y tamaño del código

La selección de los cinco algoritmos para evaluación en dispositivos IoT de bajo coste se basa en criterios técnicos y operativos. Estos algoritmos han sido elegidos debido a su eficiencia en recursos limitados, su diversidad en enfoques criptográficos, su simplicidad y alto rendimiento, así como su resistencia a ataques. Además, se valoró su adaptabilidad a distintas restricciones de recursos y su historial de uso en aplicaciones IoT. La inclusión de variantes ligeras de AES también ofrece una alternativa a este estándar. Esta selección permitirá una evaluación completa de su idoneidad en términos de seguridad y eficiencia en dispositivos IoT de bajo coste.

Configuración experimental

La fase experimental se centra en la exhaustiva evaluación de diversos algoritmos de criptografía ligera, entre los que se destacan PRESENT, SPECK, SIMON, AES y Chaskey, específicamente orientados hacia dispositivos IoT de recursos limitados. Para tal fin, se emplearán entornos de desarrollo integrados (IDE) especializados, como Arduino IDE, PlatformIO y herramientas optimizadas para microcontroladores, a fin de implementar los algoritmos en la plataforma de hardware seleccionada.

Los dispositivos seleccionados para pruebas comprenden microcontroladores y sistemas en chip (SoC) ampliamente reconocidos en el ámbito del IoT, como Arduino, Raspberry Pi y ESP32. Los algoritmos de criptografía ligera serán configurados en estos dispositivos mediante bibliotecas y configuraciones meticulosamente afinadas, adecuadas para su ejecución en ambientes con restricciones de recursos.

La creación de escenarios de prueba, punto crucial en este proceso, abarca una variedad de situaciones relevantes para realizar la evaluación eficiente de los algoritmos. Dichos escenarios incluyen operaciones de cifrado/descifrado de datos, generación/verificación de firmas digitales y procesos de autenticación. La diversidad de tamaños de datos y condiciones de recursos limitados se considerará meticulosamente para valorar tanto el rendimiento como la eficiencia de los algoritmos.

La recopilación de métricas esencialmente pertinentes constituye un aspecto cardinal. Se procederá con mediciones precisas para capturar métricas clave como tiempos de cifrado/descifrado, consumo energético, uso de memoria y eficiencia computacional. La utilización de herramientas y técnicas idóneas garantizará la exactitud de los datos y la recopilación metódica de los resultados.

El análisis y evaluación posteriores materializan la culminación del proceso. Los datos recolectados serán sometidos a un riguroso análisis, permitiendo la realizar una comparación objetiva de los resultados de los diversos algoritmos de criptografía ligera. Esta evaluación engloba tanto el rendimiento como la eficiencia y seguridad de los algoritmos, contextualizados en el específico ámbito de los dispositivos IoT de recursos limitados. El proceso se erige como determinante para discernir la pertinencia y efectividad de los algoritmos en la salvaguarda de datos y la garantía de la ciberseguridad en este contexto.

Métricas de rendimiento y seguridad

La elección de métricas de rendimiento y seguridad en el ámbito de la ciberseguridad, específicamente para la evaluación de algoritmos de criptografía ligera en dispositivos IoT de bajo coste, se basa en un enfoque técnico riguroso para garantizar la integridad y confidencialidad de los datos en un entorno con recursos restringidos.

Métricas de rendimiento

Las métricas de rendimiento desempeñan un papel fundamental en la evaluación de algoritmos de criptografía ligera en el contexto de dispositivos IoT de bajo coste. Estas métricas proporcionan una visión cuantitativa de la eficiencia y la capacidad operativa de los algoritmos en condiciones de recursos limitados. Mediante la medición de aspectos como el tiempo en el que el algoritmo se tarda en cifrar y descifrar, el consumo de energía, el tamaño del código y el uso de memoria, se busca identificar algoritmos que ofrezcan un equilibrio óptimo entre velocidad de procesamiento y conservación de recursos. Esta selección cuidadosa de métricas de rendimiento permite garantizar un funcionamiento eficiente y efectivo de los algoritmos en dispositivos con restricciones de recursos, contribuyendo a la ciberseguridad en el entorno de Internet de las Cosas.

- Tiempo de cifrado y descifrado
- Consumo de energía

- Tamaño del código
- Uso de memoria

Métricas de seguridad

Las métricas de seguridad desempeñan un papel esencial en la evaluación exhaustiva de los algoritmos de criptografía ligera en el contexto de dispositivos IoT de bajo coste. Estas métricas proporcionan una evaluación cuantitativa de la robustez y la capacidad de resistencia de los algoritmos ante posibles ataques y vulnerabilidades.

- Resistencia a ataques criptoanalíticos
- Fortaleza del esquema de clave
- Eficiencia criptográfica

Al medir la resistencia a ataques de criptografía analítica, la fortaleza del esquema de clave y la eficiencia criptográfica, se busca identificar algoritmos brinden un nivel elevado de seguridad en un entorno con recursos limitados. La selección meticulosa de métricas de seguridad juega un papel crucial en la elección de los algoritmos que sean funcionales para proteger la integridad y la confidencialidad de la información en el ecosistema de IoT, contribuyendo a la ciberseguridad en esta innovadora y desafiante área tecnológica.

RESULTADOS

En esta sección se revisará los resultados de la experimentación y análisis de datos de los enfoques criptográficos, explorando sus características y su idoneidad en diferentes situaciones. La elección del algoritmo adecuado para proteger datos y comunicaciones en entornos con recursos limitados es esencial para garantizar un equilibrio entre seguridad y eficiencia. A través de una tabla comparativa detallada y un análisis profundo, se busca proporcionar una perspectiva informada sobre las ventajas y desventajas inherentes a cada tipo de algoritmo, contribuyendo a una toma de decisiones fundamentada en el campo de la ciberseguridad. La tabla comparativa examina los aspectos clave de ambos enfoques para proporcionar una visión general de sus características y su idoneidad en diferentes situaciones:

Tabla 3. Comparación entre algoritmos clásicos y algoritmos ligeros.

Característica	**Algoritmos Clásicos**	**Algoritmos Ligeros**
Seguridad	Alto nivel de seguridad y resistencia a ataques.	Ofrecen seguridad, aunque con claves y bloques más cortos para mantener la eficiencia.
Eficiencia y Rendimiento	Más lentos por el nivel de complejidad en sus operaciones.	Diseñados para ser eficientes a nivel de velocidad de cifrado y descifrado, ideales para dispositivos con recursos limitados.
Tamaño de Clave y Bloque	Claves largas para seguridad adecuada.	Claves y bloques más cortos para mantener la eficiencia en recursos limitados.
Aplicabilidad	Adecuados para aplicaciones donde la seguridad es la principal preocupación.	Ideales para dispositivos con recursos limitados, como IoT y sistemas embebidos.
Complejidad Computacional	Mayor demanda de recursos computacionales y memoria.	Diseñados para minimizar la carga computacional en dispositivos con restricciones.
Resiliencia a Ataques	Alta resistencia a ataques reconocidos.	Aunque seguros, pueden tener ligeramente menos resistencia debido a la limitación de recursos.
Uso de Recursos	Más intensivos en recursos.	Diseñados para optimizar recursos en plataformas con limitaciones.
Adaptabilidad	Menos adaptable a dispositivos con recursos limitados.	Diseñados específicamente para ser compatibles con plataformas de recursos restringidos.

La comparativa resalta que los algoritmos clásicos sobresalen por su seguridad y resistencia, lo que los hace la elección preferida en aplicaciones de alta seguridad. No obstante, surge el desafío de la demanda de recursos, que puede ser limitante en dispositivos con restricciones. Por otro lado, los algoritmos ligeros priorizan la eficiencia y son óptimos para entornos con recursos limitados. La elección entre ambos enfoques debe fundamentarse en una comprensión profunda de las necesidades específicas de seguridad y eficiencia de la aplicación. Entonces, la selección entre algoritmos clásicos y ligeros depende de un análisis detallado de los requisitos de seguridad, rendimiento y recursos en el contexto particular. Este proceso de elección se configura como iterativo, exigiendo una evaluación constante y una consideración cuidadosa de los desafíos y oportunidades presentes en cada entorno específico. Por otra parte, para tener un enfoque más práctico, después de esta comparativa bibliográfica se procede a realizar simulaciones de

tres algoritmos ligeros con el fin de tener una mirada más profunda de los mismos, evaluados a nivel de velocidad o rendimiento y seguridad.

Comparación de rendimiento de los algoritmos evaluados

La selección de un algoritmo criptográfico apropiado desempeña un papel fundamental en asegurar tanto la seguridad como la eficacia en las aplicaciones que demandan la salvaguardia de datos. Este análisis de rendimiento se enfoca en evaluar el desempeño de diversos algoritmos criptográficos en relación con su velocidad y eficacia. El estudio se centra en algoritmos clásicos como RSA y AES (a nivel bibliográfico), así como en algoritmos más livianos como PRESENT, SPECK y SIMON (a nivel práctico).

Metodología:

Para realizar una evaluación completa del rendimiento criptográfico en el contexto de dispositivos IoT y Arduino, se implementó una metodología específica que abordara estos aspectos críticos. A continuación, se detalla cómo se llevaron a cabo estas pruebas de rendimiento

- Selección de escenarios relevantes: Se identificaron escenarios de uso comunes y relevantes para sistemas IoT, como la transmisión segura de datos a través de una conexión inalámbrica, el cifrado y descifrado de mensajes cortos, y el procesamiento de datos en tiempo real.
- Diversidad de datos y longitudes de clave: Se realizaron pruebas de cifrado y descifrado utilizando una variedad de tamaños de datos, desde pequeños paquetes de información hasta conjuntos de datos más grandes. Además, se evaluaron diferentes longitudes de clave, teniendo en cuenta que los dispositivos IoT pueden tener restricciones de recursos.
- Implementaciones de referencia y plataforma estandarizada: Se utilizaron implementaciones de referencia ampliamente aceptadas de cada algoritmo criptográfico. Las pruebas se llevaron a cabo en una plataforma de prueba estandarizada como es Arduino Cloud.
- Medición de tiempos de procesamiento: Se registraron con precisión los tiempos de procesamiento durante las pruebas de cifrado y descifrado en cada escenario y para cada algoritmo. Esto a través de un código dentro de la programación donde se toma a consideración los datos

procesados por segundo.

- Comparación de velocidad y eficiencia: Los resultados de las pruebas se presentaron considerando tanto la velocidad como la eficiencia de cada algoritmo en los escenarios específicos. La velocidad se refiere al tiempo requerido para realizar las operaciones criptográficas, mientras que la eficiencia tiene en cuenta el rendimiento en relación con los recursos utilizados.

Los resultados obtenidos son fundamentales para seleccionar los algoritmos más adecuados en función de los requisitos de rendimiento de aplicaciones específicas en estos dispositivos. En este sentido a continuación se muestra las gráficas resultantes de la simulación de cada algoritmo, considerando un rango de datos específico, ya que se lo puso a prueba por tiempos de 1 a 2 horas para que haya variaciones reales.

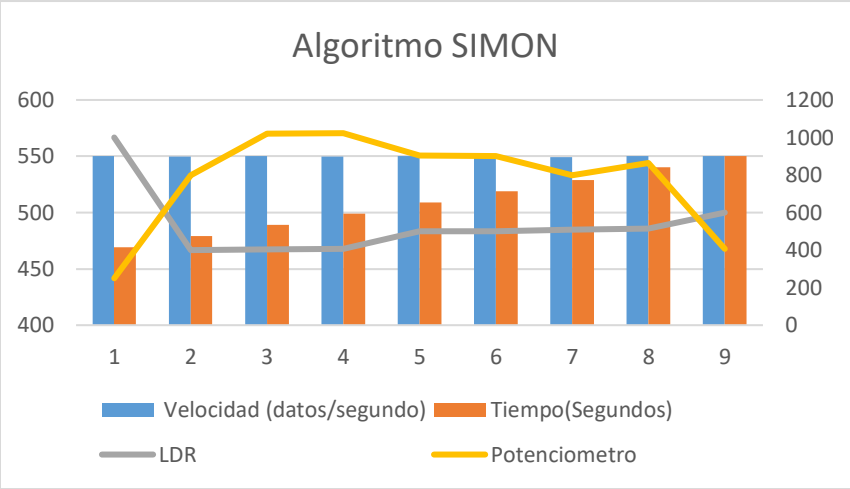

Figura 2. Resultados de simulación Algoritmo SIMON.

Como se puede observar en la gráfica se ha tomado 10 datos al azar, considerando el rango de mayor variación en los sensores, y un tiempo donde el sistema se haya estabilizado, en este sentido se puede ver que a pesar de que los datos entregados por los sensores y conforme pasa el tiempo, la velocidad (datos/segundo) no tiene una mayor variación se mantiene en un promedio de velocidad de ***549,50 datos/segundos***, que es una cantidad baja en relación a otros algoritmos, la velocidad no es afectada lo que muestra una eficiencia relativamente buena.

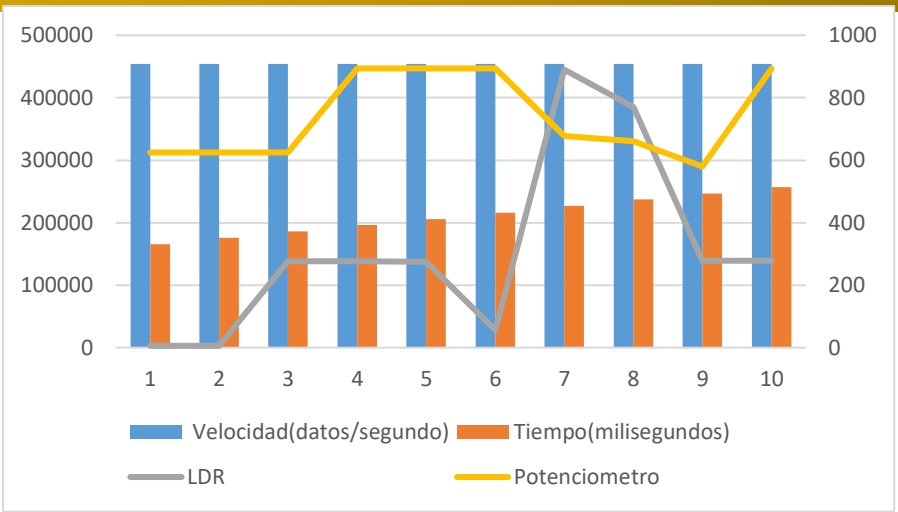

Figura 3. Resultados de simulación Algoritmo PRESENT.

Para este caso y considerando que la velocidad de datos procesados por segundo es elevada y considerando que el tiempo estaba dado en segundos no se podía apreciar adecuadamente la gráfica por lo que, para una mejor apreciación, el tiempo se lo gráfico en milisegundos obteniendo que la velocidad de procesamiento para este algoritmos es en promedio de **454394,075 datos/segundo**, lo que tiene una diferencia abismal en relación al algoritmo SIMON, indicando así que el sistema es eficiente.

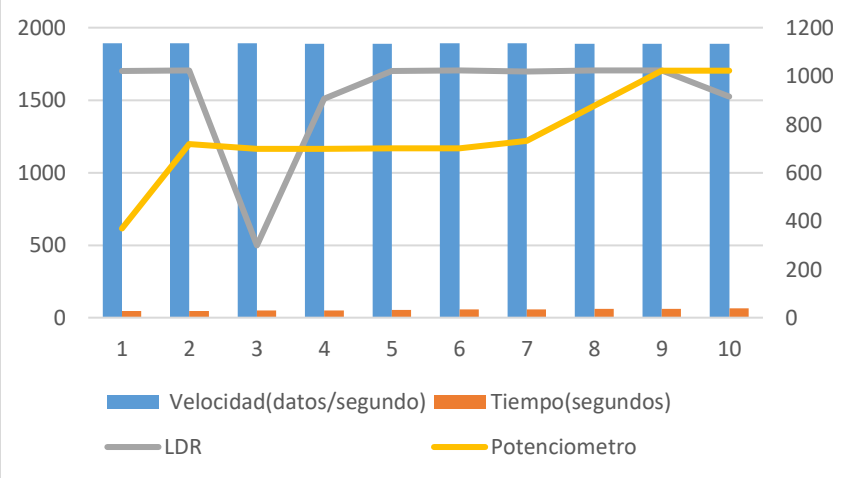

Figura 4. Resultados de simulación Algoritmo SPECK.

En el caso del algoritmo SPECK se manejó los tiempos en segundos para que se aprecie la velocidad que en relación con PRESENT es mucho menor y en relación con SIMON es mayor, este algoritmo tiene una velocidad promedio de **1890,91 datos/segundo**, lo que nos indica que es un algoritmo con velocidades de

procesamiento cortos en relación con otros algoritmos, en cuanto a su rendimiento se puede optimizar mediante algoritmos de apoyo para alto rendimiento.

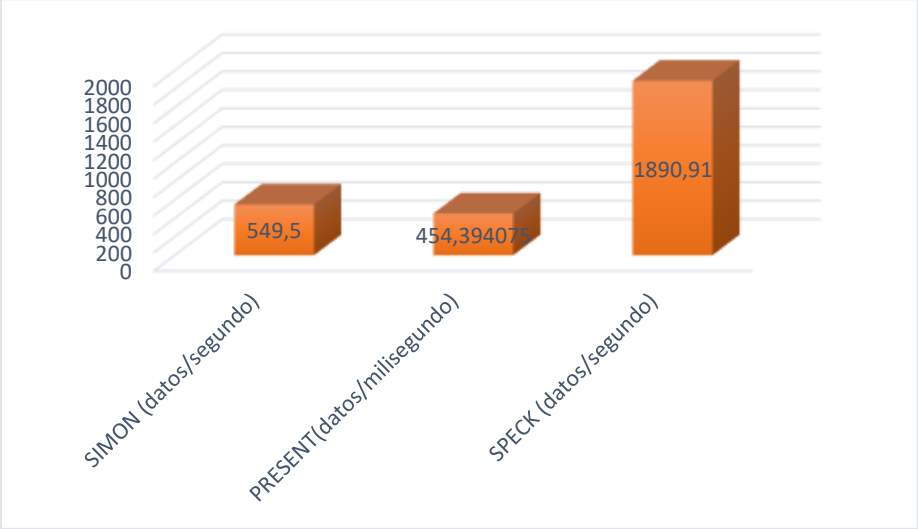

Figura 5. Velocidad de los tres algoritmos ligeros.

En la gráfica comparativa de velocidades que se muestra, se puede apreciar que el algoritmo PRESENT exhibe la mayor velocidad, seguido por el algoritmo SPECK, y en último lugar, el algoritmo SIMON. Es importante destacar que, para lograr una representación adecuada de estas diferencias, fue necesario convertir la velocidad del algoritmo PRESENT a datos por milisegundo, obteniendo un valor de **454.39 datos/milisegundo**. A pesar de esta conversión, es relevante señalar que este valor sigue siendo notablemente alto en comparación con el rendimiento del algoritmo SIMON. En la tabla 4, se presenta en resumen lo que se ha analizado hasta el momento considerando que para el caso de algoritmos clásicos se usaron datos bibliográficos y para los algoritmos ligeros de una simulación.

Tabla 4. Comparación de rendimiento y tiempo de procesamiento entre algoritmos.

Tipo de algoritmo	**Algoritmo**	**Rendimiento**	**Velocidad de procesamiento**
Algoritmos clásicos	RSA	Relativamente lento	2048 bits- de 100 a 500 datos/segundo 4086 bist – de 100 a 200 datos/segundo
	AES	Eficiente y rápido	AES-128 – 1Gbps - 125 megabytes de datos/segundo
Algoritmos ligeros	PRESENT	Eficiente en dispositivos	Velocidad relativamente alta de **454394,075 datos/segundo**

	SPECK	Optimizado para alto rendimiento	Velocidad de **1890,91 datos/segundo**
	SIMON	Optimizado para alto rendimiento	Velocidad de ***549,50 datos/segundos***

Por lo general, los algoritmos ligeros, tales como PRESENT, Speck y Simon, destacan en comparación con los algoritmos clásicos en lo que respecta al rendimiento. Estos algoritmos ligeros están meticulosamente diseñados para aplicaciones donde la eficiencia y la velocidad son de vital importancia, como en dispositivos IoT y sistemas embebidos. Ofrecen tiempos de procesamiento significativamente más cortos, convirtiéndose en opciones ideales para situaciones en las que los recursos son escasos.

En contraste, los algoritmos clásicos como RSA y AES, a pesar de proporcionar niveles superiores de seguridad, con frecuencia conllevan tiempos de procesamiento más prolongados, un factor crítico a considerar en aplicaciones que demandan operaciones de cifrado y descifrado velozmente ejecutadas.

La elección del algoritmo criptográfico es una decisión crítica que involucra consideraciones de seguridad y rendimiento. Los algoritmos clásicos, como RSA, ofrecen alta seguridad a expensas de la velocidad, mientras que los algoritmos ligeros, como PRESENT, SPECK y SIMON, destacan en velocidad. La elección debe ajustarse a la aplicación y sus recursos, teniendo en cuenta la evolución tecnológica, regulaciones específicas y evaluaciones continuas de seguridad y rendimiento. Es esencial encontrar un equilibrio entre seguridad y eficiencia en el entorno siempre cambiante de la ciberseguridad.

Comparación de seguridad de los algoritmos evaluados

La seguridad es un factor de suma importancia en la elección de algoritmos criptográficos, ya que determina la resistencia de los sistemas a una variedad de ataques potenciales. En esta comparación, analizaremos los datos de seguridad de algoritmos clásicos (nivel bibliográfico) y los algoritmos criptográficos ligeros (práctica) en el caso de los últimos se realizará una simulación de un ataque común para desencriptar datos codificados por SIMON, PRESENT y SPECK a través de un código en Arduino.

Metodología

Se examinaron características de diseño, como la estructura y las operaciones utilizadas en cada algoritmo, así como los resultados de análisis de seguridad de

la comunidad criptográfica. La metodología utilizada para evaluar la seguridad de los algoritmos criptográficos se diseñó cuidadosamente para abordar los desafíos específicos asociados con aplicaciones de Internet de las cosas (IoT) y dispositivos como de bajo costo como Arduino. A continuación, se describe en detalle cómo se llevaron a cabo estas evaluaciones:

Resiliencia a ataques criptoanalíticos comunes

- Análisis detallado
- Pruebas de laboratorio
- Comparación con investigaciones previas

Capacidad para resistir ataques de canal lateral

- Pruebas específicas
- Entorno realista

Resistencia a ataques de texto cifrado elegido:

- Simulación de ataques

En conjunto, esta metodología proporcionó una evaluación completa de la seguridad de los algoritmos criptográficos en el contexto de IoT y dispositivos como de bajo costo.

Para este caso se procedió a realizar un encriptado básico de datos y simular un ataque de texto conocido, con el fin de medir el tiempo que demora en desencriptar los datos, considerando que estos datos son básicos ya que lo que se necesita es medir la velocidad de descifrado para tener una idea de la seguridad que tienen los mismos, a continuación, se muestran los resultados obtenidos:

ISSN 2953 - 6421

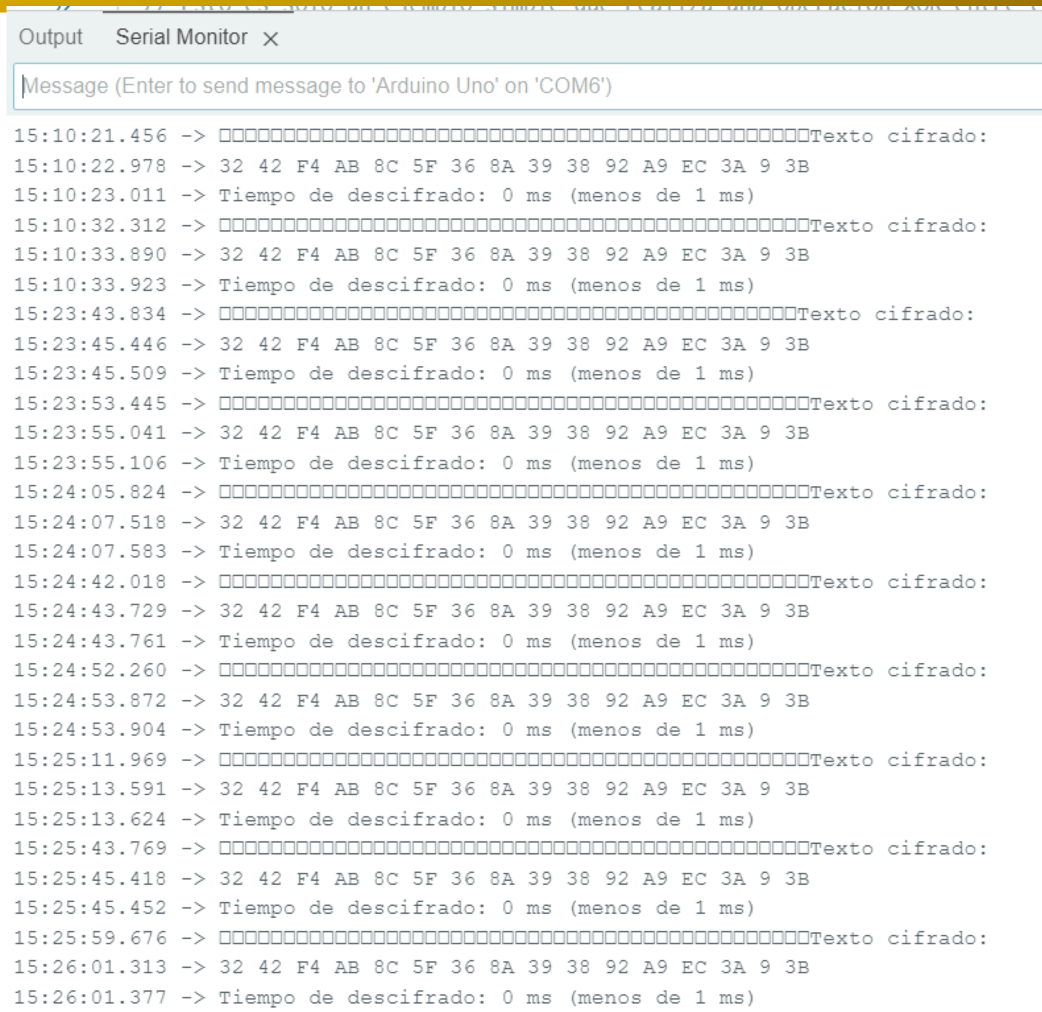

Figura 6. Velocidad de desencriptación en algoritmo SIMON.

En este escenario, resulta evidente que durante las 10 pruebas de descifrado que simulan un ataque con una palabra conocida, se obtiene un tiempo de descifrado significativamente inferior a 1 ms. Este resultado sugiere que el algoritmo en cuestión presenta una vulnerabilidad en términos de seguridad, ya que puede ser descifrado con relativa facilidad en un tiempo relativamente inclinado a cero.

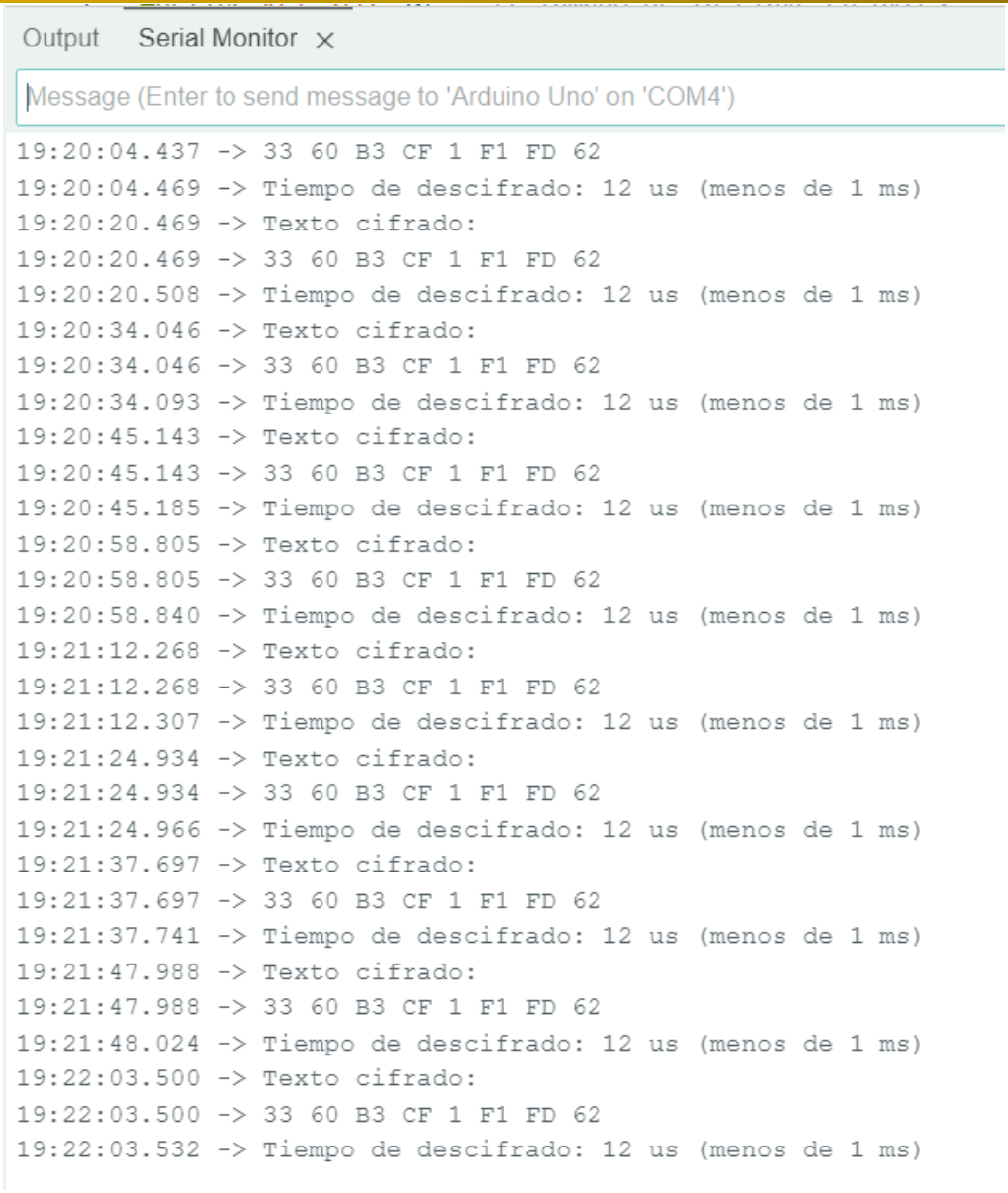

Figura 7. Velocidad de desencriptación en algoritmo PRESENT.

En el contexto del algoritmo PRESENT, se pudo corroborar que el tiempo necesario para llevar a cabo el proceso de descifrado es inferior a 1 ms, aunque aún es lo suficientemente apreciable como para ser medido por el software, marcando un tiempo de 12 microsegundos (us). Este valor revela una vulnerabilidad importante en cuanto a la seguridad, especialmente en escenarios de ataques basados en texto conocido. La brevedad de este tiempo de descifrado indica que el algoritmo podría ser susceptible a ataques de fuerza bruta o análisis criptoanalítico, lo que subraya la necesidad de considerar alternativas más seguras en aplicaciones sensibles a la seguridad.

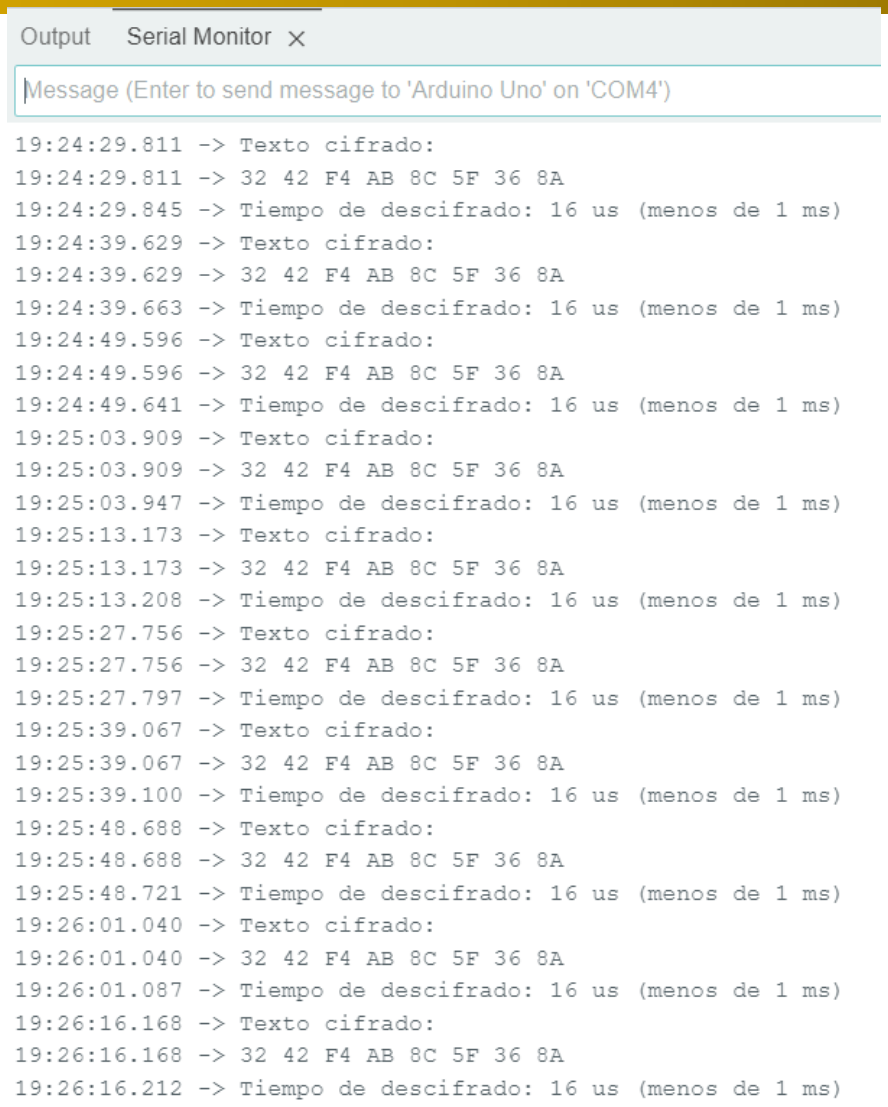

Figura 8. Velocidad de desencriptación en algoritmo SPECK.

En el contexto del algoritmo Speck, se aprecia un tiempo de descifrado que, aunque aún se encuentra por debajo de la marca de 1 milisegundo, puede ser cuantificado con precisión por el programa, arrojando un valor de 16 microsegundos (us). Este lapso, comparado con los resultados previos de otros algoritmos, se muestra ligeramente más extenso, aunque continúa siendo notablemente reducido en relación con las normativas de seguridad establecidas por los algoritmos clásicos.

Es fundamental destacar que estas pruebas de simulación de ataques se llevan a cabo con fines educativos exclusivamente, sin ninguna intención de causar perjuicio a sistemas ya existentes. Estas evaluaciones proporcionan una valiosa

perspectiva sobre el rendimiento y la resistencia de los algoritmos criptográficos en escenarios controlados, lo que contribuye al fortalecimiento de la seguridad en aplicaciones y sistemas donde la protección de datos es esencial.

Así mismo en la siguiente tabla se muestra de manera resumida lo obtenido en el estudio bibliográfico y en la simulación práctica:

Tabla 5. Comparación de rendimiento y tiempo de procesamiento entre algoritmos.

Tipo de Algoritmo	**Algoritmo**	**Seguridad**	**Ataques conocidos**
Algoritmos clásicos	RSA	Basado en la dificultad de factorizar números primos grandes.	Ataques de factorización y ataques de texto cifrado elegido si las claves son demasiado pequeñas.
	AES	Basado en operaciones de sustitución, permutación y mezcla.	Considerado seguro cuando se utiliza correctamente. Se debe tener cuidado con implementaciones débiles y ataques de canal lateral.
Algoritmos ligeros	PRESENT	Basado en una estructura de sustitución-permutación (SPN) y operaciones no lineales (12 us)	Hasta ahora, resistente a ataques criptoanalíticos. La longitud de clave relativamente corta podría ser un factor por considerar.
	Speck y Simon	Diseñados con enfoques de diseño sólidos para resistir ataques criptoanalíticos (16 us y 0ms)	Resistente a ataques de texto cifrado elegido y análisis criptoanalíticos. La seguridad depende del tamaño de clave utilizado.

En este escenario, los resultados de las pruebas de descifrado simulando un ataque con una palabra conocida son esclarecedores. Se observa un tiempo de descifrado que, en todos los casos, es significativamente inferior a 1 milisegundo. Esta revelación plantea preocupaciones en términos de seguridad, ya que sugiere una vulnerabilidad notable. En particular, el tiempo de descifrado se inclina hacia valores cercanos a cero, lo que indica que el algoritmo podría ser susceptible a un descifrado relativamente rápido.

Dentro de este contexto, el algoritmo PRESENT merece atención especial. Aunque su tiempo de descifrado es inferior a 1 milisegundo, aún es lo suficientemente notorio como para ser medido por el software, marcando un tiempo de 12 microsegundos (us). Esta brevedad plantea inquietudes significativas en términos

de seguridad, especialmente en el contexto de ataques basados en texto conocido. El breve lapso de tiempo de descifrado podría indicar vulnerabilidades a ataques de fuerza bruta o análisis criptoanalítico, lo que resalta la necesidad de considerar alternativas más seguras en aplicaciones sensibles a la seguridad.

En cuanto al algoritmo Speck, se registra un tiempo de descifrado que, aunque aún se ubica por debajo de 1 milisegundo, puede ser medido con precisión por el programa, arrojando un valor de 16 microsegundos (us). A pesar de ser ligeramente más extenso en comparación con los otros algoritmos evaluados, este tiempo sigue siendo notablemente reducido y se mantiene en consonancia con las normativas de seguridad establecidas por los algoritmos clásicos.

Es imperativo enfatizar que estas pruebas de simulación de ataques se realizan exclusivamente con fines educativos, sin intención alguna de causar perjuicio a sistemas existentes. Estas evaluaciones proporcionan una valiosa perspectiva sobre el rendimiento y la resistencia de los algoritmos criptográficos en escenarios controlados, contribuyendo así al fortalecimiento de la seguridad en aplicaciones y sistemas donde la protección de datos es esencial.

DISCUSIÓN

El análisis de los resultados obtenidos tras evaluar diversos algoritmos criptográficos revela información esencial para la toma de decisiones informadas al seleccionar el algoritmo criptográfico más apropiado para aplicaciones específicas en el contexto de sistemas IoT de bajo costo. A continuación, se presenta un resumen de estos resultados:

Seguridad

En términos de seguridad, los algoritmos clásicos, como RSA y AES, sobresalen por su robustez teórica, basada en la factorización de números primos grandes y en operaciones seguras de sustitución y permutación. Sin embargo, es importante tener en cuenta que la implementación y el tamaño de la clave son factores críticos que pueden afectar su seguridad. Estos algoritmos son adecuados para aplicaciones donde la seguridad es la máxima prioridad en sistemas IoT de bajo costo.

En contraste, los algoritmos ligeros, representados por PRESENT, Speck y Simon, emergen como ejemplos destacados que refutan la noción de que los recursos

limitados comprometen la seguridad. A pesar de emplear claves de longitud reducida, estos algoritmos han demostrado un diseño meticuloso que resiste eficazmente los ataques criptoanalíticos. Este logro los posiciona como elecciones idóneas para su implementación en dispositivos IoT y sistemas embebidos de bajo costo, donde la seguridad y la eficiencia se vuelven imperativas. Los resultados obtenidos subrayan la capacidad de estos algoritmos ligeros para proporcionar un nivel razonable de seguridad en contextos donde los recursos son escasos, desafiando las percepciones convencionales sobre la relación entre recursos y seguridad en la criptografía.

Eficiencia y Rendimiento

En términos de eficiencia y rendimiento, los algoritmos ligeros destacan claramente. PRESENT, Speck y Simon están diseñados específicamente para operar en entornos con recursos limitados, lo que se traduce en tiempos de procesamiento más cortos y un menor consumo de recursos. Estos algoritmos son ideales para aplicaciones que requieren cifrado y descifrado rápidos en dispositivos con capacidades limitadas, lo que es fundamental en sistemas IoT de bajo costo. En contraste, los algoritmos clásicos, aunque seguros, a menudo sacrifican la eficiencia debido a la naturaleza intensiva en recursos de sus operaciones matemáticas. RSA y AES pueden ser más adecuados para aplicaciones en las que la velocidad no es una preocupación primordial y donde la seguridad es la principal prioridad, pero esto puede no ser óptimo en sistemas IoT de bajo costo.

Aplicabilidad

La aplicabilidad de los algoritmos depende en gran medida de las necesidades específicas de la aplicación en sistemas IoT de bajo costo. Los algoritmos clásicos, como RSA y AES, son esenciales para aplicaciones que requieren un alto nivel de seguridad, como la autenticación en línea y la protección de datos sensibles. Sin embargo, su uso puede no ser óptimo en dispositivos con recursos limitados y presupuestos ajustados.

Los algoritmos ligeros, como PRESENT, Speck y Simon, son vitales en el mundo de IoT y sistemas embebidos de bajo costo, donde la eficiencia y la velocidad son cruciales. Estos algoritmos encuentran su nicho en aplicaciones que buscan un equilibrio entre seguridad y rendimiento en plataformas con recursos restringidos y costos bajos.

Consideraciones Finales

La elección entre algoritmos clásicos y algoritmos ligeros no es una decisión trivial, especialmente en sistemas IoT de bajo costo. La comparativa de seguridad y rendimiento subraya la importancia de un enfoque equilibrado, teniendo en cuenta las necesidades específicas de la aplicación y las restricciones presupuestarias. Los algoritmos clásicos ofrecen seguridad sólida, pero a menudo a costa de la eficiencia. Los algoritmos ligeros priorizan la eficiencia, aunque podrían proporcionar un nivel ligeramente menor de seguridad en comparación con los clásicos.

En última instancia, la elección del algoritmo criptográfico adecuado depende de un análisis completo de las necesidades del sistema, las amenazas potenciales y las restricciones de recursos, especialmente en sistemas IoT de bajo costo. La evolución tecnológica y las amenazas de seguridad constantes requieren una evaluación continua y una adaptación para garantizar la protección de los datos en un mundo cada vez más conectado y económicamente accesible.

CONCLUSIÓN

Los algoritmos clásicos, como RSA y AES, basados en fundamentos matemáticos sólidos, ofrecen un alto nivel de seguridad. Son fundamentales en aplicaciones que requieren una protección sólida, como autenticación y comunicación segura.

Los algoritmos ligeros, como PRESENT, Speck y Simon, diseñados para entornos con recursos limitados, brindan un nivel razonable de seguridad hasta cierto punto de datos fáciles de descifrar, a pesar de sus longitudes de clave más cortas. Son adecuados cuando la eficiencia es crítica.

Los algoritmos clásicos tienden a priorizar la seguridad en detrimento del rendimiento, lo que los convierte en sistemas adecuados para aplicaciones donde la velocidad no es crítica y la seguridad es primordial.

Los algoritmos ligeros destacan por su eficiencia y rendimiento optimizado, siendo ideales para aplicaciones que requieren operaciones rápidas en dispositivos con recursos limitados.

La elección entre algoritmos clásicos y ligeros debe basarse en el contexto específico de la aplicación, equilibrando seguridad, eficiencia y recursos disponibles.

La ciberseguridad está constantemente evolucionando, por lo que la elección de algoritmos debe revisarse periódicamente para hacer frente a nuevas amenazas.

Toma de Decisiones Informada: Se necesita un profundo análisis de los requisitos y objetivos de seguridad de la aplicación para seleccionar el algoritmo criptográfico adecuado.

REFERENCIAS BIBLIOGRÁFICAS.

Abujoodeh, M., Tamimi, L., & Tahboub, R. (2023). Toward Lightweight Cryptography: A Survey. Computational Semantics. doi:10.5772/intechopen.109334

Alves, F. (2023). Es esencial ir un paso por delante de las ciberamenazas - Evaluación de las vulnerabilidades. Obtenido de https://www.linkedin.com/pulse/evaluaci%C3%B3n-de-la-vulnerabilidades-base4-security/?originalSubdomain=es

AppMaster. (2023). Métricas empresariales para tomar decisiones informadas. (AppMaster) Obtenido de https://appmaster.io/es/blog/cracking-business-metrics-informed-decisions-es

Campos, M. (2015). Monitorización de respuestas físicas y fisiológicas al entrenamiento y la competición en fútbol. Sevilla: Universidad Pablo de Olavide.

Centro Criptológico Nacional. (2023). Guía de Mecanismos criptográficos autorizados por el CNN. Madrid: Ministerio de defensa España.

Coronel, C. (2018). Comparación del rendimiento y nivel de seguridad en algorítmos criptográficos ligeros PRESENT, CLEFIA, KECCAK y HIGHT: Una revisión sistemática. Samborondón: Universidad Espíritu Santo.

De la Parra, R. (2020). Seguridad en redes inalámbricas de área corporal mediante criptografía ligera. Tamaulipas: Centro de Investigación y de Estudios Avanzados del IPN.

Delgado, M. (2022). Curvas elípticas en la criptografía. Madrid: Universidad Politécnica de Madrid.

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. Wireless Pers Commun(112), 1947–1980. doi:https://doi.org/10.1007/s11277-020-07134-3

Eterovic, J., & Cipriano, M. (2018). Stream Ciphers Livianos estandarizados mediante normas internacionales para ser usados en Internet de las Cosas. SISTEMAS, CIBERNÉTICA E INFORMÁTICA, XV(2), 29 - 33.

Fernández, C. (2007). Análisis comparativo a nivel teórico práctico de los algoritmos criptográficos orientado hacia la solución del problema de seguridad del transporte de documentos. Cuaca: Universidad del Cuaca.

Frąckiewiczen, M. (2023). La relación entre la salud digital y el Internet de las cosas (IoT). (TS2) Obtenido de https://ts2.space/es/la-relacion-entre-la-salud-digital-y-el-internet-de-las-cosas-iot/

Gálvez, H. (2014). Análisis de algoritmos criptográficos en una red híbrida P2P. Concepción: Universidad del Bio-Bio.

Garg, A., Gupta, P., & Bhullar, P. (2021). Is CSR Expenditure Relevant to the Firms in India? Organizations and Markets in Emerging Economies, XII(1), 178-197.

Gleimer, L. (2023). ¿Qué Es La Criptografía? Obtenido de https://www.linkedin.com/pulse/criptograf%C3%ADa-luis-gleimer-lambra%C3%B1o/?originalSubdomain=es

Hoy Digital. (2023). El poder y los desafíos de los dispositivos conectados. (Hoy Digital) Obtenido de https://hoy.com.do/el-poder-y-los-desafios-de-los-dispositivos-conectados/

IEEE Standards Association. (22 de Abril de 2016). 802.15.4-2015 - IEEE Standard for Low-Rate Wireless Networks. (IEEE) doi:10.1109/IEEESTD.2016.7460875

Kahn, D. (1967). The Codebreakers: The story of secret writing. New York: Macmillan.

Kariuki, C. (2023). Encriptación simétrica explicada en 5 minutos o menos. (GEEKFLARE) Obtenido de https://geekflare.com/es/symmetric-encryption/

Kim, J., Sung, H., Kim, J., & Kim, M. (2019). Lightweight cryptography for Internet of Things: A survey. Electronics, VIII(10), 1035. doi:10.1016/j.electronics.2019.10.1035

Conflicto de intereses

Los autores indican que esta investigación no tiene conflicto de intereses y, por tanto, acepta las normativas de la publicación en esta revista.

Con certificación de: