Tipo de artículo: Artículo original

Diseño y desarrollo de un Algoritmo de Cifrado. BitSAY

Design and Development of one Encription Algorithm. BitSAY

Yoel David Correa Duke [1], **https://orcid.org/0000-0001-7687-8969**

[1]Estudiante de Ingeniería en Ciencias Informáticas, Facultad de Tecnologías Educativas, Universidad de las Ciencias Informáticas. Cuba.

Autor para correspondencia: yoeldcd@estudiantes.uci.cu

Resumen:

Partiendo de la necesidad de proteger los activos de información que se emplean de forma creciente en las diferentes empresas y organizaciones, se ha definido la tarea de implementar un nuevo algoritmo criptográfico que implemente una tecnología de seguridad altamente confiable y segura basada en reformulaciones de las lógicas criptográficas existentes. Sobre la base a la observación del contexto, se ha desarrollado un proceso investigativo enfocado a realizar un análisis de las características y principios de funcionamiento de los criptosistemas modernos, el estudio de las metodologías de ataque criptoanalítico y sus particularidades y; en asociación a ambos conceptos, la determinación de las vulnerabilidades presentes en los primeros en consecuencia de los segundos. Una vez estudiadas las diversas temáticas vinculadas, se aplicaron una serie de métodos inductivos y deductivos que permitieron determinar una serie de características requeridas para supera las limitantes halladas, a partir de las cuales se elaboró el diseño y fueron implementados los correspondientes aplicativos. Todo esto, con el único objetivo de: Implementar un algoritmo criptográfico que cumpla con los requisitos de seguridad y eficiencia óptimos para realizar su despliegue dentro de las diferentes plataformas informáticas en desarrollo. Finalizadas las actividades teórico-prácticas, se realizó la evaluación de las características operacionales del motor de cifrado BitSAY, las cuales ofrecieron valores altamente satisfactorios que permitieron valorar la posibilidad de implementar esta novedosa tecnología en los productos desarrollados por la Universidad de las Ciencias Informáticas a modo de plataforma de seguridad autónoma.

Palabras clave: criptografía; criptoanálisis; criptosistemas; vulnerabilidades; algoritmos.

Abstract:

Starting from the need to protect information assets that are increasingly used in different companies and organizations, the task of implementing a new cryptographic algorithm that implements a highly reliable and secure security technology based on reformulations of logic has been defined. existing cryptography. Based on the observation of the context, an investigative process has been developed focused on carrying out an analysis of the characteristics and operating principles of modern cryptosystems, the study of cryptanalytic attack methodologies and their particularities and; In association with both concepts, the determination of the vulnerabilities present in the former as a consequence of the latter. Once the various related topics had been studied, a series of inductive and deductive methods were applied that made it possible to determine a series of characteristics required to overcome the limitations found, from which the design was developed and the corresponding applications were implemented. All this, with the sole objective of: Implementing a cryptographic algorithm that meets the optimal security and efficiency requirements to carry out its deployment within the different computer platforms under development. After the theoretical-practical activities, the evaluation of the operational characteristics of the BitSAY encryption engine was carried out, which offered highly satisfactory values that allowed assessing the possibility of implementing this novel technology in the products developed by the University of Informatics Sciences as autonomous security platform.

Keywords: *cryptography; cryptanalysis; cryptosystems; vulnerabilities; algorithms.*

Recibido: 18/12/2021
Aceptado: 20/03/2022
En línea: 01/06/2022

Introducción

En respuesta a la continua necesidad de proteger de agentes delictivos aquellos datos institucionales de los cuales las entidades dependen para gestionar sus procesos y/o vincularse con sus consumidores, y dado que los mismos son generados, transmitidos y/o procesados mediante el empleo de las Tecnologías de la Informática y las Comunicaciones, los desarrolladores se han visto obligados a implementar metodologías y prácticas de diseño y desarrollo enfocadas al aseguramiento de los modelos de gestión de información y la reducción de las vulnerabilidades existentes en las distintas infraestructuras tecnológicas sobre las cuales son desplegados sus aplicativos como parte de las tareas de digitalización de los servicios y la sociedad en general.

Considerando esta situación problemática y partiendo de conceptos como la ciberseguridad, son empleados mecanismos y protocolos para proporcionar un mayor nivel de resistencia a las plataformas desplegadas frente a las distintas herramientas de intercepción y penetración que son empleadas por los agentes externos con fines lesivos. Dentro de las prácticas aplicadas con dicho fin se destacan, entre otras, el empleo algoritmos de cifrado; representados exponentes ampliamente aceptados como AES-256 y DES v3.0 y que; haciendo uso de lógicas, operan con una o varias claves secretas sobre los activos, permitiendo así su ocultamiento ante las autoridades no propietarias. mediante el truncado de los mismos en forma de criptogramas ilegibles; los cuales solo pueden ser revertidos a su estado original usando las credenciales correctas. (Algoritmos de cifrado comunes y ejemplos de aplicaciones en Android, 2020) En contraposición a estos mecanismos de seguridad, y con motivo de eludir las lógicas sobre las cuales operan, en la actualidad se da continuidad a estudios criptoanalíticos, los cuales, partiendo de investigaciones precedentes, han hallado todo un campo de soporte en tecnologías modernas como la Inteligencia Artificial y la Computación Cuántica, así como también en ramas de la matemática como el Cálculo Diferencial Avanzado. Trabajos que son el producto de las relaciones entre Centros Investigativos y Agencias Militares y de Seguridad; siendo estas últimas impulsoras de esta clase de proyectos a causa del valor atribuido a la información para realizar sus operaciones de tácticas de seguimiento y espionaje (Criptoanálisis, n.d.) La combinación de todos estos actores en su conjunto representa un riesgo real que puede llegar a comprometer los criptogramas; a día de hoy, generados con dichos sistemas de cifrado e implícitamente vulnerar los protocolos y plataformas donde se han desplegado; mismas que

mueven los engranes de los sistemas económicos y las redes de comunicación de todo el mundo (Gomez, 2021); no siendo Cuba una excepción dados los intereses geopolíticos de algunos actores regionales.

Lo expresado anteriormente plantea como Problema de Investigación la inexistencia de un algoritmo criptográfico nacional, cuya lógica no se vea sujeta a las vulnerabilidades teóricas postuladas y que sea capaz de ser integrado dentro de los procesos de informatización como plataforma de Soberanía Tecnológica, proponiendo como Hipótesis que: "Si se implementa un algoritmo de cifrado que herede lógicas implícitas en los actuales, y que introduzca otras de mayor complejidad, éste será invulnerable, tanto a las técnicas de criptoanálisis actuales, como a aquellas aún en desarrollo". Se ha desarrollado el presente trabajo y sus correspondientes aplicativos definiendo como Objetivo General: Diseñar e implementar un algoritmo criptográfico bajo la denominación BitSAY que cumpla con los requisitos de seguridad y los valores de eficiencia óptimos, necesarios para realizar su despliegue dentro de plataformas y productos de origen nacional; y en última instancia, ser extrapolado a contextos de aplicación foráneos.

Materiales y métodos

El desarrollo de esta investigación se organizó en 6 etapas fundamentales donde se llevaron a cabo un conjunto de tareas analíticas, deductivas y prácticas, que permitieron, mediante la asignación de los intervalos de trabajo según su complejidad y criticidad, la correcta ejecución de las actividades y con ello la consecución de los objetivos planteados.

Como punto de partida, se procedió a realizar un estudio del contexto y los exponentes relevantes relacionados a la seguridad de los activo de información en la industria del desarrollo de productos y la prestación de servicios informáticos. Partiendo de esta idea se consultó un grupo de materiales multimedia de tipo audiovisual y en formato de libros digitales, vinculados a dicho campo, donde quedaban expuestos principios de funcionamiento; tanto de algoritmos de cifrado como de ciertas prácticas criptoanalíticas actuales y en desarrollo, así como las pautas evolutivas que dieron cabida a su desarrollo.

Una vez finalizada esta etapa de consulta teórica; y con ella esclarecidos los elementos contextuales y los riesgos existentes en el entorno de la ciberseguridad para los criptosistemas, se llevó a cabo un proceso deductivo que permitió determinar las causas no explícitas en la documentación, que hacían a muchos de los existentes vulnerables a las técnicas de criptoanálisis estudiadas. En base a esta deducción, y una vez definida el principio de hipótesis que sustentara el posterior desenlace de la investigación, se procedió a continuación a inducir mediante una rápida lluvia de ideas todo un conjunto de características que permitieran superar las vulnerabilidades evidenciadas; siendo éstas el principio funcional del aplicativo que a continuación sería implementado.

Tras definir las características funcionales del algoritmo como producto a las fases previas realizadas, se inició el diseño a nivel lógico del mismo. Durante esta fase fueron determinados los modelos estructurales y la asignación de los flujos de trabajo entre los distintos componentes, también se puntualizaron temas antes obviados, como las limitaciones de hardware, el tratamiento de excepciones, y los parámetros operativos y rangos de uso de recursos óptimos para su funcionamiento. Señalar además, que en paralelo se definió un concepto de interface para agilizar los procesos de prueba, y una iconografía identificativa que para el producto una vez este fuere completado.

Una vez establecidas las pautas de desarrollo, se procedió a la selección de las herramientas de codificación, siendo JAVA en su versión OpenJDK v11 el lenguaje selecto: dado su alto nivel de portabilidad, sus facilidades para operar con hilos, ficheros y excepciones, y sobre todo por su semántica basada en clases y objetos; idónea para la estructuración de los componentes diseñados. Como IDE, se determinó hacer uso del NetBeans v8.2 teniendo en cuenta: su simple instalación y manejo, sus herramientas de depuración, y sus facilidades para controlar las tareas en segundo plano. Tras ser seleccionados los medios se procedió a implementar el motor de cifrado BitSAY CoTaAnKe.

Luego de completarse la codificación del aplicativo, y con motivo de evaluar sus características operativas en función de los valores óptimos establecidos se procedió a realizar un conjunto de pruebas que permitieran; mediante el análisis de los resultados obtenidos, determinar los límites de aplicabilidad del algoritmo.

1 - Antecedentes Históricos de la protección de la Información.

Ya sea usada como recurso bélico estratégico y decisivo o por la mera privacidad de su contenido, mucha información ha debido ser tratada a lo largo de la historia de una manera particularmente segura en fin de propiciar que solo aquellos con el privilegio o el derecho de disponer de ella así lo hagan (Velasco, 2014) Partiendo de esta idea es posible definir: Que los principios de los criptosistemas modernos son el resultado de un proceso evolutivo, en el cual han intervenido toda una serie de factores históricos y exponentes teóricos-tecnológicos, que han dado paso a la criptología actual.

En base a este consenso; y para comprender los principios de funcionamiento, implícitos y heredados por los algoritmos de cifrado, se decidió hacer un pequeño resumen de sus precedentes.

Como primer principio de operación, tenemos los algoritmos basados en sustitución mono alfabética como (El cifrado de Cesar, y las piedras Rosseta de Ejipto) y el poli alfabético; representad por: el Cifrado de Polibio y las tablas de Blaise Vigener), ambas modalidades vulnerables al análisis frecuencial o probabilístico (Díaz, 1995). Otro principio de funcionamiento heredado es la transposición columnar de matrices; tanto su forma simple; resaltando la Scitala de Homero, como en su variante guiada por clave donde se emplean matrices indexadas. Finalmente otro exponente

histórico a considerar dada su gran relevancia fue: El mecanismo de cifrado, basado en discos, empleado por la maquina Alemana Enigma durante la II Guerra Mundial para el cifrado de las ordenes militares procedentes del alto mando Nazi.

En este proceso se destacaron ensayos y estudios que permitieron fundamentar los principios históricos de la criptografía y el criptoanálisis, siendo los más significativos; no en este orden: Los 6 principios de Kerchoft, Polygraphia de Johannes Trithemius y Traicte des Chiffre de Blaise de Vigenere.

Otros principios de funcionamiento más modernos son aquellos basados en le cifrado de flujos de datos de forma lineal como el algoritmo RC4, y los que subdividen la información en bloques independientes; introducido por DES y aplicable a AES-256 y 3DES. También están los algoritmos asimétricos como RSA que en base a propiedades matemáticas de euler permiten el empleo de llaves complementarias.

2 - Técnicas de criptoanálisis.

En base a comprender que hacía vulnerables a los algoritmos actuales, se emprendió un recorrido en profundidad atraves del campo del criptoanálisis, con tal de esclarecer las características y limitaciones de este tipo de prácticas. En primer lugar se analizó la técnica de rompimiento por fuerza bruta o conocida por su acrónimo BEAST, la cual se basa en usar todas las posibles combinaciones de llaves hasta obtener la correcta, trabajo que ;aún y dado el crecente incremento de las capacidades del hardware, no es rentable dado el espacio de llaves de muchos algoritmos; rondando los trillones de combinaciones, pero no siendo descartable dado el acercamiento a la era post-cuántica; permitirá eludir todas las limitaciones del hardware. (Criptoanálisis)

Otras prácticas basadas en principios matemáticos las constituyen el criptoanálisis lineal, el diferencial y el frecuencial o estadístico que analizan los criptogramas para aplicar la inversión de su lógica en fin de determinar la clave con la cual fueron creados en base a resoluciones de combinatoria matemáticas. En este sentido además, en el caso de los algoritmos basados en cifrado por bloques pueden catalogarse tres formas de riesgo fundamentales, siendo estas la deducción: parcial, total o local, de las claves de bloque.

Desde un punto de vista más cercano a los propietarios de la información, están los riesgos de Intercepción de claves; por causa de negligencia propia de los mismos, y los ataques basados en diccionarios de credenciales frecuentes, siendo estos últimos a día de hoy potenciables mediante el empleo de tecnologías probabilísticas y deductivas automatizadas como las Inteligencias Artificiales; que apoyadas en las grandes bases de conocimiento disponibles en internet pueden determinar; basado en el seguimiento de las tendencias y comportamientos; las potenciales credenciales de los objetivos.

3 - Vulnerabilidades de los Algoritmos modernos.

Una vez estudiadas las características comunes en las alternativas de cifrado actuales; y en complemento analizadas las prácticas de criptoanálisis a las cuales los mismos se ven expuestos en su contexto, y partiendo de una evaluación crítica de los factores condicionantes, se determinaron las causas o principios funcionales de muchos de estos que los hacen vulnerables.

Para demostrar el análisis realizado, en la siguiente lista se exponen los principios generales sobre los cuales trabajan muchos algoritmos criptográficos modernos como AES y 3DES.

- Empleo de operaciones de lógica booleana como XOR, NOT y AND.
- Uso del modelo Feistel para la simplificación de la reversión del proceso.
- Cifrado en bloques simétricos.
- Substitución polialfabética de valores de byte.
- Derivación de claves complejas en base a credenciales más simples como contraseñas.
- Transformaciones de Permutación matricial simples.
- Permutación pseudoaleatoria de elementos.
- Cifrado de bloques en varias rondas.

Vistas estas característica era evidente que sus lógicas están implementadas con el objetivo de optimizar el uso de recursos empleados y evitar alta complejidades ciclomáticas por unidad de bloque procesado. Partiendo de esta observación y sustentado por un proceso cognitivo de deducción, fue posible determinar las siguientes vulnerabilidades; no explicitas en la bibliografía:

- El procesamiento de bloques simétricos tanto en el cifrado como en el descifrado de los medios.
- Ausencia de redistribuciones a nivel de bloque durante la salida de estos al cifrar o inversamente durante su lectura al descifrar.
- Empleo de operaciones de desplazamiento matricial lineales o simples en su lógica.
- Uso de claves de bloque de insuficiente longitud o rango.

4 - Definición de la lógica de BitSAY CoTaAnKe.

Teniendo en cuenta las capacidades de cómputo y memoria de los sistemas actuales y tras inducirse un grupo de soluciones para enfrentar las vulnerabilidades actuales de los criptosistemas modernos en base a los análisis previos, fue posible plantear una serie de complejizaciones a las lógicas de estos esquemas enfocadas a ofrecer un alto nivel de robustez a los criptogramas generados, sin sacrificar características tan críticas como su eficiencia y velocidad. Sustentado en estas características y tomando una serie de consideraciones técnicas, se definieron los siguientes principios funcionales para el motor criptográfico; siendo algunos de ellos variaciones de los mecanismos precedentes y otros particularidades propias de su lógica algorítmica.

- Hacer uso de Operaciones de lógica booleana como XOR, NOT a nivel de bit mediante un esquema de aplicación selectivo y pseudoaleatorio, que dificulte su seguimiento mediante lógicas análisis lineal.
- Implementar una función Feistel complejizada que simplifique las etapas de cifrado y descifrado de los bloques y sus demás componentes, que cuente con particularidades propias.
- Permitir la paralelización del cifrado y descifrado de bloques contiguos, siendo esto configurable en base a las restricciones del hardware sobre el cual sea portado.
- Emplear un modelo de encriptación a nivel de bloques, donde estos sean capturados y guardados con dimensiones variables o asimétricas pseudoaleatoriamente seleccionadas durante su entrada y/o salida sin la presencia de incoherencias en los medios cifrados o descifrados.
- Utilizar una tercera subcapa de cifrado a nivel de fragmento o sub-bloque que realice las operaciones a nivel de matriz; incluidas permutaciones de lógica complejizadas como (Columnar and Vertical Jumping Distribution), y que use igualmente el principio de asimetría en las estructuras de datos procesadas. Los fragmentos además deben ser redistribuidos y procesados en varias rondas de forma pseudoaleatoria y durante las mismas se complejizarán las claves de control y el alfabeto substitutivo empleado para realizar el truncado de las secuencias de byte.
- Implementar una serie de mecanismos de validación, que requieran de un segmentos de meta-información generado durante el cifrado, y que permita: asegurar el uso de la credencial correcta durante el descifrado, impedir la inyección de datos mediante control de extensión de salida y entrada, y reconfigurar el estado de los parámetros de procesamiento.
- Implementar interfaces de comunicación que permitan el tratamiento de excepciones y el seguimiento del progreso de las operaciones ejecutadas.

Una vez planteadas todos estos requisitos funcionales se procedió a realizar el diseño de las estructuras algorítmicas y matemáticas involucradas.

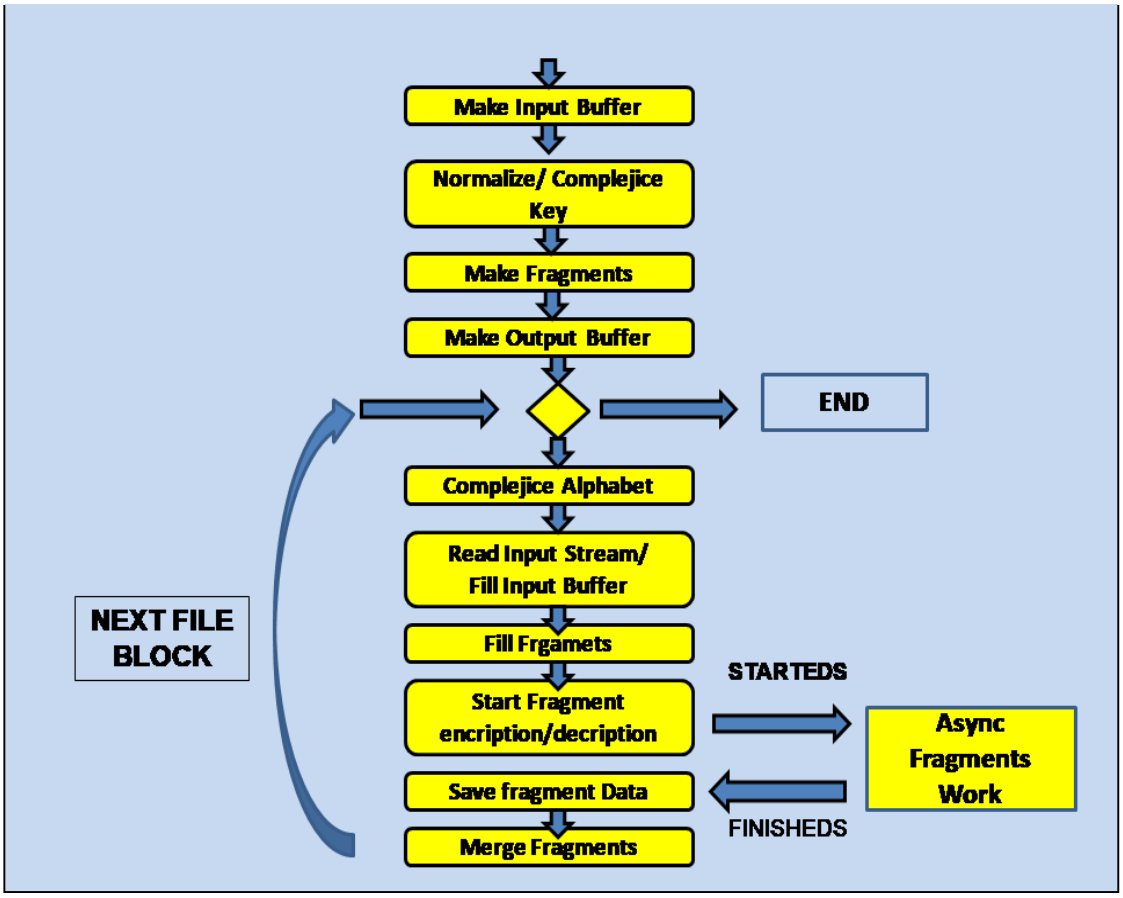

Figura 1. Diagrama de flujo de las operaciones a Nivel de Bloque.

5 - Definición del Modelo Estructural del Algoritmo.

BitSAY es un concepto de algoritmo que se estructura en varios componentes asociados a cada diferente nivel de cifrado. En base a esto; y aplicando principios de diseño como “Eslabón más Débil” o “Divide y Venceras”, a los mismos se les han atribuido responsabilidades y complejidades ciclomáticas linealmente-proporcionales a la profundidad sobre la cual son procesamiento las estructuras de datos del medio. Teniendo todo esto en cuenta se han definido los siguientes componentes estructurales y sus correspondientes relaciones de control.

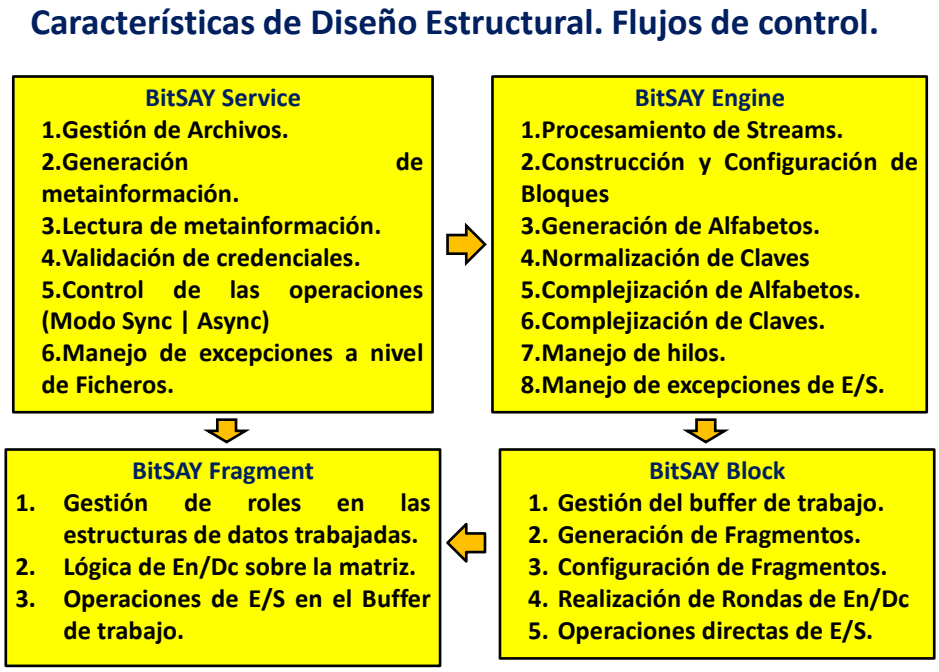

Figura 2. Componentes y modelo de control del Sistema.

6 - Diseño de una interface de Control

Con el objetivo de proporcionar un producto de fácil manejo para el usuario promedio, y partiendo de las características funcionales definidas para el motor de cifrado a nivel de código, se elaboró un modelo de interface gráfica la cual proporcionaría un mayor nivel de usabilidad al producto en entornos de escritorio. Dicha interface se codifico como un módulo totalmente independiente y no es de suma obligatoriedad su ejecución a la hora de ejecutar el motor de cifrado. La misma cuenta con un serie de controles individuales y simples que permiten la selección de los archivos y definir la configuración de un alto número de parámetros a la hora de trabajar con los ellos; tanto en etapas de cifrado como durante el descifrado. Esta además incluye un conjunto de diálogos que permiten al usuario conocer: el estado de las operaciones en progreso, la validez de las credenciales insertadas, parte de la meta-información asociada a los criptogramas generados; una vez se usa la credencial valida, y diferentes reportes de error relacionados a eventos de excepción.

Resultados y discusión

Una vez desarrollado el diseño e implementación del algoritmo de cifrado BitSAY se procedió a realizar sobre el mismo un grupo de pruebas con el fin de medir sus distintos parámetros operativos en función de los requisitos óptimos planteados. Para la realización de las mediciones se aplicaron diferentes parámetros de rondas de seguridad y numero de hilos óptimos; 7 Rondas y 10 Hilos, a diferentes dimensiones de archivo que representaron las muestras de prueba. Además para la captura de los datos estadísticos se emplearon herramientas como Java Mision Control y el propio IDE, y en fin de agilizar su procesamiento se empleó Microsoft Office Excel 2017. A continuación se muestran los resultados promedios de las mediciones realizadas.

Tabla 1 Resultados de las mediciones realizadas al motpr de cifrado BitSAY.

Muestra	Tamaño Original (MB)	Medición 1 Encriptación		
		CPU %	Memoria (s)	Tiempo (s)
Archivo pequeño	15,5	40,0%	85,6	1
Archivo mediano	92,1	34,1%	91,2	4
Archivo grande	548,4	25,0%	92,9	35
Muestra	**Tamaño Cifrado (MB)**	**Medición 2 Desencriptación**		
		CPU %	Memoria (s)	Tiempo (s)
Archivo pequeño	16,1	38,0%	79,4	1
Archivo mediano	95,5	27,0%	94,1	5
Archivo grande	568,5	55,0%	100,6	25

Partiendo de estos resultados, y en el fin de valorar autocríticamente los mismos, se les decidió agrupar en torno a 4 aspectos o categorías evaluativas fundamentales:

- ***Complejidad Criptográfica*:**

Se diseñó un algoritmo que hereda lógicas precedentes aplicándolas mediante un enfoque de configuración más complejo y en complemento con definiciones propias asegura su invulnerabilidad. Para muestra de ello están principios introducidos como el cifrado a nivel de fragmento y su redistribución a nivel de bloque, procesamiento de bloques de entrada y salida asimétricos, el empleo de operaciones matriciales como la Distribución de rebote guiado o el uso de NOT y XOR selectivo.

- ***Velocidad de Cifrado*:**

Como bien muestran las estadísticas el algoritmo cumplió con los requisitos mínimos establecidos en cuanto a tasa de bloques cifrados por segundo, dado que en base a su velocidad en MB/s se estimó una media de 3000 bloques/segundo.

- ***Consumo de memoria*:**

Si bien en algunos casos particulares los valores de uso de memoria fueron algo superiores; como se aprecia en la siguiente gráfica, puede considerarse que se obtuvieron resultados factibles que no suponen un gran desafío para las capacidades del hardware computacional moderno y que varía primeramente en función de las dimensiones de los medios de entrada; tanto para el caso de su cifrado como en su descifrado del mismo.

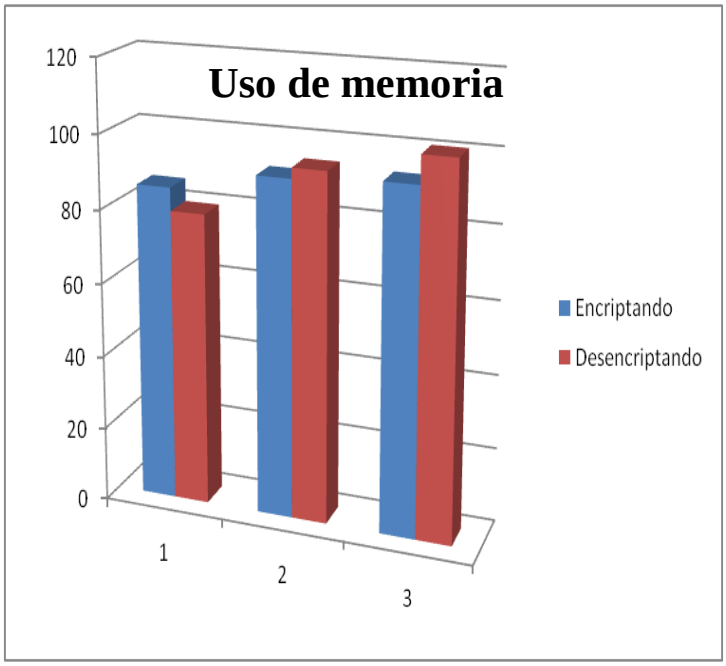

Figura 3. Gráfico con los valores promedios de uso de Memoria RAM.

- ***Uso del CPU*:**

En relación al empleo de la CPU también se obtuvieron resultados satisfactorios que demostraron la importancia de todas las optimizaciones aplicadas al aplicativo durante sus etapas de diseño e implementación. La siguiente gráfica corrobora este hecho.

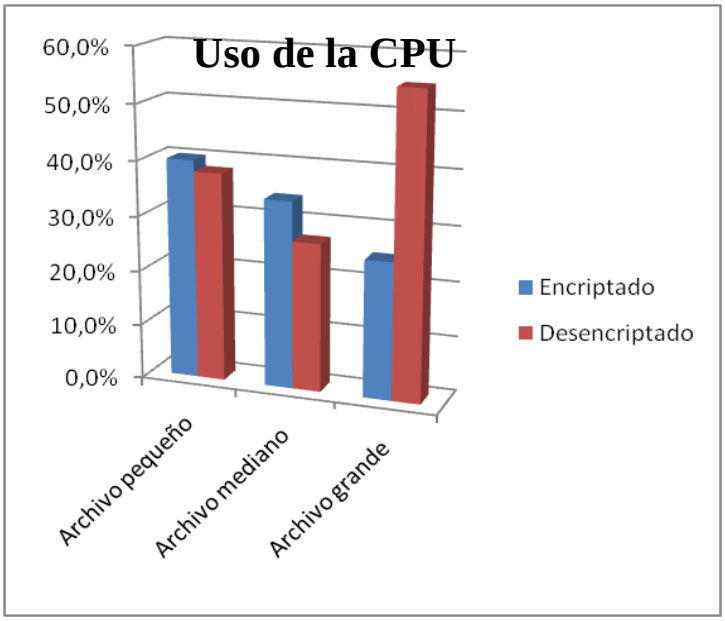

Figura 4. Gráfico con los valores promedios de uso de CPU.

Como es observable, BitSAY posee un alto nivel de configuración y portabilidad. Debido a esto es altamente adaptable y es posible realizar su implementación en dispositivos con prestaciones limitadas como los móviles, artículos vestibles y equipos IoT; en fin de asegurar los datos que estos procesan sin explotar demasiado las características de su hardware.

En asociación a todas estas características técnicas, a nivel de usabilidad el módulo de interface desarrollado; bajo la denominación BitSAY Security, proporciona un modelo de control simplificado y amigable que puede ser fácilmente empleado por los usuarios promedio sin requerir de una curva de aprendizaje elevada. Además su estética, contrastante y minimalista es agradable a la vista y la selección de colores para los controles principales transmite de forma subjetiva la intención de la operación que realiza. También cabe considerar que se han definido valores en los reguladores que son factibles; tanto en mínimo como en máximo, para establecer un rango operacional suficientemente seguro y ergonómico. Por último, se destaca la selección de una imagen iconográfica que incentiva al usuario a usar el producto dado su similitud a un candado, el empleo de una paleta de colores fuertes y la simetría de su geometría hexagonal.

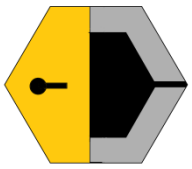

Figura 5 Concepto iconográfico de BitSAY

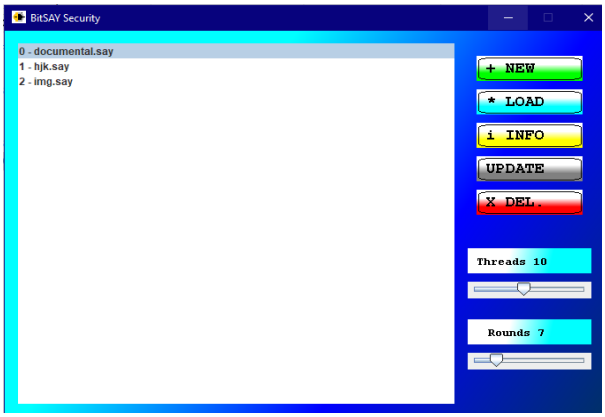

Figura 6. Interface de usuario principal BitSAY Security.

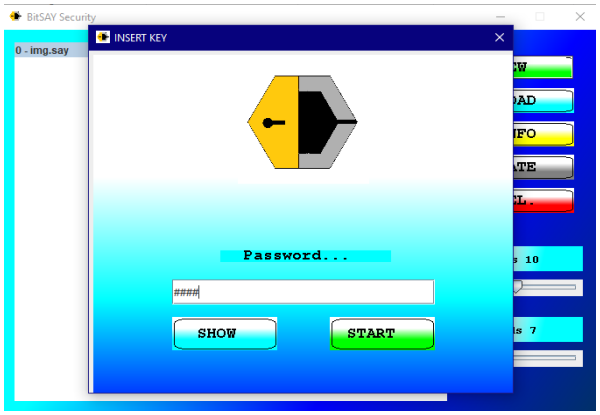

Figura 7. Cuadro de inserción de credencial.

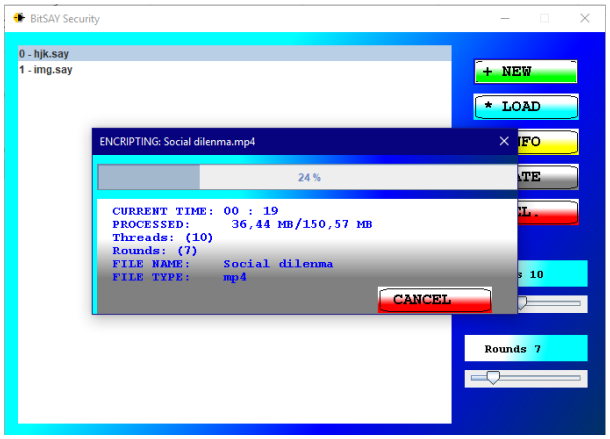

Figura 8. Cuadro de información y progreso de tareas.

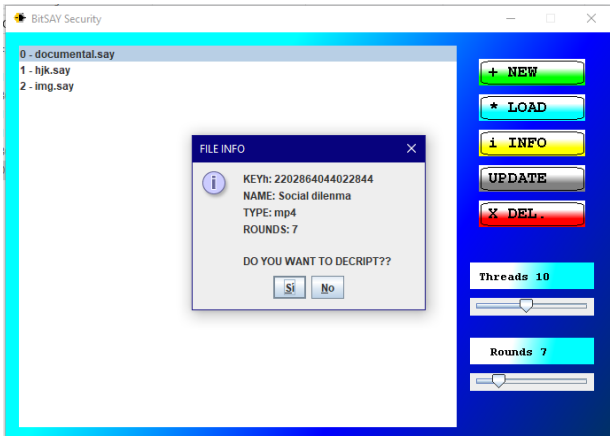

Figura 9. Cuadro de información con los datos de salida y configuración del criptograma.

Conclusiones

El estudio desarrollado en relación al contexto de la ciberseguridad y los algoritmos de cifrado modernos, contribuyó no solo a la educación general integral de este joven investigador sino; que además, permitió su crecimiento profesional en vistas a su vocación de futuro desarrollador, dada la importancia que el tratamiento de este tema tiene atribuida. En complemento con esto y sustentado por los resultados obtenidos es posible dar por cumplidos los objetivos con los cuales se decidió desarrollar esta investigación e implementar los correspondientes aplicativos.

BitSAY es un algoritmo altamente complejo que toma lo mejor de las lógicas presentes en los algoritmos actuales e introduce otras novedosas que le permiten cumplir con altos estándares de seguridad sin sacrificar características como rendimiento o consumo de recursos. Además de esto y dada la naturaleza pseudoaleatoria de procedimientos internos como el tratamiento de los bloques de datos, la generación claves de normalizadas y la complejización de alfabetos substitutivos, es posible establecer que es altamente robusto a las técnicas de análisis criptográfico basadas en probabilidad, las cuales constituyen la base de esta clase de estudios. En conjunto a este principio y dada su facilidad para ser adaptado a diferentes plataformas y lenguajes, este mecanismo es un exponente novedoso a considerar en fin de asegurar la integridad de los activos de información que puedan y deban ser tratados por soluciones informáticas de origen nacional, pudiendo incluso ser extrapolado a un contexto de aplicación foráneo.

Por otro lado: Aún y cuando en la actualidad este algoritmo es capaz de brindar alta seguridad a medios confidenciales; con él, protegidos, es necesario plantear su continua evolución en vista al riesgo que trae atribuido el continuo desarrollo de los estudios criptoanalíticos y su extensión a nuevas y más versátiles tecnologías de soporte, para la integridad de los criptogramas generados.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Yoel David Correa Duke.
2. Curación de datos: Yoel David Correa Duke.
3. Análisis formal: Yoel David Correa Duke.
4. Investigación: Yoel David Correa Duke.
5. Metodología: Yoel David Correa Duke.
6. Software: Yoel David Correa Duke.
7. Supervisión: Yoel David Correa Duke.
8. Validación: Yoel David Correa Duke.
9. Visualización: Yoel David Correa Duke.
10. Redacción – borrador original: Yoel David Correa Duke.
11. Redacción – revisión y edición: Yoel David Correa Duke.

Referencias

Algoritmos de cifrado comunes y ejemplos de aplicaciones en Android. (2020). Obtenido de https://programmerclick.com/Algoritmos%20de%20cifrado%20comunes%20y%20ejemplos%20de%20aplicaciones%20en%20Android%20-%20programador%20clic.html

Criptoanálisis. (s.f.). Obtenido de Wikipedia: https://es.wikipedia.org/w/index.php?title=Criptoanalisis&redirect=no

Cuba, L. C. (1948). *Rebeca Rosell Planas.* La Habana: Archivo Nacional de Cuba.

Díaz, J. C. (1995). *Criptografía Historia de la Escritura Cifrada.* Complutense.

Gomez, B. (18 de Abril de 2021). *AES-256 ¿Qué es? ¿Cómo funciona? (Mejor explicación)*. Obtenido de https://www.profesionalreview.com/2021/04/18/aes-256/

Neira, B. S. (2011). Implementation of a cryptography algorithm AES on a vehicular traffic controller. Obtenido de Implementation of a cryptography algorithm AES on a vehicular traffic controller.

Neuro Chispas. (s.f.). Obtenido de Permutaciones y combinaciones fórmulas: https://www.neurochispas.com/Permutaciones y combinaciones fórmulas

Principios de Kerckhoffs. (s.f.). Obtenido de Wikipedia: https://es.wikipedia.org/w/index.php?title=Principio_de_Kerckhoffs&redirect=no

Triguedo, J. J. (2005). *Iintroducción a la criptografía.* La Mancha: Universidad de Castilla.

Velasco, J. J. (20 de Mayo de 2014). *Breve historia de la criptografía*. Obtenido de https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html