

Propuestas de mejora DES y Triple DES a lo largo de su historia

DES and Triple DES improvement proposals throughout its history

Laura Ximena Ahumada-Urquijo¹, James Valencia-Ortiz², Maria Fernanda Velandia-Beltrán³, John Brayan Mendoza-Calderón⁴

Resumen - En el presente artículo se realiza un análisis profundo respecto a la historia de DES y su sucesor Triple DES en el mercado de la seguridad y el cifrado de datos de manera segura. Se estudian las diferentes variaciones y mejoras que se han propuesto en materia investigativa en relación con los usos de Triple DES desde antes de ser aprobado como un estándar para el cifrado de datos a nivel mundial. De igual manera es importante mencionar que las propuestas recolectadas y analizadas son de diferentes partes del mundo lo que solidifica el nivel de investigación realizado, debido a la variedad de fuentes encontradas.

De esta manera se realiza un recorrido por la historia de este algoritmo para ofrecer al lector una amplia perspectiva respecto al funcionamiento y diferentes usos que se le han dado.

Finalmente, se logra determinar que DES y 3-DES han sido algoritmos ampliamente utilizados en el área de la seguridad informática, pero actualmente son vulnerables a diferentes ataques como fuerza bruta y criptoanálisis diferencial, debido a esto se propone el uso de otro algoritmo como AES o realizar mejoras en la implementación de DES y 3-DES.

Palabras clave: DES, Triple DES, encriptación, historia, evolución, propuestas de mejoras, variaciones de DES y 3DES.

Abstract - This paper provides an in-depth analysis of the history of DES and its successor Triple DES in the security market and secure data encryption. The different variations and improvements that have been proposed in research related to the uses of Triple DES since before it was approved as a standard for data encryption worldwide are studied. It is also important to mention that the proposals collected and analyzed are from different parts of the world, which solidifies the level of research carried out, due to the variety of sources found.

In this way, the history of this algorithm is traced in order to provide the reader with a broad perspective on how it works and the different uses that have been made of it.

Finally, it's determined that DES and 3-DES have been algorithms widely used in security information systems, but currently they are vulnerable to different attacks such as brute force and differential cryptanalysis, because of this it is suggested the use of other algorithms, for instance AES, or to include improvements in the DES and 3-DES implementation.

¹ Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

² Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

³ Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

⁴ Ingeniería en Telemática, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Keywords: DES, Triple DES, encryption, history, evolution, proposed improvements, variations of DES and 3DES.

1. Introducción

Desde el año 1976 el algoritmo de cifrado Data Encryption Standard - DES fue definido como un estándar FIPS (Federal Information Processing Standards) en los Estados Unidos de América. Y el año siguiente en 1977 fue publicado como FIPS PUB 46. Desde ese momento su uso se propagó por todo el mundo como un método para cifrar información y mantenerla segura durante los procesos de comunicación en diferentes actividades o transacciones. A pesar de ello desde sus inicios fue refutado con el argumento de hacer uso de una clave de cifrado demasiado corta, lo que implicaría una vulnerabilidad potencial.

Después de alrededor de 20 años funcionando como unos de los estándares más robustos y utilizados para el cifrado de información, en la década de 1990 se intensificaron los intentos por quebrar y vulnerar la seguridad de DES, ante lo cual los investigadores aumentaron sus esfuerzos por proponer alternativas para el cifrado de datos evitando que la información importante y sensible fuera violada. Fue en el año 1998 cuando las predicciones se hicieron realidad y el algoritmo DES con su clave de 56 bits fue roto mediante técnicas de búsqueda exhaustiva de clave. Allí surgió la necesidad de establecer 3DES como una variación de DES que brindaba una seguridad mayor y más robusta. Frente a las diferentes propuestas realizadas por científicos e investigadores, se eligió 3DES por la gran aceptación y seguridad que tenía DES. Siguiendo su línea y su legado, 3DES hacía uso de un proceso similar, pero con un sistema de tres claves lo que aumentaba la complejidad de vulnerar el algoritmo. Triple DES consiste en replicar el algoritmo DES, tres veces haciendo uso de claves diferentes en cada uno de los pasos.

Este último algoritmo se ha mantenido estable desde esa fecha y ha competido en el mercado con otros algoritmos muy robustos como AES, Blowfish, Twofish y algunos otros, demostrando su robustez y alta aceptación. Es por ello que la documentación de la que se trata el siguiente apartado de este artículo, consiste en exponer diferentes análisis, estudios y propuestas que se han realizado en todo el mundo a lo largo de los años, entorno a estos dos algoritmos, especialmente, con base en 3DES cuya seguridad y complejidad es mucho mayor, y que aún es considerado un estándar avalado para el cifrado de datos.

2. DES y Triple DES

2.1. Un modo propuesto para el cifrado triple-DES

En el inicio de este recorrido se escogió un artículo publicado en el año 1996 por IBM Journal of Research and Development en [1]. Allí los autores Coppersmith, Johnson y Matyas proponen incluir una operación al algoritmo 3DES, en la cual, para cada uno de los 3 pasos de encriptación, se introducen valores secretos de enmascaramiento que finalmente se combinan con las salidas generadas en cada uno de los pasos antes de ingresar al siguiente. De esta manera se agrega un nivel de seguridad mayor al propuesto por DES y 3DES.

Esta propuesta se dio respecto a la necesidad de reemplazar el algoritmo DES, que hasta ese momento aún se encontraba vigente y avalado por NIST, pero con la latente posibilidad de ser vulnerado por su corta clave de 56 bits, especialmente por los ataques basados en la búsqueda exhaustiva de claves. Partiendo de allí ya se encontraba propuesto 3DES, sin embargo, sin aval para ser tratado como un algoritmo de encriptación oficial. Es por ello por lo que 3DES sirvió como base para la investigación y propuesta realizada por los autores en [1].

A pesar de la solidez encontrada en esta investigación, se llegó a la conclusión de que el nivel de complejidad agregado en esta variante del algoritmo 3DES es demasiado alto. Lo anterior implicaría un nivel de procesamiento mucho mayor en cada uso que se diera al algoritmo y por ello no fue seleccionado como sucesor de DES en el año 1998.

2.2.El algoritmo DES mejorado

En el año 1996, Seung-Jo Han, Heang-Soo Oh y Jongan Park proponen en [2] una mejora para el algoritmo DES, dado a que observaron que con el incremento de la capacidad de procesamiento del hardware existía una potencial brecha de seguridad al poder vulnerar la seguridad del algoritmo DES con métodos de criptoanálisis diferencial.

En el diseño del algoritmo Improved-DES se incluye lo siguiente: El texto plano que ingresa es de 96 bits, el cual se divide en 3 bloques de 32 bits, los cuales se irán operando de a parejas en cada ronda, y se van rotando de forma que en cada ronda se intercambian las parejas, tal como lo muestra el diagrama de la figura 1.

Las S-Boxes usadas en las funciones de cada ronda se amplían a 16.

En cada ronda se utilizarán dos funciones, una aplicada para el lado izquierdo y otra para el derecho, como se observa en la figura 1.

Con estos cambios realizados, realizan una serie de pruebas en las cuales miden el efecto avalancha del algoritmo con la medición de la correlación entre los bits de entrada y salida y la dispersión de los bits de salida al modificar un bit de entrada. Esta medición la hacen para cada una de las S-Box tanto del algoritmo DES como del propuesto Improved-DES.

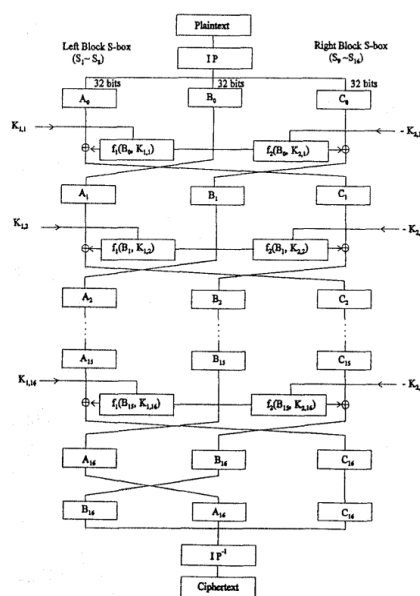


Figura 1. Algoritmo del modelo Improved-DES. [1]

Finalmente, los autores concluyen, que al haber agregado 8 S-Boxes, para un total de 16, y al crear los 3 bloques de información que utilizan 2 funciones diferentes en cada ronda, se logró obtener un algoritmo con una mayor robustez y un mejor efecto avalancha, que permite que la cantidad de datos para realizar un ataque de criptografía diferencial suba al valor de $2^{62.96}$ a diferencia de los 2^{47} del algoritmo DES convencional, lo cual lo hace mucho más difícil de vulnerar.

2.3.Reducción de la búsqueda exhaustiva de claves del estándar de cifrado de datos (DES)

Posteriormente en [4] cuya investigación fue publicada en el año 2007 por la revista Computer Standards & Interfaces, se analiza la vulnerabilidad hallada en DES en años anteriores. En este artículo, Raphael Phan de Swinburne University of Technology, plantea una optimización en los procesos de explotación del algoritmo DES mediante la búsqueda exhaustiva de claves.

El análisis realizado por el autor, se elaboró con base en la alta usabilidad que tenía el algoritmo DES en el mercado, aún existiendo otras posibilidades como 3DES y AES. A partir de allí y teniendo como punto de referencia la vulnerabilidad hallada en DES. El autor propone que hasta el momento en el que él inicia su investigación la debilidad explotada de DES solo era una, cuya fuente era la búsqueda exhaustiva de claves, y que está, aún requería una gran capacidad de procesamiento computacional para que pudiera ser efectiva, y quebrar la seguridad del algoritmo, y aun así tardaba bastante tiempo, alrededor de 24 horas.

Teniendo en cuenta este análisis realizado, el autor propone una solución con la que se pueden explotar las debilidades de DES, disminuyendo el tiempo y la capacidad de procesamiento requeridos, así se mejora el rendimiento de la búsqueda exhaustiva de claves en DES.

Para la propuesta realizada, el autor hizo uso de técnicas matemáticas mediante las cuales se optimizó el algoritmo de búsqueda exhaustiva de claves, haciendo uso de las llaves de paridad de DES. Con este hallazgo se concluyó que los procesos de explotación de vulnerabilidades del algoritmo DES se podrían optimizar. De esta manera el autor ratifica la necesidad de remover el algoritmo DES del mercado y usar su sucesores o variantes como 3DES y AES.

De acuerdo con los planteamientos e intenciones del autor, ratificamos los esfuerzos realizados, teniendo en cuenta que a pesar de que se hubieran encontrado debilidades en el algoritmo DES, en ese momento aún era usado en muchas partes del mundo como estándar para el cifrado de datos. De esta manera el autor contribuyó al proceso de migración del algoritmo DES a 3DES y AES, cuya seguridad era mucho más robusta, y daba un mayor nivel de seguridad frente a la protección de información en diferentes ámbitos.

2.4.Implementación y Análisis de AES, DES y Triple DES sobre Red GSM

Ya en el año 2010 fue publicado [5] por Majithia Sachin y Dinesh Kumar en el Departamento de Tecnología de la Información, DAVIET, Jalandhar en el marco de la Revista internacional de informática y seguridad de redes. En donde se propone un cifrado adicional para la tecnología GSM (Sistema Global para Comunicaciones Móviles) mediante la implementación de algoritmos como AES, DES y 3DES ya que los algoritmos criptográficos que se utilizan allí

ya han estado expuestos a ataques y han sido descifrados previamente. Entonces con ese cifrado adicional es que se pretende garantizar la confidencialidad suficiente.

Ellos comparan el cambio en el rendimiento de la seguridad mediante el uso de diferentes longitudes de clave para los algoritmos de cifrado. Los gráficos se trazan entre los tiempos necesarios para encontrar la clave correcta y se juega con diferentes longitudes de clave. Seguido de esto se presentan algunos escenarios en donde se aumenta la longitud de la clave como se puede evidenciar en las figuras 2, 3 y 4.

Aunque en el artículo referencia se toman más muestras aumentando en número de bits, con lo anterior se puede evidenciar claramente que AES supera a sus contrincantes en todos los escenarios, y mientras mayor sea la longitud de clave mayor será la distancia de diferencia en segundos con respecto a DES y 3DES. También se analiza la efectividad de los algoritmos mencionados contra ataques de fuerza bruta implementados en un entorno de desarrollo como MATLAB Y JAVA, y como resultado allí se concluye que AES les proporcionó una mejor seguridad contra estos ataques, Entonces se concluye proponerlo como un algoritmo de cifrado estándar para GSM.

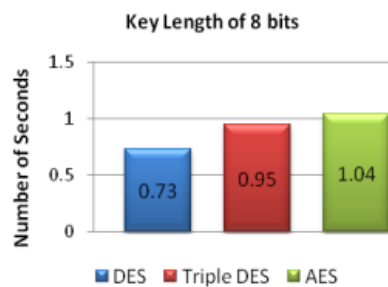


Figura 2: Número de segundos necesarios con una longitud de clave de 8 bits.[5]

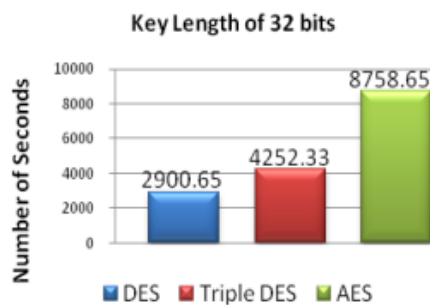


Figura 3: Número de segundos necesarios con una longitud de clave de 32 bits.[5]

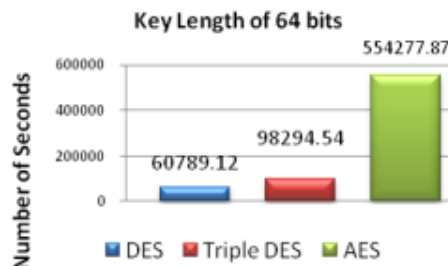


Figura 4: Número de segundos necesarios con una longitud de clave de 64 bits.[5]

2.5.Implementación y análisis de varios criptosistemas simétricos

Seguimos en el año 2010 donde fue publicado [6] Himani Agrawal y Monisha Sharma en la Revista india de ciencia y tecnología en donde se implementa los algoritmos de cifrado simétrico DES y el estándar de cifrado de datos triple 3DES, también, el estándar de cifrado avanzado AES, BLOWFISH y RC4 en el software MATLAB y son comparados en algunos puntos.

Estos puntos son el efecto de avalancha debido a la variación de un bit en el texto sin formato que mantiene constante la clave, el efecto de avalancha debido a la variación de un bit en la clave que mantiene constante el texto sin formato, la memoria requerida para la implementación y el tiempo de simulación requerido para diferentes longitudes de mensaje.

Con lo anterior se logra identificar que en 3DES, la memoria requerida para la implementación es la más alta, lo que significa que es el algoritmo más lento. Este es el principal inconveniente de 3DES. Varias aplicaciones basadas en Internet han adoptado triple DES. Pero debido a varios inconvenientes, no es un candidato razonable para el uso a largo plazo.

También se logra deducir que en AES el efecto de avalancha es más alto. AES está siendo considerado como un reemplazo para DES. AES es ideal para cifrar mensajes enviados entre objetos a través de canales de chat y es útil para objetos que forman parte de un juego o cualquier cosa que implique transacciones monetarias.

2.6.Implementación 3DES basado en FPGA

Seguimos en el año 2010 donde fue publicado [7] por Fang Ren, Leihua Chen, y Tao Zhang en el marco de la revista internacional de informática y seguridad de redes del Centro de Servicios de Ciencia y Tecnología Meteorológica Servicio Meteorológico de Shanxi, China. Donde el escrito nos expone que los algoritmos de cifrado de bloques como DES, 3DES y AES se pueden realizar tanto como en software y en hardware, estos cifrados de software cumple la función de cifrado al hacer circular el software de cifrado en un equipo.

Además de ocupar recursos del host, el artículo también menciona que los cifrados de software se computan más lento y tienen menor seguridad que los cifrados de hardware, y que en algunas ocasiones exige una transmisión de datos de alta velocidad.

El cifrado de hardware cumple la función de cifrado mediante un dispositivo de cifrado de hardware que es independiente del sistema del equipo, y toda la memoria y el cálculo de los datos clave se realizan internamente por hardware, no ocupa recursos del host, computa más rápido, tiene mayor seguridad, estabilidad y compatibilidad. 3DES garantiza su seguridad al mejorar la complejidad del algoritmo mientras mantiene el sistema original sin grandes modificaciones porque se basa en el algoritmo DES en la capa base. Pero el defecto básico es la lentitud del cifrado de software, que a menudo implica operaciones de bits como transposición, cambio de posición, OR exclusivo, etc.

2.7. Cifrado y descifrado de datos mediante triple DES y análisis de rendimiento del sistema criptográfico

En el año 2014 fue publicado [8] por International Journal of Scientific Engineering and Research (IJSER), este artículo fue escrito por Karthik y Muruganandam. Aquí observamos un proceso de investigación comparativo el cuál tiene como objetivo exponer una técnica creada para el cifrado de un mensaje secreto por medio de un cifrado de bloques con base en dos algoritmos criptográficos, la cual es denominada comunicación secreta expuesta. Para la investigación realizada, los autores hacen uso de los cinco objetivos de la criptografía que permiten mantener el secreto protegido, es decir:

Autenticación: Siempre se debe validar y verificar la identidad del receptor y del emisor.

Secreto o confidencialidad: La no revelación de información a personas no autorizadas.

Integridad: La información no sufre modificación ni por el emisor ni por el receptor.

No repudio: ni el emisor ni el receptor pueden negar falsamente que hayan enviado un determinado mensaje.

Fiabilidad y disponibilidad del servicio: En cualquier instante de tiempo se puede tener acceso a la información.

Los autores desarrollaron un software haciendo uso del framework .NET llamado Cryptograph.NET. Mediante este sistema se realiza un análisis previo sobre el rendimiento de diferentes algoritmos. Adicionalmente, los autores hacen uso de resultados obtenidos en fuentes de información externas para complementar su investigación. A partir del proceso analítico realizado a los algoritmos; DES, 3DES, AES, Rijndael, BF y Blowfish, fue posible concluir que AES supera a sus homólogos en dos frentes; el número de solicitudes procesadas por segundo y el tiempo de respuesta de diferentes solicitudes de usuario. De igual manera, se concluye que Blowfish ofrece un rendimiento óptimo respecto a sus competidores. Y finalmente que el rendimiento de 3DES mejora con Modo de Libro de Códigos Electrónica (ECB) y Encadenamiento de Bloques de Cifrado (CBC) respecto a otros algoritmos.

En el marco de la investigación realizada, es importante recalcar su relevancia en los diferentes mercados internacionales que hacen uso de estos algoritmos en sus procesos. Lo anterior debido a la comparación expuesta en el documento, la cual permite al lector obtener sus propias conclusiones frente al funcionamiento de los diferentes algoritmos que operan alrededor del mundo, y seleccionar el de su preferencia teniendo en cuenta todas las características analizadas.

2.8.El diseño e implementación de un algoritmo de cifrado simétrico basado en DES

También en el año 2014 fue publicado [9] por LI Yongzhen y Zhou Ying bing en el marco del Departamento de Informática y Tecnología de la universidad de Yanbian, y aquí el artículo ratifica que DES ha mantenido su posición dominante en el área del cifrado de datos durante las últimas décadas. Sin embargo, en el campo del hardware informático ya ha demostrado ser inseguro. Lleva poco tiempo traducir el texto cifrado a su texto sin formato correspondiente utilizando el método de fuerza bruta a un costo razonable. Esto se debe principalmente al pequeño tamaño de clave DES empleada.

Ante estos problemas, el objetivo de este artículo es sugerir una alternativa en DES para obtener mayor seguridad y mejor eficiencia de ejecución aumentando el tamaño de la clave y actualizando la técnica de iteración. Se realizaron comparaciones con DES y 3DES. Los resultados han demostrado que el algoritmo propuesto supera a los dos algoritmos anteriores. Este documento analizó la debilidad existente en DES y propuso dos nuevos métodos que operaron simultáneamente con dos procesos DES únicos. El primer método intercambió los resultados de la ronda, lo que agregó confusión al texto cifrado; el segundo método alternó la subclave entre las dos partes para obtener el efecto de emplear una longitud de clave duplicada (112 bits) para cifrar un bloque de 64 bits.

Los resultados de la simulación indicaron que, en términos de eficiencia operativa, los nuevos métodos superaron claramente a 3DES y se mantuvieron al mismo nivel que DES. Con respecto a la seguridad, los nuevos métodos proporcionan un rendimiento más seguro que DES y al menos tan seguro como 3DES.

2.9. Análisis de rendimiento de DES+9 y Triple DES

Ya en el año 2015 fue publicado [10] en el marco de la Revista internacional de aplicaciones informáticas en la Facultad de Ingeniería de la Universidad de Kakinada por el Dr. O. Srinivasa Rao. En el cual se analizan los algoritmos DES y 3DES como algoritmos de cifrado simétrico altamente utilizados comparándolos en términos de cálculo de tiempo de cifrado y descifrado de datos.

En primera instancia de DES explica que se definen dos entradas para la función de cifrado como lo son el texto sin formato que se va a cifrar y la clave respectiva, para lo cual el texto sin formato debe tener una longitud de 64 bits y la clave debe tener una longitud de 56 bits. Como se puede apreciar en la figura 5.

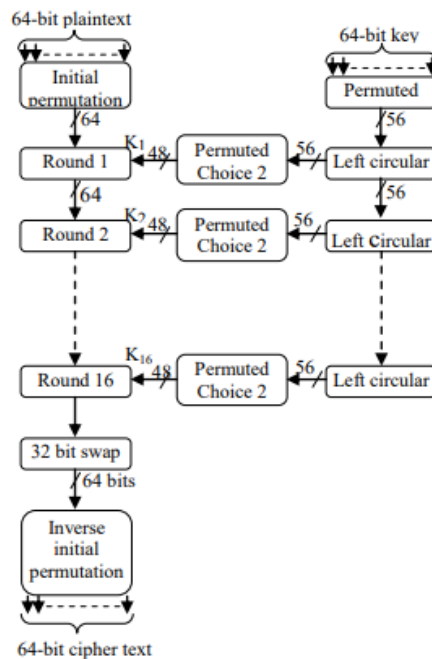


Figura 5: Representación general del funcionamiento del algoritmo DES. [10]

En el lado izquierdo de la figura, podemos ver que el procesamiento del texto sin formato se desarrolla en tres fases. Primero, el texto sin formato de 64 bits pasa a través de una permutación inicial (IP) que reorganiza los bits para producir la entrada permutada. A esto le sigue una fase que consta de dieciséis rondas de la misma función, que involucra tanto funciones de permutación como de sustitución. La salida de la última ronda (decimosexta) consta de 64 bits que son una función del texto sin formato de entrada y la clave. Las mitades izquierda y derecha de la salida se intercambian para producir la salida previa. Finalmente, la salida previa se pasa a través de una permutación que es la inversa de la función de permutación inicial, para producir el texto cifrado de 64 bits. De esta manera se expone cómo funciona el algoritmo hasta este entonces.

Luego con lo que compete a 3DES dice que se desarrolló para abordar las fallas en DES sin diseñar un criptosistema completamente nuevo. DES como ya sabemos, utiliza una clave de 56 bits y no se considera suficiente para cifrar datos confidenciales. 3DES simplemente amplía el tamaño de la clave de DES aplicando el algoritmo tres veces seguidas con tres claves diferentes, como se puede evidenciar en la figura 6.

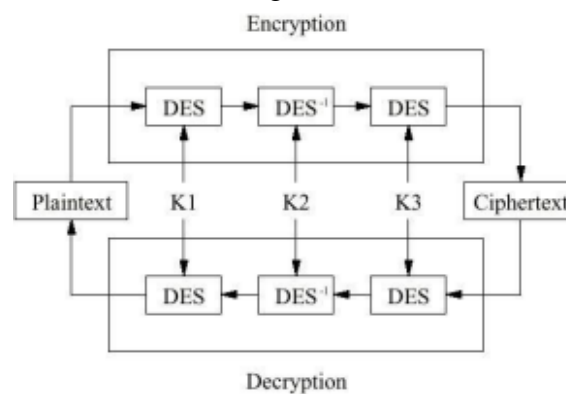


Figura 6. Representación general del funcionamiento del algoritmo DES. [10]

Al final se concluye que el algoritmo 3DES resulta ser el más eficiente en términos de efecto avalancha, aunque consume más recursos, y en los dos algoritmos el tiempo de cifrado resulta ser mayor al tiempo de descifrado.

3. Una evaluación exhaustiva de los algoritmos criptográficos: DES, 3DES, AES, RSA y Blowfish

Siguiendo la línea comparativa en el año 2015 fue publicado [11] por Procedia Computer Science, cuyos autores son Priyadarshini, Prashant, Narayan y Meena. En esta investigación los autores exponen la necesidad del público de escoger un algoritmo criptográfico que sea de bajo coste y alto rendimiento. Al ser dos características difíciles de combinar, se someten los algoritmos; DES, 3DES, AES, RSA y Blowfish a pruebas exhaustivas que permitan presentar una comparación mostrando fortalezas y debilidades de cada uno, de tal manera que el público pueda escoger con mayor certeza el algoritmo que desea usar según sus necesidades.

Para ello, primero es importante definir cada uno de los algoritmos que fueron usados en esta investigación, esta definición se puede encontrar en la tabla 1.

Algoritmo	Definición
DES	<p>El Estándar de Cifrado de Datos es un cifrado de bloques de clave simétrica. El DES fue creado en 1972 por IBM utilizando el algoritmo de encriptación de datos. Fue adoptado por el gobierno de Estados Unidos como algoritmo de cifrado estándar. Es vulnerable a los ataques de clave cuando se utiliza una clave débil.</p>
3DES	<p>Algoritmo de Cifrado de Datos Triple, que es un cifrado de bloques. El estándar de cifrado de datos triple se publicó por primera vez en 1998 y recibe su nombre porque aplica el cifrado DES tres veces a cada bloque de datos, cifrado - descifrado - cifrado utilizando DES.</p>
AES	<p>El algoritmo Advance Encryption Standard fue desarrollado en 1998 por Joan Daemen y Vincent Rijmen, este algoritmo permite una combinación de longitud de datos y clave de 128, 192 y 256 bits. Este algoritmo es cifrado por bloques de clave simétrica.</p>
Blowfish	<p>Blowfish es un cifrado simétrico por bloques que puede utilizarse como sustituto informal de DES o IDEA. Blowfish fue diseñado por Bruce Schneier como una alternativa rápida y gratuita a los algoritmos de cifrado existentes.</p>
RSA	<p>RSA fue creado en 1977, es un algoritmo de clave pública y tiene un tamaño de clave de 1024 a 4096 bits. Consta de tres pasos: el primero es la generación de clave para cifrar y describirá, el segundo es donde se cifra el mensaje y el tercero es el descifrado.</p>

Tabla 1. Definición de diferentes algoritmos de cifrado.

En el artículo se desarrolla un software en lenguaje Java con el IDE eclipse, y específicamente los paquetes Crypto y Java Security. Los aspectos usados para la comparación fueron: tiempo de cifrado, tiempo descifrado, memoria en uso, efecto avalancha, entropía y número de bits requeridos para codificar de manera óptima. Así los autores ofrecen una comparativa al lector en la que muestran cuales son las fortalezas y debilidades de cada algoritmo, permitiendo al lector seleccionar el que mejor se acopla a sus necesidades.

3.1.Implementación de alto rendimiento del algoritmo DES en FPGA

Debido a la corta longitud de llave y de bloque de texto plano del algoritmo DES, que permite un uso de memoria bajo, en el año 2015 Murtada. M. Abdelwahab propone un algoritmo DES simplificado en [13] para aplicar a tarjetas programables FPGA.

Para realizar esto, el autor señala que se hace uso de solamente una ronda para encriptar el mensaje, y la encriptación se realiza mediante una operación XOR entre el texto y la llave. El algoritmo de encriptación es el siguiente:

- Generar una llave de 64 bits y dividirla en dos mitades de 32 bits mediante una permutación.
- La mitad izquierda sufre una rotación de bits a la izquierda una posición.
- La mitad derecha sufre una rotación de bits a la derecha una posición.
- Mediante otra permutación se juntan las mitades para tener una llave de 64 bits nuevamente.
- El texto a cifrar ingresa como una cadena de 64 bits.
- El texto se divide en dos mitades de 32 bits.
- Cada mitad del texto se opera con la llave mediante una operación XOR.
- Cada mitad cifrada se une para tener el texto cifrado completo de 64 bits.
- El texto cifrado se pasa a través de una operación de permutación y combinación final para entregar el resultado.

El autor concluye que con el diseño propuesto fue posible tener un rendimiento de 278.282 Mbps, lo cual es un rendimiento competitivo teniendo en cuenta otras implementaciones de DES enfocadas a su uso en tarjetas FPGA.

3.2.Implementación CUDA del algoritmo DES para plataformas ligeras

En el año 2017 se publicó [14] en la revista ACM International Conference Proceeding. El autor, haciendo referencia al nacimiento del internet de las cosas, propone como alternativa de seguridad, implementar DES en el procesador CUDA, que, a su vez, aprovecha la potencia de las GPUs. Él explica que las GPUs tiene mayor accesibilidad gracias a que utiliza arquitectura SIMD para ejecutar múltiples hilos a la vez, los mismos que facilitan la entrada al registro, memoria local, memoria compartida y memoria global, que además, tienen gran potencia para realizar cálculos y, por ende, las aplicaciones ejecutadas funcionan con mayor velocidad. El autor sostiene que, al implementar DES en CUDA, las tablas y contraseña se definen en la zona de memoria y aumenta el rendimiento porque es posible acceder a los datos con eficiencia y recuperarlos del caché a gran velocidad. El único inconveniente, señala el autor, resulta cuando los hilos del bloque son menores de 32 porque el Warp no funciona correctamente, en otras palabras, la propuesta es útil para procesar gran cantidad de datos al mismo tiempo.

3.3.Análisis de los mecanismos de encriptación para la seguridad de la información en redes de comunicaciones

En el mismo año, la revista SATHIRI publicó [15]. En este artículo, los autores realizan una comparativa profunda entre diferentes algoritmos de encriptación de datos. Para ello,

recurrieron a varias herramientas de código abierto como OpenSSL, TrueCrypt y DiskCryptor para analizar la velocidad del proceso cifrado-descifrado a través de un benchmark cambiando el tamaño del bloque y de la clave. En OpenSSL se puso a prueba los algoritmos RC4, DES, IDEA, AES y Blowfish en cuanto a velocidad en dos modos de operación CBC y IGE, en TrueCrypt y DiskCryptor se evaluaron los algoritmos AES, Twofish y Serpent.

Se demostró que en cuanto a velocidad se refiere, RC4 es la mejor opción, pero es muy vulnerable a ataques y poco práctico. Respecto a robustez, AES es muy seguro a pesar de su vulnerabilidad porque “secret” funciona con una longitud de clave de 128 bits; y, “Top Secret”, con claves de 192 o 256 bits; en el análisis del rendimiento y tamaño de la clave resulta más eficiente ECC en los dos parámetros; en el tamaño de textos encriptados y tiempo necesario para romper la clave, ganó ECC que ocupa menos ancho de banda porque su tamaño del texto es inferior; y por último, midiendo la complejidad ciclomática, RSA es más compleja en el cifrado y descifrado.

3.4. Modelo de seguridad en computación Cloud combinando el algoritmo DES y Bit Menos Significativo (LSB)

Para el año 2018 ya era conocido el hecho de que el algoritmo DES podía ser vulnerable a ataques como Man In The Middle o Fuerza Bruta, es por esto que M Basri, H Mawengkang y E M Zamzami proponen en [16] un anillo de seguridad adicional haciendo uso de la esteganografía, de esta forma se hace uso de una imagen para ocultar el mensaje encriptado.

El método de encriptación DES toma segmentos de 64 bits del mensaje y mediante una llave de 64 bits genera segmentos encriptados de 64 bits. En este proceso se crean 8 bloques cifrados que al final se unen en uno solo de 64 bits, en este punto el último bloque de 8 bits será el que se ocultará en la imagen mediante el algoritmo LSB.

Para poder ocultar el mensaje en la imagen, se hace uso del hecho de que para representar una imagen, cada pixel se representa mediante 3 grupos de 8 bits, para cada color base Rojo, Verde y Azul (RGB), de esta forma se usará el bit menos significativo de cada color para ir ocultando el mensaje encriptado.

De esta forma, para descifrar se haría el proceso inverso en el cual se buscan los bits menos significativos de cada color de la imagen para ir recopilando el mensaje encriptado y en seguida se sigue el proceso de descifrición DES usual.

Este artículo demuestra la necesidad de mejorar los mecanismos de seguridad del algoritmo DES y la latente preocupación por ser víctima de ataques informáticos que violen su seguridad.

3.5. Triple DES: Preservación de la privacidad en la salud con Big Data

En el año 2018 fue publicado [17] por Science+Business Media. Allí vemos una profundización en materia de 3DES en el sector de la salud y con técnicas de Big Data para la recolección de información. Se observa en esta investigación como los autores usan 3DES para preservar la privacidad de la información recolectada.

Los autores realizan un detallado análisis de la actualidad de las técnicas de Big Data utilizadas en el sector de la salud y la medicina, en donde la mayor conclusión es la falencia en cuanto a seguridad de la información recolectada.

En el artículo se propone una solución alternativa que hace uso de 3DES, sin embargo, con una pequeña variación que involucra la anonimización en el proceso de cifrado que desarrolla 3DES, y este nuevo algoritmo denominado A3DES es aplicado a los procesos de recolección de información mediante técnicas de Big Data en temas relacionados con salud y medicina.

3.6.Un enfoque de seguridad para el sistema de gestión de archivos mediante el cifrado de datos algoritmo estándar (DES)

En el 2019, los autores presentaron [20] en la International Journal of Advanced Trends in Computer Science and Engineering. En esta publicación, los autores analizaron el funcionamiento de DES y su relación con el ciclo de vida del sistema, específicamente, el rápido desarrollo de aplicaciones respecto a la recopilación de datos, análisis de costes, requisitos, identificación de los métodos usados en diseños, pruebas, despliegue y mantenimiento del sistema. Los autores, recogieron los resultados derivados del análisis experimental de pruebas en componentes de hardware y software y unidades del sistema de integración y aceptación. Resaltó la eficacia de DES en su época en cuanto a complejidad y latencia temporal en conectividad de red, sistema y servidores físicos y web se refiere. Es seguro en todos los parámetros evaluados pero los autores sugieren que el uso de un sistema de archivos basado en la informática de gestión es necesario para evitar pérdidas en la información.

3.7.Algoritmo DES modificado para mejorar el rendimiento ante errores y mejorar la seguridad para entornos inalámbricos

La comunicación inalámbrica se ha extendido bastante con los avances en las redes de telecomunicación, al ser un canal abierto puede ser susceptible a ataques informáticos. Los algoritmos de encriptación como DES se basan en el efecto avalancha, el cual produce que al tener un solo cambio en un bit del texto plano produce un gran cambio en el texto cifrado y viceversa, de esta forma se evita tener una correlación obvia entre los textos planos y cifrados. El efecto avalancha es deseable en los algoritmos de encriptación simétricos, pero al estar en una comunicación inalámbrica en la cual pueden haber fallos por ruidos y esto provocaría que al descifrar la información el mensaje no esté correcto.

Los autores en [21] proponen un algoritmo DES Modificado (M-DES) en el cual se plantea reducir el efecto avalancha y mejorar la seguridad para ser usado en transmisión de información por medios inalámbricos. La propuesta consta de cambiar las S-Boxes y agregar una ronda adicional al algoritmo. La arquitectura se muestra en la figura 7.

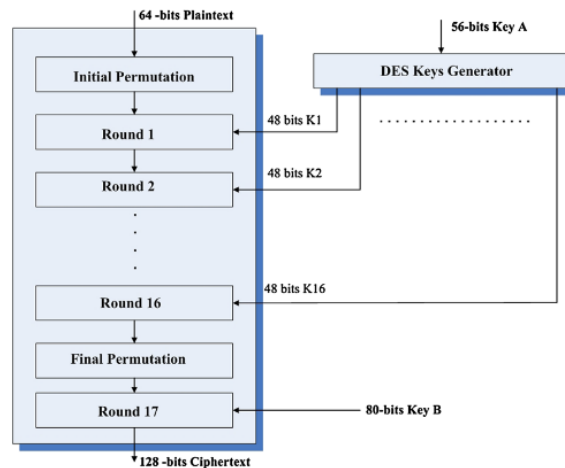


Figura 7. Arquitectura algoritmo M-DES. [21]

Los autores realizan principalmente dos cambios al algoritmo DES: el primero, consiste en que las S-Boxes uno a cuatro, tendrán la tabla de mapeo de la primera S-Box de DES, y las S-Boxes cinco a ocho tendrán la tabla de mapeo de la segunda S-Box de DES. En el algoritmo DES Original cada S-Box tiene un mapa diferente, en M-DES son solo 2 tablas de mapeo; el segundo cambio consiste en agregar una ronda 17 al final del algoritmo, la cual recibe la salida encriptada de las 16 rondas y la permutación final, junto con una llave de 80 bits, que permitirá convertir la salida de 64 bits en una salida de 128 bits.

Con el nuevo algoritmo prueban el Bit Error Rate (BER) mostrando que es mucho menor que DES, asimismo realizan pruebas de seguridad, demostrando que para un ataque de fuerza bruta es necesario 2^{136} intentos, mientras que para un ataque de criptoanálisis diferencial serían necesarios 2^{47} parejas de datos.

Esta información permite concluir que el algoritmo DES Modificado (M-DES) propuesto brinda un mejor comportamiento en ambiente de comunicación inalámbrica, puesto que disminuye el efecto avalancha dando una mayor robustez frente a los posibles errores de pérdida de bits y además mejora la seguridad del algoritmo original, haciendo casi imposible con los recursos actuales en computación de ser descifrado.

3.8. Implementación de la lotería de IoT en el estándar de cifrado de datos

En 2020, la International Journal of Scientific Engineering and Research presentó al público [24]. En este artículo, los autores hacen un estudio respecto a los dispositivos IoT para vulnerar la seguridad del DES dado su uso como herramientas de ataque. Presentan resultados de Brute-force attack contra DES demostrando que un cluster de 200 dispositivos IoT es capaz de encontrar la clave en una media de 350 segundos y un cluster de 2000 dispositivos IoT lograr encontrar la clave en 0,015 segundos. Para llegar a tales resultados, se realizó una prueba llamada IoT Lotto que consiste en sincronizar todos los dispositivos IoT para que trabajen en paralelo con comunicación rápida entre módulos y usando la arquitectura de computación distribuida en la delegación de subtarea a cada dispositivo IoT participante, el resultado: un ataque contundente y rápido al DES. Entre más dispositivos IoT más eficiente es, lo suficientemente bueno como para vulnerar AES Y Triple DES. Así como avanzan, se solidifican y robustecen los algoritmos de encriptación, así mismo, los ataques cibernéticos también evolucionan. Entre más información sensible y confidencial haya en internet, más probabilidades hay de que sea robada la información, pues resulta valiosa para los hackers.

3.9. Una optimización eficiente y segura del algoritmo 3-DES usando un algoritmo mejorado de creación de llaves

Para el año 2020 se conocía que el algoritmo 3-DES tenía potenciales fallos de seguridad, debido a que la clave de 192 bits que se dividía en 3 de 64 bits podían ser atacadas mediante fuerza bruta. Es por esto que Akshitha Vuppala, R Sai Roshan, Shaik Nawaz y JVR Ravindra en [25] publican el algoritmo FORTIS mediante el cual se refuerza el método para la generación de llaves.

El algoritmo consiste en lo siguiente, la llave principal de 64 bits es entregada al Permuted Choice 1, el cual la convierte en una llave de 56 bits truncando 8 bits de paridad, luego la divide en dos partes de 28 bits cada una, denominadas C y D. La parte C se mantiene sin modificaciones, pero la parte D se modifica mediante el Comparator, el cual compara C y D bit a bit, si ambos bits son iguales asigna un cero lógico y si son distintos asigna un 1 lógico, de esta forma se crea la llave denominada X. Luego de esto, la parte C ingresa al Versatile Right Shifter y la parte X ingresa al Versatile Left Shifter.

Cada uno de estos shifter lo que busca es realizar una rotación circular a izquierda o derecha según el shifter elegido. Para realizar esta rotación se basa en los bits lógicos de X, si es un cero se mueve una posición, y si es un 1 se mueve dos posiciones. En la figura 8 se muestra el pseudocódigo propuesto por los autores.

Los autores realizaron simulaciones mediante las cuales graficaban las trazas de potencia del algoritmo, allí se puede evidenciar picos en los momentos en los cuales el algoritmo debe realizar operaciones costosas a nivel de computación, lo cual, según el artículo puede ser de utilidad para un atacante al momento de deducir las llaves de la encriptación. En dichas gráficas se mostraba que usando el algoritmo FORTIS eran menos notorios los picos de potencia en comparación con el algoritmo Triple-DES convencional.

Algorithm 1 FORTIS Algorithm

```
Let number of inputs be [0:63]
The 64 bits are reduced to 56 bits by removing the 8 parity bits
56 bits are divided into blocks C and D
C is directly taken as input of versatile right shifter
while bits ≤ 27 do
  if C[bits] = D[bits] then
    X[bits]=0
  else
    X[bits]=1
  end if
end while
The 28 bits of X are given as inputs to versatile left shifter
if C[0] = 0 then
  Bits of C are shifted towards right by one position
else
  if C[0] = 1 then
    Bits of C are shifted towards right by two positions.
  end if
end if
if X[0] = 0 then
  Bits of X are shifted towards left by one position
else
  if X[0] = 1 then
    Bits of X are shifted towards left by two positions.
  end if
end if
The two blocks are concatenated and given as inputs to PC-2
PC-2 reduces 56 bits to 48 bits
The process is repeated for 16 rounds to generate 16 sub keys.
```

Figura 8. Pseudocódigo del algoritmo FORTIS. [25]

Por otro lado, realizaron el cálculo de la probabilidad de acierto entrópica (Probability of Guessing Entropy), la cual significa la cantidad de intentos promedio para adivinar un valor de una llave. En dicho cálculo los autores muestran que en cerca del 86.6% de las muestras la probabilidad fue menor para el algoritmo FORTIS en comparación con Triple-DES convencional.

De esta forma, el artículo concluye que la implementación del Comparator y los Versatile Shifters generan una mayor complejidad para los atacantes al momento de vulnerar las llaves del algoritmo Triple-DES.

3.10. Implementación del algoritmo de cifrado y descifrado DES basado en FPGA

En el 2020, el [26] fue presentado en el Indonesian Journal of Electrical Engineering and Computer Science. En esta nueva propuesta, el autor presenta un análisis del DES aplicado en dispositivos FPGAs. Estos dispositivos aseguran eficiencia en el proceso de computación porque son de alto rendimiento y dan la posibilidad de implementar la computación paralela a través de la construcción de elementos de procesamiento (PE) paralelos llamados procesadores virtuales.

Cualquier sistema que implemente FPGA da resultados más rápidos y precisos que los basados en el tradicional PC. Los FPGAs son una plataforma reconfigurable que da tiempo y soluciones para implementaciones criptográficas que además, no es costoso a diferencia de otros sistemas como ASIC. Los cálculos complejos se resuelven con suma facilidad en los dispositivos FPGAs reduciendo el tiempo necesario para el cifrado de un código. El autor sostiene que su sistema de encriptación es competitivo, rápido, consume menos energía y agregado a ello, propone usar pipelining para aumentar el rendimiento en en cada etapa del cifrado. El inconveniente más relevante sucede cuando la frecuencia sobrepasa la permitida por el sintetizador y el dispositivo empieza a fallar.

3.10.Nueva modificación en el algoritmo FEistel DES basado en claves multinivel

En el mismo año, International Journal of Electrical and Computer Engineering mostró [27] como su nueva publicación. Basándose en las debilidades del cifrado de mensajes, los autores plantean un algoritmo # mucho más seguro por su complejidad pues se necesita un número de intentos 21173 para descifrar el mensaje. Funciona sustituyendo las debilidades de XOR con una operación # con tamaños de bits de bloques variables y usando dos claves adicionales resultado de la combinación de cuatro estados, así, en cada ronda se aumenta la seguridad y complejidad. La diferencia resulta del cambio de una clave que genera el DES a múltiples claves independientes.

Los autores dan una muestra detallada de las modificaciones que proponen en cuanto los niveles de entrada y salida y luego presentan la evaluación en complejidad, tiempo de cifrado y rendimiento, análisis de las pruebas NIST y análisis de histograma.

Como conclusión, el autor plantea una sustitución total de XOR y una modificación de DES en cuanto a su estructura por una más compleja como la presentada.

3.11. Investigación sobre la encriptación de datos contables mediante el algoritmo DES bajo el Sistema de microprocesador

Cerca del final de este recorrido encontramos [28] que fue publicado en el año 2021 por Microprocessors and Microsystems. Allí se hace un análisis de la actualidad de los sistemas de transacciones bancarias realizadas mediante chip en los cuales se hace un proceso de cifrado de mensajes para mantener la información segura de personas no autorizadas.

Los autores proponen que el sistema actual tiene algunas falencias en cuanto a seguridad relacionado con procesadores criptográficos de cifrado simétrico los cuales pueden ser invertidos, contraseñas desequilibradas y baja seguridad en la clave única utilizada. De acuerdo a la conclusión elaborada, se realiza la propuesta de un algoritmo que implica el cifrado y descifrado de datos con una clave secreta. Esta clave es usada con el fin de cambiar el significado del mensaje. En la propuesta el emisor de la clave es capaz de ejecutar todos los mensajes permitiendo la eliminación del usuario y la clave.

A pesar de ser una propuesta bastante prometedora, es importante resaltar que la propuesta diseñada carece de detalle y especificación técnica por lo cual se debe seguir perfeccionando para llegar a los objetivos propuestos de ofrecer un método más seguro para las transacciones bancarias a través de un chip, haciendo uso de un sistema de microprocesadores para el cifrado y descifrado de la información.

3.12. Investigación en estándar de encriptación de información basado en AES para el Internet de las cosas

Con el creciente auge del Internet de las cosas, con lo cual se puede intercambiar información entre personas, personas y cosas o cosas y cosas, se incrementa la importancia de proteger la información con mecanismos de seguridad más robustos y eficientes. Debido a esto Na Su, Yi Zhang, Mingyue Li han diseñado el algoritmo DESI (Data Encryption Standard in IoT) en [29]. El algoritmo DES tiene la falencia de tener una llave muy corta y un paquete de información pequeño, es por esto que surge el algoritmo AES en el cual se pueden tener longitudes de llaves de 128, 192 o 256 bits y mejora la seguridad de la encriptación, ahora con la proliferación de IoT se hace necesario mejorar la seguridad y el tiempo de respuesta de los algoritmos. DESI usa un concepto similar a AES en el cual se realizan rondas de encriptación con 4 fases: sustitución de bytes, rotación de filas, mezcla de columnas, y suma de la llave.

En la sustitución de bytes, se realiza mediante una operación no lineal que es la encargada de agregar la parte de seguridad al algoritmo, que consta de dos partes: primero convierte los bytes a su inverso multiplicativo, en el caso del cero lo deja igual, luego realiza una multiplicación por una matriz constante y al resultado le suma un vector constante.

En la rotación de filas, organiza el texto de 16 bytes en una matriz 4x4, en la cual la primera fila la deja como está, la segunda la rota a la derecha 3 posiciones, la tercera la rota a la derecha 2 posiciones y la cuarta la rota a la derecha 1 posición. Esta etapa agrega la parte de difusión del algoritmo.

Para la mezcla de columnas se realiza una operación matricial entre la matriz 4x4 obtenida del paso anterior y una matriz de coeficientes.

Finalmente, se realiza la suma de la llave, pero la llave cambia en cada ronda de acuerdo al algoritmo de expansión de llave, el cual consiste en tomar segmentos de 4 bytes de la llave, y para calcular el i -ésimo segmento se suma con el segmento $(i-1)$ de esta forma la llave va generando una dependencia con el segmento anterior. Cuando el segmento i es múltiplo de 4 se le aplica una función $g()$ no lineal para agregar mayor difusión al algoritmo.

Los autores sostienen que de acuerdo a la literatura para evitar ataques de Shortcut es necesario tener al menos 6 rondas, es por esto que ellos utilizaron 7 rondas, una adicional para garantizar la seguridad del algoritmo, pero lo suficientemente pocas para garantizar que su ejecución fuera rápida.

Al final, concluyen que el algoritmo DESI mejora la seguridad de encriptación, llegando a tener la misma seguridad que AES pero mejora los tiempos, ya que de acuerdo a la tabla 2, los tiempos de ejecución entre DESI y AES fueron menores en DESI. Debido a esto, sostienen que DESI es una buena alternativa para implementar en el intercambio de información en IoT.

Data size (KB)	AES runtime (ms)		DESI runtime (ms)	
	encrypt ion	Decryp t	encrypt ion	Decryp t
20	99	109	62	78
40	208	218.7	140	156
60	317.3	332.7	203	223.7
80	426.3	442	281	301.7
100	525.3	541	353.7	379.3

Tabla 2. Comparación de tiempos entre AES y DESI.

3.13. Mejora basa en llave para DES en seguridad en textos

A pesar del tiempo el algoritmo DES es ampliamente utilizado como estándar de encriptación en diversas áreas que involucran el intercambio de información, debido a que cada vez se comparte más información a través de redes y sistemas informáticos, incluyendo datos en tiempo real a través de aplicaciones en Internet, es importante garantizar la confidencialidad y seguridad de los datos, tanto en su transmisión como en su almacenamiento. Debido a esto se han propuesto diversas mejoras al algoritmo DES, Omar Reyad, Hanaa M. Mansour, Mohamed Heshmat y Elnomery A. Zanaty proponen en [30] una nueva técnica para la generación de llave mediante una función denominada key-distribution la cual consiste en lo siguiente:

- Realizar la permutación PC-1 para transformar la llave de 56 bits, de aquí los primero 8 bits permanecerán constantes todas las rondas.
- En cada posición aplica la función Odd/Even, la cual consiste en que en la posición par que exista un 1, lo vuelve 0, y la posición impar que exista un 0 lo vuelve un 1.
- El resultado lo divide en dos mitades, C0 y D0.
- Realiza una rotación a la izquierda a cada mitad C0 y D0.
- Aplica la permutación PC-2 y concatena las dos mitades.
- El resultado es la entrada para obtener las llaves siguientes en las próximas rondas.

Una vez tiene la llave generada, realiza el algoritmo DES convencional, teniendo en cuenta que en cada ronda aplica la función key-distribution para crear la llave.

De esta forma los autores concluyen que con su algoritmo Key-based Enhancement DES (KE-DES) es posible aumentar la seguridad del algoritmo DES convencional debido a su implementación de la función key-distribution que permite crear una llave fuerte para el proceso. Por otro lado, resaltan que la velocidad de ejecución no se ve afectada en gran medida debido a que realizaron la comparación con el algoritmo DES y obtuvieron que el tiempo, aunque subió, permanece en el orden de los microsegundos.

4. Conclusiones

Al final de todo este repaso analítico por la historia de estos dos algoritmos, se logra evidenciar que han sido de gran ayuda y también parte fundamental en las diferentes implementaciones y comparaciones con las otras propuestas de mejora de las cuales han sido partícipes. Ya que como parte de la historia de la criptología aunque no sean los más óptimos, ni la mejor opción al momento de brindar seguridad, si fueron ampliamente utilizados en sistemas de seguridad, ya que fueron básicamente los pioneros.

Por otra parte, ambos han sido la fuente o la base para el surgimiento de varios sistemas de seguridad a lo largo de todo este recorrido por su historia, ya que partieron de lo que estos brindan y de sus falencias para crear mejoras que se han implementado en diferentes tesis ya expuestas en este artículo.

Las principales falencias son claras, en cuanto a DES resulta tener una llave muy corta y un paquete de información pequeño (56 bits), y esto ha provocado que la encriptación mediante este método haya sido rota hasta en menos de un día por ataques de fuerza bruta. En cuanto a 3DES ocurre algo similar, debido a que la clave de 192 bits se divide en 3 de 64 bits y esto hace que también puedan ser atacadas mediante fuerza bruta.

También cabe mencionar que en la mayoría de documentación de estos algoritmos resalta a AES, que es conocido como el sucesor de ellos y consecuente a esto resulta ser el más seguro, ya que tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits, superiores a DES y 3DES.

Referencias

- [1] D. Coppersmith, D. B. Johnson, and S. M. Matyas, "A proposed mode for triple-DES encryption," IBM Journal of Research and Development, vol. 40, no. 2, pp. 253–262, 1996. <https://doi.org/10.1147/rd.402.0253>
- [2] S.-J. Han, H.-S. Oh, and J. Park, "The Improved Data Encryption Standard (DES) algorithm," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, 1996.
- [3] N. GAO, Q. WANG, and Z. LI, "A reconfigurable architecture for accelerating DES, 3DES and AES," in Proceedings of the 11th Joint International Computer Conference: JICC 2005, 2005, pp. 474-476.

- [4] R. C. W. Phan, "Reducing the exhaustive key search of the Data Encryption Standard (DES)," *Computer Standards & Interfaces*, vol. 29, no. 5, pp. 528–530, 2007. doi: <https://doi.org/10.1016/j.csi.2006.11.010>
- [5] M. Sachin and D. Kumar, "Implementation and Analysis of AES, DES and Triple DES on GSM Network," *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, pp. 298-303, 2010.
- [6] H. Agrawal and M. Sharma, "Implementation and analysis of various symmetric cryptosystems," *Indian Journal of Science and Technology*, vol. 3, no. 12, pp. 1173-1176, 2010.
- [7] F. Ren, L. Chen, and T. Zhang, "3DES implementation based on FPGA," in *Proceedings of the International Conference on Web Information Systems and Mining*, 2011, pp. 218-224.
- [8] S. Karthik and A. Muruganandam, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, pp. 140-144, 2014.
- [9] Z. Yingbing and L. Yongzhen, "The design and implementation of a symmetric encryption algorithm based on DES," in *2014 IEEE 5th International Conference on Software Engineering and Service Science*, 2014, pp. 517-520.
- [10] S. Rao, "Performance analysis of DES and triple DES," *International Journal of Computer Applications*, vol. 130, no. 14, pp. 30-24, 2015.
- [11] P. Patil, P. Narayankar, D. Narayan, and S. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science*, vol. 70, pp. 1-7, 2015. <https://doi.org/10.1016/j.procs.2016.02.108>
- [12] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 241-246, 2015
- [13] M. M. Abdelwahab, "High performance FPGA implementation of Data encryption standard," *2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE)*, 2015, pp. 235-238. <https://doi.org/10.1109/icneee.2015.7381424>
- [14] Z. Güler, F. Özkaynak, and A. Çınar, "CUDA implementation of DES algorithm for lightweight platforms," in *ACM International Conference Proceeding Series*, vol. Part F131935, 2017, pp. 49-52. <https://doi.org/10.1145/3143344.3143356>

- [15] P. M. Velasco, M. S. Jiménez, and G. X. Chafla, "SATHIRI Vol. 12 –N° 1, pp. 91–103," January-June 2017, ISSN 1390-6925, LATINDEX 21955, <https://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/38/92>
- [16] M. Basri, "Cloud Computing Security Model with Combination of Data Encryption Standard Algorithm (DES) and Least Significant Bit (LSB)," IOP Conference Series: Materials Science and Engineering, vol. 970, no. 1, p. 012027, 2018. <https://doi.org/10.1088/1742-6596/970/1/012027>
- [17] R. R. Devi and V. C. Vijaya Chamundeeswari, "Triple DES: Privacy Preserving in Big Data Healthcare," International Journal of Parallel Programming, vol. 48, no. 3, pp. 515-533, 2018. <https://doi.org/10.1007/s10766-018-0592-8>
- [18] Ratnadewi, Adhie, R. P., Hutama, Y., Saleh Ahmar, A., and Setiawan, M. I., "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)," Journal of Physics: Conference Series, vol. 954, p. 012009, 2018.
- [19] D. Rachmawati, A. S. Harahap, and R. N. Purba, "A hybrid cryptosystem approach for data security by using triple des algorithm and ElGamal algorithm," IOP Conference Series: Materials Science and Engineering, vol. 453, p. 012018, 2018.
- [20] I. T. Plata, E. B. Panganiban, and B. B. Bartolome, "A security approach for file management system using data encryption standard (DES) algorithm," International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 5, pp. 2042-2048, 2019.
- [21] W. Y. Zibideh and M. M. Matalgah, "Modified Data Encryption Standard encryption algorithm with improved error performance and enhanced security in wireless fading channels," Security and Communication Networks, vol. 8, no. 4, pp. 565–573, 2014.
- [22] N. Adam, M. Mashaly, and W. Alexan, "A 3des double-layer based message security scheme," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), May 2019, pp. 1-5.
- [23] M. Haithem and R. A. R. Lateef, "Intelligent TRIPLE DES with N Round Based on Genetic Algorithm," Iraqi Journal of Science, pp. 2058–2066, 2019.
- [24] M. M. Alani, M. Alrammal, and M. Naveed, "Implementing IoT lottery on data encryption standard," Journal of Communications, vol. 15, no. 10, pp. 735–740, Oct. 2020.
- [25] A. Vuppala, R. S. Roshan, S. Nawaz, and J. V. R. Ravindra, "An efficient optimization and secured Triple Data Encryption Standard using enhanced key scheduling algorithm," Procedia Computer Science, vol. 171, pp. 1054–1063, 2020.

- [26] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 774–781, 2020.
- [27] S. M. Kareem and A. M. S. Rahma, "New modification on feistel DES algorithm based on multi-level keys," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3125–3135, 2020.
- [28] M. Haithem and R. A. R. Lateef, "Intelligent TRIPLE DES with N Round Based on Genetic Algorithm," *Iraqi Journal of Science*, pp. 2058–2066, 2019.
- [29] N. Su, Y. Zhang, and M. Li, "Research on data encryption standard based on AES algorithm in internet of things environment," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2019.
- [30] O. Reyad, H. M. Mansour, M. Heshmat, and E. A. Zany, "Key-based enhancement of Data Encryption Standard for Text Security," in *2021 National Computing Colleges Conference (NCCC)*, 2021.