MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

ESTUDIO COMPARATIVO DE LA EFICIENCIA DE LOS ALGORITMOS CRIPTOGRÁFICOS AES Y RSA: CASO DE ESTUDIO DE UNA INSTITUCIÓN EN LA CIUDAD DE GUAYAQUIL

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Sara Noemí LAYANA MOLINA

Bajo la dirección de:
Ing. Washington Antonio CEVALLOS GAMBOA, MSIG, MBA, PhD

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Febrero del 2017

Estudio comparativo de la eficiencia de los algoritmos criptográficos AES y RSA: Caso de estudio de una institución de la ciudad de Guayaquil.

Comparative study of the efficiency of AES and RSA cryptographic algorithms: Case study of an institution in Guayaquil city.

Sara Noemí LAYANA MOLINA[1]
Washington Antonio CEVALLOS GAMBOA [2]

Resumen

El presente trabajo realiza una investigación y análisis sobre los algoritmos criptográficos considerados más utilizados, AES y RSA, con el fin de obtener información sobre su funcionamiento, características, estructura, componentes y sobre todo realizar una comparación entre ellos y conocer sobre su eficiencia y robustez para encontrar el más idóneo que asegure una adecuada implementación y solución para garantizar un nivel razonable de seguridad de la información, que en la actualidad es tan necesaria para el desarrollo de las organizaciones y a la vez tan vulnerable ante cualquier atacante informático que busque robarla, alterarla o modificarla. Para lograr el objetivo planteado en este trabajo de investigación, se utilizó una simulación de cifrado, realizada en cinco archivos de texto de diferentes tamaños, empleando los algoritmos seleccionados, a través de un software de uso libre llamado JCryptool, para lo cual se utilizaron los siguientes parámetros para evaluar el rendimiento de los mismos: tiempo de cálculo, uso de memoria, bytes de salida. De este modo, los resultados evidencian que los valores del tiempo de cálculo, el uso de memoria y los bytes de salidas utilizados por el algoritmo RSA son mayores a los parámetros evaluados con el algoritmo AES, en todos los archivos utilizados en la simulación.

Palabras clave:	Criptografía, simulación de cifrado, algoritmo AES, algoritmo RSA

Abstract

The present work makes a research and analysis on the most commonly used cryptographic algorithms, AES and RSA, in order to obtain information about its operation, characteristics, structure, components and first of all, to know its efficiency and robustness to find the most suitable to ensure an adequate implementation and solution to ensure a reasonable level of information security, which at the moment is so necessary for the development of organizations and at the same time it is so vulnerable to any computer attacker that seeks to steal, alter or modify it. In order to achieve the objective set out in this research, it was used an encryption simulation, made in five text files of different sizes, using the selected algorithms, through a free software called JCryptool, which the following parameters were used to evaluate the performance of the same ones: calculation time, use Memory, output bytes. In this way, the results show that the values of the calculation time, the memory usage and the output bytes used by the RSA algorithm are greater than the parameters evaluated with the AES algorithm, in all the files used in the simulation.

Key words	Cryptography, encryption simulation, AES algorithm, RSA algorithm

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail slayana@uees.edu.ec.
[2] Magíster en Sistemas de Información Gerencial. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

INTRODUCCIÓN

En la actualidad, se evidencia que cada aspecto de la gestión de las organizaciones, depende en gran medida de la información para prosperar, es así que, el desarrollo y definición de las actividades propias de su naturaleza dependen del uso adecuado de la misma, para realizar mejores planificaciones, toma de decisiones y obtener mejores resultados.

De tal manera, con la evolución de la ciencia digital y el uso del internet, esta información puede quedar expuesta y ser pública, lo que origina la proliferación de atacantes informáticos que buscan el robo, deterioro, eliminación, mala utilización o divulgación de la misma, por lo que cualquier persona u organización que maneje cierta cantidad de información se puede convertir en un blanco de estos ataques y podría experimentar consecuencias desfavorables para su desarrollo.

De acuerdo al reporte de investigación emitido por Verizon (2016) sobre infracciones informáticas, el 63% de los encuestados han experimentado robo de contraseñas o información confidencial, así mismo, según el estudio emitido por IBM (2016), realizado a 383 organizaciones, un 48% de todas las alteraciones de información fueron causadas por ataques informáticos, lo que causó pérdidas de 170 millones de dólares.

Por lo tanto, es importante desarrollar e investigar nuevos mecanismos de seguridad que puedan preservar la integridad, disponibilidad y confidencialidad de la información y sus recursos que incluyen hardware, software, firmware, datos y telecomunicaciones, en especial cuando el volumen de la información crece y se hace más compleja (Stallings, 2011). Así mismo, se debe conocer la existencia de técnicas aplicadas para resguardar la privacidad como utilizar un número de código secreto cuando se utiliza una tarjeta de crédito o como cuando se escribe una carta privada se la envía en un sobre sellado para asegurar su confidencialidad.

De acuerdo al reporte emitido por CERT Australia (2015), una de las principales agencias asociadas al Centro Australiano de Seguridad Cibernética, entre los principales mecanismos de seguridad se incluyen, planes de continuidad del negocio, de gestión del riesgo de seguridad, políticas y procedimientos de seguridad de la información, de gestión de cambios, acceso e identidad del usuario, de auditoría, de medios removibles, de gestión de registros, de gestión de claves y de control criptográfico.

Por tal motivo, se evidencia que entre los requisitos indispensables para la protección de la información está la utilización de la criptografía, que comenzó hace miles de años atrás, dentro y entre los gobiernos y las fuerzas militares, al principio, utilizando lápiz y papel, o quizás simples ayudas mecánicas. Luego, a principios del siglo XX, la invención de complejas máquinas mecánicas y electromecánicas, proporcionó medios de encriptación más sofisticados y eficientes, pero después de que la era de Internet fuera introducida en la década de 1990, los algoritmos y protocolos criptográficos se hicieron necesarios y cruciales para mantener los sistemas y la información confidencial de forma segura (Darwish, 2015).

Por lo tanto, la criptografía es necesaria para proteger la información contra amenazas externas, ya que si los atacantes lograren ingresar a la información, no podrán hacer uso de la misma si está encriptada ya que transforma la información en formato ininteligible, de la misma manera protege la información de amenazas internas las cuales representan un 73% de todas las infracciones (nuBridges, Inc, 2008).

Y a pesar de aquello, según una encuesta realizada a 304 organizaciones de diversos países, emitida por PWC (2015), una empresa que ofrece servicios de aseguramiento en Reino Unido, solo un 10% utiliza la criptografía para asegurar su información, por lo tanto, las organizaciones no han demostrado interés por implementar este tipo de mecanismo de seguridad por considerarlo un tema complejo, dado que intervienen otras disciplinas como las

matemáticas y la lógica (Ahmad Milad & Zaiton Muda, 2012), y por la falta de difusión o la falta de investigación sobre la eficiencia de los algoritmos criptográficos y sus diferencias, que pueden ayudar a las instituciones en la protección de la información.

Por lo tanto, es importante conocer la fortaleza de un algoritmo criptográfico que se basa en la forma en que es vulnerable a los ataques realizados (Vellaiyan, Alagarsamy, & Krishnan, 2012). Inclusive, se debe considerar que el algoritmo sea eficiente y conveniente para las organizaciones. A la vez debe ser robusto, ya que muchos intentarán por todos los medios extraer y descifrar la información protegida.

Con base en lo anterior, el objetivo de este trabajo de investigación es realizar un estudio y análisis comparativo entre dos de los algoritmos de encriptación ampliamente utilizados, Advanced Encryption Standard [AES] y Rivest, Shamir y Adleman [RSA], mediante una simulación que permita establecer sus fortalezas y eficiencia, para su aplicación e implementación en las organizaciones.

MARCO TEÓRICO

Hasta aquí, se ha manifestado la importancia de utilizar criptografía para la protección de la información. A continuación se presenta una revisión de literatura en cuanto a la evolución de aspectos teóricos más relevantes al igual que los estudios de campo realizados mediante los algoritmos criptográficos RSA y AES.

La criptografía a través del tiempo.

Según Zulkifli (2007) la criptografía se ha utilizado desde las antiguas civilizaciones. En 3500 A.C., los egipcios desarrollaron escritura jeroglífica, que utilizaban en las tumbas de reyes fallecidos y gobernantes, no para ocultar secretos, sino para contar la historia del difunto con toda elegancia. Mientras que alrededor del año 600 A.C. los eruditos hebreos utilizaban un cifrado de sustitución mono alfabético que consistía en la inversión del alfabeto, entonces *A* era traducido a *Z* y viceversa. Así, el primer dispositivo criptográfico militar fue la llamada escítala, utilizada por los espartanos en el año 500 A.C. que consistía en cifrado de transposición, con una cinta que se enrollaba de forma espiral a una vara o bastón y se escribía de forma longitudinal, cuando se terminaba el mensaje se desenrollaba la cinta y se enviaba al receptor quien tenía que enrollarla en una vara gemela para leer el mensaje.

Así mismo, otro método de criptografía fue utilizado por Julio César entre los años 58 A.C. y 49 A.C., él implementaba el método que en su honor obtuvo el nombre de Cifrado César, con el fin de enviar instrucciones militares altamente confidenciales a sus generales ya que no confiaba en su mensajero o por el temor de que el mensaje pudiera caer en las manos de sus oponentes y sea utilizado en su contra. Así, este método era simple y rápido, el mismo que consistía en el cambio del alfabeto con un desplazamiento de 3, es decir que *A* era traducido a *D*, *B* traducido a *E* y así sucesivamente (Paraskevo & Gianna, 2013).

Durante la era de oro islámica del siglo IX, el árabe Abu Yusuf Ya'qub al-Kindi descubrió una técnica para derrotar la cifra de sustitución mono alfabética, mediante las propiedades intrínsecas de los idiomas que ciertas letras ocurren más a menudo que otras, por tal motivo surgió la necesidad de un sistema de cifrado más fuerte que la sustitución mono alfabética que sea resistente al análisis de frecuencia. Cerca de finales del siglo XVI, un diplomático francés jubilado Blaise de Vigenere introdujo el cifrado de Vigenere, que fue una forma de cifrado de sustitución poli alfabética, en donde *A* puede ser traducido a *J* y en otra ocasión puede ser *T*, y *B* puede ser traducido con *J* o con *R*, de esta manera el análisis de frecuencias resulta menos efectivo (Stallings, 2011).

Sin embargo, Friedrich Wilhelm Kasiski descubrió un método para romper el método de Vigener, por lo que durante la Primera Guerra

Mundial, fue necesario el uso de las máquinas mecánicas para realizar el cifrado lo que marcó el inicio del período de la criptografía, donde surgieron máquinas como Enigma que fue utilizada por el ejército alemán y creada por un inventor alemán, Arthur Scherbius, la cual constaba de tres elementos conectados por cables: un teclado para introducir el mensaje de texto plano, una unidad codificadora que encripta una carta de texto plano en una carta de texto cifrado y una placa de presentación formada de varias lámparas para indicar la letra del texto cifrado, aunque en 1932, Marian Rejewski fue acreditado como la persona quien descifró Enigma (Zulkifli, 2007).

Luego de esto, llegó la era de la ciencia digital, lo que ocasionaba que gran cantidad de operaciones se manejen electrónicamente y que los datos sean guardados en computadoras en forma digital, por lo que eran susceptibles de ser interceptados por cualquier persona y ya no solo sería necesaria la criptografía para los militares, sino también para cualquier institución u organización que utilizaba computadoras para administrar datos (McDonald, 2009).

Así en 1973, la Oficina Nacional de Normas [NBS], ahora el Instituto Nacional de Estándares y Tecnología [NIST], emitió una solicitud pública de propuestas para una criptografía que utilice la misma clave para el cifrado y descifrado, de ahí surge el término simétrico, el resultado fue el método Data Encryption Standard [DES], adoptado como norma federal el 23 de noviembre de 1976, que utilizaba una clave privada de 56 bits, anteriormente de 128 bits (Darwish, 2015).

De este modo, surgió la criptografía simétrica, también llamada de clave secreta o privada, la cual generalmente, los algoritmos se utilizan para cifrar los datos para el almacenamiento. Además hay dos tipos de criptografía simétrica el cifrado de flujo y cifrado de bloque, en donde el primero funciona bit a bit o byte a byte, mientras que el segundo opera bloque por bloque (Paraskevo & Gianna, 2013).

Sin embargo, aún existía un problema y era la distribución de las claves, ya que la clave todavía no podía ser distribuida físicamente mediante mensajería porque comprometía su confidencialidad, por tal motivo Diffie & Hellman (1976) presentaron su trabajo, en donde demostraba un método que permitía aceptar una clave pública compartida y otra secreta, sin transmitir la clave secreta (Zulkifli, 2007).

De este modo, surgió la criptografía asimétrica, o de clave pública, la cual utiliza dos claves, una clave pública conocida por todos y una clave privada conocida por su propietario solamente, las dos claves están vinculadas con propiedades matemáticas, un mensaje cifrado con criptografía de clave pública solo puede descifrarse eficientemente utilizando la clave privada correspondiente, estos esquemas se utilizan principalmente para que dos o más partes puedan establecer una clave compartida de una manera segura, o para los algoritmos de firma digital utilizados para proporcionar autenticidad e integridad de los datos intercambiados (Paraskevo & Gianna, 2013)

De esta manera, Rivest, Shamir, & Adleman (1976) desarrollan el algoritmo de clave pública RSA de ahí el nombre que toma la primera letra de cada nombre. Por lo tanto, con RSA, están involucradas dos claves que son clave pública y clave privada, la clave pública puede ponerse a disposición de terceros mientras la clave privada se mantiene en secreto (Mehrotra & Mishra, 2011).

Con el tiempo surgen varios algoritmos de clave privada y clave pública que van evolucionando y mejorando de acuerdo a las necesidades y a la tecnología, y es en 1996 durante una competencia para seleccionar un estándar de encriptación para reemplazar el existente en ese momento DES, que se presenta el algoritmo AES, como una propuesta para el NIST, que fue nombrado originalmente como Rijndael, en honor a sus desarrolladores del algoritmo; Vicente Rijmen y Joan Daemen. Así, el comité de NIST (2001) anunció la AES como el estándar de Estados Unidos, el cual utiliza el cifrado de clave

simétrica, donde la misma clave se usa para cifrar y descifrar los datos, así como el principal desafío consiste en el intercambio de esa clave con total privacidad ya que si no se encuentra esta clave entonces todo el proceso de cifrado es comprometido e inútil (Darwish, 2015).

¿Qué es Criptografía?

La palabra criptografía se deriva de las palabras griegas kryptos, que significa oculto, y Graphia, que significa escritura por lo que se considera como el arte de la escritura oculta, ya que la criptografía se originó por la necesidad de intercambiar o almacenar información sensible de forma que solo las partes involucradas puedan entender (Peltier, 2013).

Así mismo, en la literatura se evidencian numerosos esfuerzos por definir la criptografía, entre ellos se puede nombrar a Princy (2007) quien señala, que la criptografía es la ciencia y el estudio de la escritura secreta, por lo que de texto claro o texto plano se transforma en texto cifrado que también es llamado un criptograma. Así mismo, Zulkifli (2007) indica que un sistema de criptografía está compuesto de dos funciones complementarias, cifrado y descifrado, el cifrado funciona en texto sin formato para transformarlo en forma ininteligible basada en la clave de entrada, el descifrado opera en el texto cifrado para recuperar el mensaje original utilizando la clave de descifrado.

En cambio, Blaze (1996) indica que la criptografía se refiere al uso de funciones matemáticas, llamadas *cifras*, que separan la seguridad del contenido de un mensaje desde la seguridad de los medios sobre los que se transmite.

Dado que los esfuerzos han sido varios para describir la criptografía, en la Tabla1 se presentan las definiciones de criptografía consideradas más relevantes.

Tabla1.- Definición de criptografía

Autor y Año	Concepto
(Robling Denning, 1983)	La criptografía es la ciencia y el estudio de la escritura secreta. Un cifrado es un método secreto de la escritura, por el cual texto plano o texto claro se transforma en texto cifrado, a veces llamado un criptograma. El proceso de transformación del texto en texto cifrado se llama encriptación o cifrado; El proceso inverso de transformación texto cifrado en texto plano se llama descifrado. Ambos cifrado y descifrado son controlados por una clave o claves criptográficas.
(Blaze, 1996)	La criptografía se refiere al uso de funciones matemáticas, llamadas *cifras*, que separan la seguridad del contenido de un mensaje desde la seguridad de los medios sobre los que se transmite.
(Menezes, Oorschot, & Vanstone, 1996)	La criptografía es el estudio de técnicas matemáticas relacionadas con aspectos de seguridad de la información tales como confidencialidad, integridad de datos, autenticación de entidad y autenticación original de datos. La criptografía no es el único medio de proporcionar seguridad de la información, sino más bien un conjunto de técnicas.
(Bellare & Rogaway, 2005)	Criptografía se trata de construir y analizar protocolos que superen la influencia de los adversarios
(Calderbank, 2007)	La criptografía es el cifrado del texto de tal manera que personas externas al código no pueden entenderlo, pero el lector deseado es capaz de descifrar el encriptado para entender el mensaje.
(Goldwasser & Bellare, 2008)	La criptografía es sobre la comunicación en presencia de un adversario. Abarca muchos problemas (encriptación, autenticación, distribución de claves para nombrar algunos). El campo de la criptografía moderna proporciona una teoría sobre la base del cual podemos entender qué

	son exactamente estos problemas, cómo evaluar protocolos que pretenden resolverlos, y cómo construir protocolos en cuya seguridad podemos tener constancia.
(Kayarkar, 2012)	La criptografía es el estudio y la práctica de las técnicas en las que el texto sin formato por cifrado se convierte en un texto ofuscado y no legible.
(Gupta, 2012)	La criptografía son los métodos que permiten que la información sea enviada de forma segura de tal manera que el único receptor capaz de recuperar esta información, sea aquel que posea la clave para descifrar el mensaje.
(Padmavathi & Ranjitha, 2013)	La criptografía es una manera efectiva de proteger información, es un método para almacenar y transmitir datos en forma que solo aquellos a los que se destina para leer y procesar.
(Asole & Mundada, 2013)	La criptografía es la técnica utilizada para evitar el acceso no autorizado a los datos. La criptografía hace uso de los algoritmos de cifrado y descifrado. Asegura los datos de tal manera que incluso si cualquier tercero intenta interpretar los datos, no puede descifrarlo. Los datos se transmiten en un estado encriptado o codificado y más tarde descifrados o decodificado por el destinatario. La criptografía hace uso de *claves* para cifrar o descifrar los datos.
(Saranya & Phani Krishna, 2013)	La criptografía es el proceso de ocultar o transformar la información mediante un cifrado o un código para que se vuelva ilegible para todas las demás personas, excepto aquellos que tienen una clave para la información. La información codificada resultante se denomina información cifrada.
(Kolhe, Raza, & Patheja, 2013)	La criptografía es un proceso de cifrado / descifrado de un texto plano / cifrado utilizando el algoritmo apropiado y la longitud de clave adecuada.
(Rafiq, 2014)	La criptografía es la técnica de proteger la información transformándola en un formato ilegible, denominado texto cifrado. Solo aquellos que poseen una clave secreta pueden descifrar o descifrar el mensaje en texto plano. El objetivo principal de la criptografía es asegurar la información cambiándola de una forma que no puede ser entendida y leída por los atacantes.
(Marcella, 2014)	La criptografía es el proceso de conversión de un texto sin formato en un texto cifrado o encriptado utilizando un algoritmo, haciendo que el texto resultante sea ilegible sin una clave de descodificación. Un cifrado es una manera de hacer una palabra o un mensaje secreto cambiando o reordenando las letras en el mensaje.
(Bhanot & Hans, 2015)	La criptografía es una forma de garantizar que la confidencialidad, la autenticación, la integridad, la disponibilidad y la identificación de los datos del usuario se pueden mantener, así como la seguridad y la privacidad de los datos se puede proporcionar al usuario.
(Kaur & Arora, 2015)	La criptografía es la ciencia de la seguridad de la información. La palabra se deriva de los kryptos griegos, es decir, ocultos. La criptografía puede definirse como la conversión de datos en un código codificado que se puede descifrar y enviar a través de una clave pública o privada.
(Pawar, Tandel, Zeple, & Sonawane, 2015)	La criptografía es la técnica en el proceso de cifrado y descifrado utilizada para ocultar datos simples de usuarios no autorizados mediante la conversión en forma ilegible y recuperarlo de nuevo en original.

Fuente: Elaboración propia, basada en la revisión de la literatura.

De acuerdo a las definiciones anteriormente expuestas, se puede resumir que la criptografía es la ciencia y el estudio de la escritura secreta, por el cual transforma un texto plano en texto cifrado, utilizando técnicas o funciones matemáticas, con el objetivo de que sea ilegible para todas las personas, excepto aquellos que tienen una clave para descifrarlo, para así conservar la confidencialidad, integridad y autenticidad de la información.

Algoritmo Rivest, Shamir y Adleman [RSA]

En tiempos de guerra, fue esencial que el enemigo no sepa las estrategias que se estaban tramando, porque ganar o perder una guerra dependía del secreto de las operaciones para sorprender al enemigo, por tal motivo se utilizó la criptografía como un instrumento para enviar mensajes secretos y transmitir estrategias sin que el enemigo se entere, sin embargo, hubo un problema, ¿cómo transmitir la clave de forma segura?, a todos los lectores deseados del mensaje, ya que si uno de los libros de claves de los alemanes utilizados para Enigma no hubiera sido interceptado, ellos hasta podrían haber ganado la guerra (Zulkifli, 2007).

Fue cuando Whitfield Diffie, trabajando en colaboración con Martin Hellman, tuvo la idea de incorporar a su cifrado una clave pública, la clave privada es la clave de descifrado y la clave pública es la clave de cifrado, por lo tanto, si una persona, Bob, quiere enviar un mensaje a otra persona, Alice, todo lo que tiene que hacer es usar la clave pública de Alice para cifrar el mensaje. Ahora la única persona en el universo que puede descifrar ese mensaje es Alice, porque tiene la clave privada, entonces Bob encripta el mensaje usando la clave pública, pero no puede descifrarlo a menos que el decodificador tenga una pieza especial de conocimiento desconocido para el resto del mundo, la clave privada (Calderbank, 2007).

Aunque Diffie concibió la idea de la clave pública, en realidad no tenía una función específica de un solo sentido que cumpla con los requisitos. Sin embargo, el trabajo de Diffie & Hellman (1976) mostró que había solución para la distribución de claves y despertó interés entre otros matemáticos y científicos. Por mucho que lo intentara, Diffie y sus socios Hellman y Merkle no podían descubrir tal algoritmo, ese descubrimiento fue hecho por otro trío de investigadores: Ron Rivest, Adi Shamir y Leonard Adleman, quienes desarrollaron el algoritmo RSA, donde R es para Rivest, S para Shamir, y A para Adleman, de cifrado de clave pública o clave asimétrica, llamado así porque una de las claves puede ser compartida con todos y otra clave debe mantenerse privada y las dos claves que se utilizan en el proceso de cifrado y descifrado son diferentes (Makhmali & Mat Jani, 2013).

De esta manera, RSA fue desarrollado en el otoño de 1976 y publicado en 1977, el cual es ampliamente utilizado para el cifrado, el intercambio de claves y la firma digital. De tal modo, el algoritmo RSA implica tres pasos principales; generación de claves, una privada y una pública, encriptación y descifrado, como el nombre lo indica, cualquier persona puede recibir información sobre la clave pública, pero por otro lado la clave privada debe mantenerse en secreto, la idea es que cualquiera puede usar la clave pública para cifrar un mensaje, pero solo la persona que posee la clave privada correspondiente puede descifrarlo, la clave del poder y la seguridad del algoritmo RSA se basa en los problemas de factorización, donde la única manera de romper el RSA es encontrar un algoritmo eficiente para factorizar grandes números (Calderbank, 2007).

Por otro lado, RSA, tiene solo una ronda de encriptación, utiliza un bloque de cifrado y de una clave de tamaño variable, el proceso consiste en generar dos números primos grandes del mismo tamaño, al menos de 100 dígitos, los cuales se mantienen en secreto al lado del remitente, estos números serán llamados p y q, el producto de estos números primos da el valor de n, el producto se utilizará como módulo para la clave pública y la privada. Su longitud, generalmente

expresada en bits, es la longitud de la clave (Mehrotra & Mishra, 2011).

Luego, se selecciona un entero aleatorio denominado *e* o exponente público, donde *e* debe ser mayor a 1 y el máximo común divisor *(e, (p-1), (q-1)) = 1*, el número *e* se publica como exponente de clave pública. A continuación, busca la inversa multiplicativa de *e (mod ((p-1) (q-1)))*, denominada *d* o exponente privado. La clave pública es *(n, e)* y la clave privada es *d* (Makhmali & Mat Jani, 2013).

De este modo, uno de los principales beneficios del algoritmo RSA es que la clave pública puede ser creada y enviada a alguien para cifrar un mensaje, pero solo la clave privada del receptor se puede utilizar para descifrarlo, y si la clave pública es lo suficientemente grande, solo alguien con conocimiento de los factores primos puede decodificar el mensaje, ya que su seguridad se basa en la dificultad de factorizar enteros grandes (Bhanot & Hans, 2015).

Además, este algoritmo ha sido utilizado en cientos de productos de software y en diversas aplicaciones tales como exploradores de Internet de Microsoft y Netscape, como Lotus, Notes, Intuit Quicken, entre otros, también se puede utilizar para el intercambio de claves, firmas digitales, o cifrado de pequeños bloques de datos, también es utilizado en protocolos de comercio electrónico [SSL] (Makhmali & Mat Jani, 2013).

Tal es el caso que, RSA se ha usado ampliamente para el establecimiento de canales de comunicación seguros y para la autenticación de la identidad del prestador de servicios sobre un medio de comunicación inseguro. Así, en el esquema de autenticación, el servidor implementa clave pública, la autenticación con el cliente se lleva a cabo mediante la firma de un mensaje único del cliente con su clave privada, creando así lo que se llama una firma digital. De esta manera, la firma se devuelve entonces al cliente, que la verifica con la clave pública conocida del servidor (Bhanot & Hans, 2015).

De acuerdo a Padmavathi & Ranjitha (2013), RSA es el algoritmo de cifrado de clave pública más utilizado. Se requiere claves de al menos 1024 bits para una buena seguridad, en donde claves de tamaño de 2048 bits proporcionan una mejor seguridad.

A pesar de que RSA parece muy seguro y ha sido ampliamente utilizado por muchas empresas y aplicaciones, una forma poco común de manipulación ha pretendido romper RSA, ya que tres miembros de la Universidad de Michigan han afirmado que podrían romper simplemente ajustando la fuente de alimentación de un dispositivo. Además, su método era activar el voltaje del CPU de tal manera que genera un solo error de hardware por ciclo de reloj, comprometiendo al servidor a voltear bits individuales de la clave privada a la vez, ya que varias iteraciones del proceso juntarán lentamente la contraseña, por lo que, en un procesador Pentium 4 y 104 horas de tiempo de procesamiento, podrían *hackear* un cifrado de 1024 bits en OpenSSL (Makhmali & Mat Jani, 2013).

Por otro lado, RSA es lento para cifrar grandes volúmenes de datos, ya que consume mucho tiempo para cifrar datos, por lo que se considera como una desventaja de los algoritmos de clave asimétrica debido al uso de dos claves asimétricas, por otro lado, una nueva amenaza en este algoritmo es la inserción de una clave falsa en el nivel de descifrado, por lo tanto, la clave secreta debe ser privada y correcta para lograr el cifrado de manera exitosa (Bhanot & Hans, 2015).

Algoritmo Advanced Encryption Standard [AES]

El NIST (1997) inició un proceso para seleccionar un algoritmo de cifrado de clave simétrica, en el cual se utiliza la misma clave tanto para el cifrado como para el proceso de descifrado, por lo tanto, el secreto de la clave se mantiene en privado y funciona con alta velocidad, que se utilizaría para proteger información federal y mensajes

confidenciales, no clasificados, para promover las responsabilidades estatutarias del NIST.

Después de lo cual, el NIST (1998) anunció la aceptación de quince algoritmos candidatos y solicitó la asistencia de la comunidad criptográfica de investigación en el análisis de los candidatos. Así, este análisis incluyó un examen inicial de las características de seguridad y eficiencia de cada algoritmo. NIST revisó los resultados de esta investigación preliminar y seleccionó MARS, RC6, Rijndael, Serpent y Twofish como finalistas. Después de haber revisado el análisis público de los finalistas, el NIST decidió proponer Rijndael como el Advanced Encryption Standard [AES] (Nechvatal, y otros, 2000).

De tal manera, el nombre original de AES era Rijndael, ya que fue nombrado por sus desarrolladores, Vincent Rijmen y Joan Daemen. Así, el algoritmo fue presentado como una propuesta al NIST para seleccionar un estándar de cifrado para reemplazar el existente en ese momento Data Encryption Standard [DES], que fue publicado en 1977. Así, el comité del NIST anunció el AES como estándar estadounidense el 26 de noviembre de 2001, el cual utiliza cifrado simétrico de una misma clave para cifrar y descifrar los datos (Darwish, 2015).

Por lo tanto, el algoritmo criptográfico debe ser un trabajo integral de proceso de cifrado y descifrado y preservar una alta seguridad de los datos que se transmiten. Básicamente, los algoritmos de cifrado se dividen en tres categorías principales: transposición, sustitución y transposición - técnica de sustitución. Internamente, las operaciones del algoritmo AES se realizan en una matriz bidimensional de bytes llamada estado. Además, el estado consiste en cuatro filas de cada bytes, cada una contiene Nb número de bytes, donde Nb es la longitud del bloque dividido por 32 (Vellaiyan, Alagarsamy, & Krishnan, 2012).

Igualmente, el algoritmo AES se basa en un principio de diseño conocido como una red de sustitución-permutación. Así, este algoritmo tiene un tamaño de bloque fijo de 128 bits y un tamaño de clave de 128, 192 o 256 bits, el tamaño de la clave utilizado para un cifrado AES especifica el número de rondas de transformación (Darwish, 2015). Por lo tanto, AES utiliza 10, 12 o 14 rondas, dependiendo del tamaño de la clave que puede ser 128, 192 o 256 bits, respectivamente (Prajapati, Patel, & Macwan, 2014).

Por lo cual, cada ronda consta de varios pasos de procesamiento, cada uno de los cuales contiene cuatro similares pero diferentes etapas, incluyendo una que depende de la propia clave de cifrado. Luego, se aplica un conjunto de rondas inversas para descifrar los datos, es decir, transformar el texto cifrado de nuevo en el texto plano original, utilizando la misma clave de cifrado, la cual es originalmente de 16 bytes, por lo que se utiliza en el algoritmo de expansión de clave para generar un número de subclaves donde cada subclave se utiliza en cada ronda en el proceso de cifrado. Así, la clave original se divide en claves *round* donde se necesita una después de cada ronda y antes de la primera (Darwish, 2015).

De acuerdo a Bhanot & Hans (2015), estas claves se aplican junto con otras operaciones matemáticas en una matriz de datos que están presentes en bloques de tamaño particular, es decir, en la matriz de estado. Por lo tanto en, este proceso de cifrado incluye los siguientes pasos: Primero obtiene las diferentes claves de cifrado, luego inicializa la matriz de estado con datos de bloques o texto sin formato, después comienza con la matriz de estado inicial agregando la clave, para realizar el proceso de manipulación del estado en nueve rondas, después de la décima ronda de manipulación, se obtiene la salida final como texto cifrado.

Según Makhmali & Mat Jani (2013); Mahajan & Sachdeva (2013); y Darwish (2015), el proceso de encriptación de este algoritmo tiene las siguientes funciones principales (véase Tabla2 y Figura1):

Tabla2.- Funciones principales del algoritmo AES

Etapa	Proceso	Detalle
Etapa inicial	*AddRoundKey*	
Rondas	*SubBytes*	En este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda (Véase Figura1).
	ShiftRows	En este paso se realiza una transposición donde cada fila de la matriz es rotada de manera cíclica un número determinado de veces (Véase Figura1).
	MixColumns	Operación de mezclado que opera en las columnas de la matriz, combinando los cuatro bytes en cada columna usando una transformación lineal, cada columna de la matriz es multiplicada por un polinomio constante c(x) (Véase Figura1).
	AddRoundKey	Cada byte de la matriz es combinado con la clave *round*; cada clave *round* se deriva de la clave de cifrado usando una iteración de la clave. (Véase Figura1).
Etapa final	*SubBytes*	
	ShiftRows	
	AddRoundKey	

Fuente: Elaboración propia, basado en Makhmali & Mat Jani (2013); Mahajan & Sachdeva (2013); y Darwish (2015)

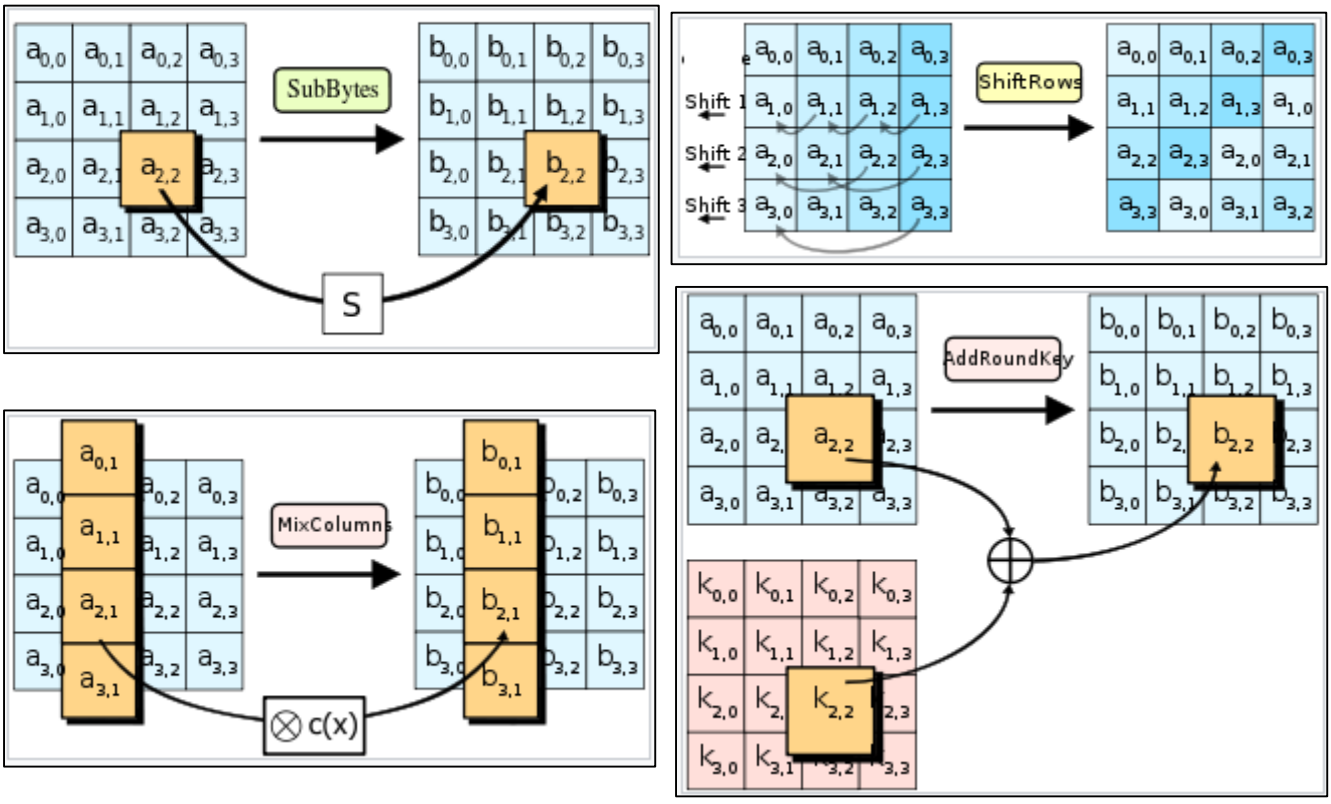

Figura1.- Rondas de AES
Fuente: Vinda (2013)

Por lo tanto, AES se caracteriza no solo por la seguridad, sino también por su velocidad. Es así que, puede ser implementado en varias plataformas especialmente en dispositivos pequeños (Mahajan & Sachdeva, 2013). Además, en la evaluación realizada por el NIST para escoger el algoritmo estándar que reemplace al DES se especificó el conjunto de criterios de evaluación que se utilizarían para comparar los algoritmos candidatos, entre ellos estaban seguridad, costo y características de implementación, pero la seguridad fue el factor más importante y abarcó características como la resistencia del algoritmo al criptoanálisis, la solidez de su base matemática, la aleatoriedad de la salida del algoritmo y seguridad relativa en comparación con otros candidatos.

De tal manera, los resultados arrojaron que AES tenía un margen de seguridad adecuado, a pesar de que el margen de seguridad es un poco difícil de medir porque el número de rondas cambia con el tamaño de la clave. Sin embargo, su estructura es bastante simple, lo que puede haber facilitado su análisis durante el tiempo especificado del proceso de desarrollo de AES (Nechvatal, y otros, 2000).

Sin embargo, según Jackson (2011), investigadores anónimos de Microsoft y una universidad de investigación con sede en Bélgica llamada Katholieke Universiteit Leuven han descubierto una manera de romper el algoritmo AES, su ataque puede recuperar una clave secreta de tres a cinco veces más rápido de lo que se creía posible. No obstante, los investigadores advierten que el ataque es complejo, por lo que no se puede llevar a cabo fácilmente utilizando las tecnologías existentes, ya que en la práctica, la metodología utilizada por los investigadores llevaría miles de millones de años de tiempo de computadora para romper el algoritmo.

A pesar de eso, indican que el resultado de este proyecto puede significar una fisura en la armadura del estándar AES, considerado irrompible, podría ser más fácilmente roto por las computadoras más rápidas de mañana, o por nuevas técnicas en un futuro. A consecuencia de esto, los creadores de AES, Joan Daemen y Vincent Rijmen han reconocido la validez del ataque (K.U. Leuven, 2011).

Después de haber realizado la revisión de literatura, en la Tabla3 se agrupan las características de los algoritmos RSA y AES, de acuerdo a estudios previos.

Tabla3.- Características AES y RSA

Factores	AES	RSA
Desarrolladores	Vicente Rijmen y Joan Daemen	Rivest, Shamir y Adleman
Año de publicación	2001	1977
Tamaño de la clave	128, 192, 256 bits	>1024 bits
Tamaño del bloque	128 bits	Mínimo 512 bits
Clave de cifrado y descifrado	La misma	Diferentes
Escalabilidad	No escalable	No escalable
Algoritmo	Algoritmo Simétrico	Algoritmo Asimétrico
Cifrado	Más Rápida	Más Lenta
Descifrado	Más rápido	Más lento
Consumo de energía	Bajo	Alto
Seguridad	Excelente Seguridad	Menos seguro
Repositorio de claves	Necesario	Necesario
Posibles vulnerabilidades	Ataque de fuerza bruta	Ataque de fuerza bruta y de Oracle
Rondas	10/12/14	1
Velocidad de simulación	Rápida	Rápida
Caballo de Troya	No probado	No

Implementación de Hardware y Software	Más Rápida	No eficiente
Algoritmo de cifrado y descifrado	Diferente	El mismo

Fuente.- Elaboración propia, basado en Mahajan & Sachdeva (2013).

Estudios Previos de los algoritmos AES y RSA

Al realizar una investigación, es necesario contar con una recopilación y análisis multidisciplinario de diferentes especialistas de los datos considerados más relevantes para poder definir en líneas generales diferentes soluciones para un determinado problema, mediante la valorización de todos sus efectos, para lo cual esta investigación ha revisado diversos estudios previos, que analizan y realizan comparaciones de los algoritmos criptográficos.

Dado que los estudios realizados sobre los algoritmos AES y RSA han sido varios, en la Tabla4 se muestra los resultados considerados más relevantes, que diferentes autores obtuvieron al realizar simulaciones y comparaciones entre ellos.

Tabla4.- Estudios Previos de los algoritmos AES y RSA

Autor y año	Resultados
(Mehrotra & Mishra, 2011)	En esta investigación se realiza una comparación de los parámetros tiempo, utilización de memoria y byte de salida, utilizando el mismo archivo de texto para cinco experimentos. Al analizar los resultados se nota que RSA tiene un menor byte de salida en comparación con el algoritmo AES, el tiempo tomado por el algoritmo RSA es mucho mayor que el tiempo que toma AES, en el uso de la memoria se observa que no aumenta según el tamaño del archivo en ambos algoritmos, y que los usos de memoria del algoritmo RSA son más altos para todos los tamaños de texto mientras que el uso de memoria es menor. En conclusión, de acuerdo a los datos arrojados en el resultado experimental, concluyen que el algoritmo AES tiene menos uso de memoria mientras que el algoritmo RSA consume el tiempo de cifrado más largo y el uso de memoria muy alto pero el byte de salida es menor en el caso del algoritmo RSA.
(Vellaiyan, Alagarsamy, & Krishnan, 2012)	En este estudio se presenta el rendimiento y la comparación con respecto a varios parámetros. La relación de cifrado se mide en términos de mínimo, moderado o máximo. La velocidad se define por el siguiente término como rápido, lento, moderado. Se especifica la sintonización como si o no. El valor clave se mide en términos de valor de bit utilizado. Los resultados experimentales se implementan utilizando el estudio visual. Como resultado se concluye que la proporción de cifrado es alta en el uso de las técnicas de cifrado de clave simétrica. La longitud de clave es alta en el tipo de cifrado asimétrico, por lo tanto, para romper el código es complejo en RSA. En el aspecto de velocidad, el cifrado de clave simétrica se determina como bueno. Por último, se determina que el algoritmo RSA es más seguro, ya que utiliza la factorización de un número primo alto para la generación de claves. Por lo tanto, el algoritmo RSA se encuentra como la mejor solución en este método.
(Makhmali & Mat Jani, 2013)	Eligen AES como mejor opción, debido a las siguientes razones: 1.- El tamaño del bloque: Los datos que se cifran en su sistema son largos y podrían contener hasta varias páginas de datos. Teniendo en cuenta este hecho, AES es la mejor opción, por tener un mayor tamaño de bloque y se demuestra en el experimento ser capaz de evitar ataques de fuerza bruta.

	2.- El tamaño de la clave: Comparativamente, AES tiene el tamaño clave más grande. 3.- Aplicabilidad: AES es de código abierto, y puede ser fácilmente implementado en aplicaciones basadas en web utilizando una variedad de lenguajes de programación como PHP. Incluso es posible modificar el proceso real de AES ya que tiene acceso y puede trazar claramente el proceso; aunque no se aconseja porque su proceso es notablemente complicado y una pequeña manipulación falsa en el proceso puede causar inconsistencias a lo largo del resto.
(Mahajan & Sachdeva, 2013)	En este trabajo investigativo, se utiliza cuatro archivos de texto de diferentes tamaños para realizar cuatro experimentos, donde el rendimiento del algoritmo de cifrado es evaluado considerando los siguientes parámetros: tiempo de cifrado y tiempo de descifrado. El tiempo de cifrado se considera el tiempo que un algoritmo de cifrado toma para producir un texto cifrado de un texto sin formato. Basándose en los archivos de texto se llega a la conclusión de que el algoritmo AES consume menos cifrado y RSA consume más tiempo de cifrado. También se observó que el algoritmo de descifrado de AES es mejor. A partir del resultado de la simulación, se evaluó que el algoritmo AES es mucho mejor que RSA.
(Padmavathi & Ranjitha, 2013)	En esta investigación los resultados experimentales se implementan utilizando el *Visual Studio Net*. Se evalúan los algoritmos AES, DES y RSA considerando los siguientes parámetros: 1.- Tiempo de cifrado, es decir, el tiempo que se tarda en producir un texto cifrado y el tiempo que se tarda en producir texto del texto cifrado. 2.- Tamaño del búfer, es decir, la variación en el uso de memoria. Con base en el resultado experimental se concluyó que el tiempo de cifrado, descifrado y el uso de búfer es menor en comparación con el algoritmo DES. Pero RSA consume más tiempo de cifrado y el uso del búfer es también muy alto. También se observa que el descifrado del algoritmo AES es mejor que otros algoritmos. A partir del resultado de la simulación, se evaluó que el algoritmo AES es mucho mejor que el DES y el RSA.
(Prajapati, Patel, & Macwan, 2014)	En este estudio, se evalúa el rendimiento del algoritmo de cifrado considerando los siguientes parámetros: 1.- Tiempo de cifrado 2.- Uso de la memoria El tiempo de cifrado se considera como el tiempo que un algoritmo toma para producir un texto cifrado de un texto plano. Para esta simulación se utilizan tres algoritmos AES, DES y RSA utilizando cinco archivos de 32KB, 64KB, 128KB, 256KB, y 512KB. Basado en los archivos de texto utilizados en el experimento se concluyó que los algoritmos AES y DES consumen menos tiempo de cifrado comparado con el RSA y el algoritmo DES utiliza menos memoria, mientras que la diferencia de tiempo de cifrado entre los algoritmos AES y DES es muy pequeña. Cuando el tamaño de los datos aumenta entonces el algoritmo criptográfico asimétrico realiza más lento el cifrado comparado con el algoritmo simétrico.
(Bhanot & Hans, 2015)	En este trabajo de investigación se encuentra que cada algoritmo tiene sus propios beneficios de acuerdo con diferentes parámetros. A partir del trabajo realizado en esta investigación se observa que la fuerza de cada algoritmo de cifrado depende de la gestión de claves, tipo de criptografía, número de claves, número de bits utilizados en una clave. Cuanto más larga sea la longitud de la clave y la longitud de los datos será el consumo de energía que conducirá a más disipación de calor. Por lo tanto, no es aconsejable utilizar secuencias cortas de datos y longitudes de clave. Todas las claves se basan en las propiedades matemáticas y su fuerza disminuye con respecto al tiempo. Las

	claves que tienen más número de bits requieren más tiempo de cálculo que simplemente indica que el sistema tarda más tiempo en cifrar los datos.
(Bisht & Sapna, 2015)	Aquí el estudio de algoritmos de clave simétrica, AES y DES, y asimétrica, RSA y DIFFIE-HELLMAN, se realiza de acuerdo a diferentes factores. La clave utilizada es definida en términos de cifrado y descifrado, si es igual o diferente. El algoritmo utilizado se define de acuerdo a su tipo simétrico o asimétrico. La longitud de la clave se utiliza según el valor del bit. La velocidad se define en términos de rápido o lento. El consumo de energía se toma como baja o alta. La seguridad se define como excelente, menos segura y no segura. El costo se define como más barato o costoso. La implementación según su algoritmo utilizado es simple o compleja. De acuerdo al análisis de los resultados se determinó que los algoritmos de clave simétrica se consideran buenos en términos de velocidad y consumo de energía. En el cifrado de clave simétrica el algoritmo AES se encuentra en términos de mejor costo, seguridad e implementación. En cifrado de clave asimétrica algoritmo RSA es mejor en términos de velocidad y seguridad.
(Verma, Guha, & Mishra, 2016)	Este trabajo presenta un estudio comparativo de diferentes algoritmos como, AES, DES, 3DES, Blowfish y RSA. Cada algoritmo ha sido comparado en diferentes conjuntos de parámetros, como son, consumo de recursos, seguridad, rendimiento, resistencia al criptoanálisis y sintonización. De los resultados se ha encontrado que entre el algoritmo de cifrado simétrico, AES y Blowfish son los algoritmos más seguros y eficientes. La velocidad y el consumo de energía de estos algoritmos son mejores en comparación con los otros. En caso de cifrado asimétrico el algoritmo, RSA es seguro y puede ser utilizado para la aplicación en redes inalámbricas debido a su buena velocidad y seguridad.
(Karule & Nagrale, 2016)	En este estudio se realizan experimentos con diferentes tipos y tamaños de archivos con extensión como .jpeg, .txt, .doc y .pdf, para comparar dos algoritmos AES y RSA. El rendimiento de los algoritmos de cifrado se evalúa considerando los siguientes criterios: 1.- Tiempo de cifrado 2.- Uso de memoria (tamaño de archivo cifrado) Del análisis comparativo se concluye que RSA requiere menos tiempo de cifrado en comparación con AES, sin embargo el uso de memoria de AES es menor en comparación con RSA para los cuatro tipos de archivos con extensión .jpeg, .txt, .doc y .pdf. De acuerdo a los resultados, RSA funciona mejor que AES en términos de tiempo de cifrado.

Fuente: Elaboración propia, basada en la revisión de la literatura.

Hasta aquí, se ha presentado una revisión de literatura sobre los aspectos teóricos considerados más relevantes al igual que los estudios previos y análisis de la criptografía y sus algoritmos ampliamente utilizados RSA y AES.

METODOLOGÍA.

Esta investigación aplicó un enfoque cualitativo, ya que presenta una investigación y recolección de datos considerados más relevantes, para entender las características de los algoritmos criptográficos estudiados, teniendo en cuenta todos los elementos que los rodean y llevando a cabo estudios intensivos a pequeña escala.

Así también, en esta investigación se aplica un alcance descriptivo porque abarca el estudio a través de la descripción, registro y análisis en función de los datos obtenidos de una simulación de cifrado de cinco archivos de texto de diferentes tamaños: 9 KB, 76 KB, 712 KB, 1011 KB, 10135 KB, realizada a través de un software de uso libre llamado JCryptool, para lo cual se consideraron los siguientes parámetros de

evaluación: tiempo de cálculo, uso de memoria y bytes de salida, mediante la observación, medición e interpretación cuidadosa de los resultados, se pudo verificar el comportamiento y la eficiencia de los algoritmos estudiados.

Por este motivo, Hernández, Fernández & Baptista (2010) indican que la metodología descriptiva tiene como propósito especificar características y propiedades importantes que según Dankhe (1986) es un análisis mediante la medición y evaluación de un fenómeno que afecta a personas o grupos.

Por lo tanto, para alcanzar los objetivos específicos de la investigación se realizaron las siguientes actividades (véase Tabla5):

Tabla5.- Diseño de la investigación

Actividad	Descripción
Identificación de algoritmos criptográficos propuestos	En esta fase se realizó la investigación de las características y funcionamiento de los algoritmos criptográficos propuestos para establecer sus diferencias y similitudes, de esta manera, desarrollar una metodología que permitía demostrar sus atributos y robustez para el aseguramiento de la información.
Definición de los índices de medición	En este proceso fue necesario definir el contexto del problema e identificar el objetivo de la investigación, para tener una definición clara de lo que se desea simular, en este caso se especificó los índices de medición para determinar la eficiencia de los algoritmos, de acuerdo a los estudios previos y al análisis realizado de la literatura se determinó que para evaluar el rendimiento de los algoritmos AES y RSA se consideraron los siguientes parámetros: - Tiempo de cálculo. - Uso de memoria. - Bytes de salida.
Selección del software simulador	Esta actividad corresponde a la selección del software con el que se realizó la simulación, de acuerdo a los parámetros que se determinaron en la etapa anterior, para esto se escogió el software de uso libre JCryptool, el cual contiene los elementos estructurales propios de los procesos necesarios para dar respuesta al objetivo de este trabajo de investigación ya que es una plataforma de *e-learning* de código abierto que permite experimentar con diversos algoritmos criptográficos, entre ellos AES y RSA.
Definición del control de la simulación	Para trabajar con los resultados de una simulación, es preciso definir y disponer de información como el tiempo de inicio y de término de la simulación, el equipo informático utilizado para la elaboración de la simulación, la cantidad de corridas o simulaciones necesarias y los controles deseados. Por lo tanto, después de realizar la revisión de la literatura se estableció que la simulación de cifrado debía realizarse a cinco archivos de texto plano de diferentes tamaños, para poder verificar el comportamiento y la eficiencia de los algoritmos estudiados, los cuales fueron: - Archivo1 (9KB) - Archivo2 (76 KB) - Archivo3 (712 KB) - Archivo4 (1,011 KB) - Archivo5 (10,135 KB) También la computadora seleccionada para realizar la simulación tenía las siguientes características: - Sistema Operativo Windows 7 - Procesador Intel Core I5 CPU 1.70 GHz - Memoria RAM de 4.00 GB (3.41 GB utilizable)
Pruebas y validación	Se realizaron las pruebas necesarias para el manejo del software de simulación y se comprobó que la corrida de simulación se ejecuta de acuerdo a lo especificado en el mismo.
Ejecución de la simulación	Después de cada simulación de cifrado de cada archivo se comprobó la consistencia de los resultados e identificó cualquier resultado incongruente con el

	comportamiento del software. Aquí, se generaron los datos deseados y luego fue posible elaborar interpretaciones de los resultados con bastante detalle que refleje el comportamiento de cada algoritmo.
Interpretación	Se interpretaron los resultados que arrojó la simulación y con base a esto se evaluó la eficiencia de los algoritmos que se estima que puedan resolver el problema planteado para luego realizar una conclusión.

Fuente: Elaboración propia.

ANÁLISIS DE RESULTADOS

El resultado de la simulación de los algoritmos de cifrado AES y RSA se muestra en la Tabla6, se observa que el tiempo tomado por el algoritmo RSA para los archivos 2, 3, 4 y 5 es mayor comparado con el tiempo que toma el algoritmo AES. Lo mismo sucede con los siguientes parámetros de evaluación, la memoria utilizada por RSA en todos los archivos es mayor que la que usa el algoritmo AES, al igual que los archivos de salidas, los que son generados por el algoritmo RSA son de mayor tamaño que los de AES.

Tabla6.- Resultados de la simulación en JCryptool.

	Algoritmo	Tiempo en segundos	Memoria en KB	Archivo de salida en bytes
Archivo1 (9kb)	AES	1.9	125,348	8,240
	RSA	1.9	126,596	9,088
Archivo2 (76KB)	AES	5.6	137,612	77,680
	RSA	5.7	142,676	84,992
Archivo3 (712kb)	AES	8.3	140,812	740,464
	RSA	10.3	140,956	810,112
Archivo4 (1,011KB)	AES	10.1	142,654	1,034,432
	RSA	12.9	143,765	1,131,776
Archivo5 (10,135KB)	AES	51.9	225,460	10,378,240
	RSA	87.7	230,792	11,353,984

Fuente: Elaboración propia, basada en la simulación con el programa JCryptool.

De acuerdo a la simulación, el primer índice o parámetro de evaluación es el tiempo en segundos, véase Figura2, de acuerdo a los resultados se puede observar que para el primer archivo que pesa 9KB el tiempo que se toma para encriptar tanto con el algoritmo AES como para RSA es el mismo, no así con el segundo archivo de 76KB, aquí ya se empieza a observar una pequeña diferencia de 0.1 segundos entre el tiempo del RSA y el AES, en los siguientes archivos se puede verificar que el tiempo que toma el algoritmo RSA es mucho mayor al del AES, teniendo una diferencia considerable de 35.8 segundos en el quinto archivo de tamaño 10,135KB, por lo que se puede deducir que mientras mayor sea el volumen de información, mayor será la diferencia de tiempo entre los dos algoritmos, siendo mayor el del RSA.

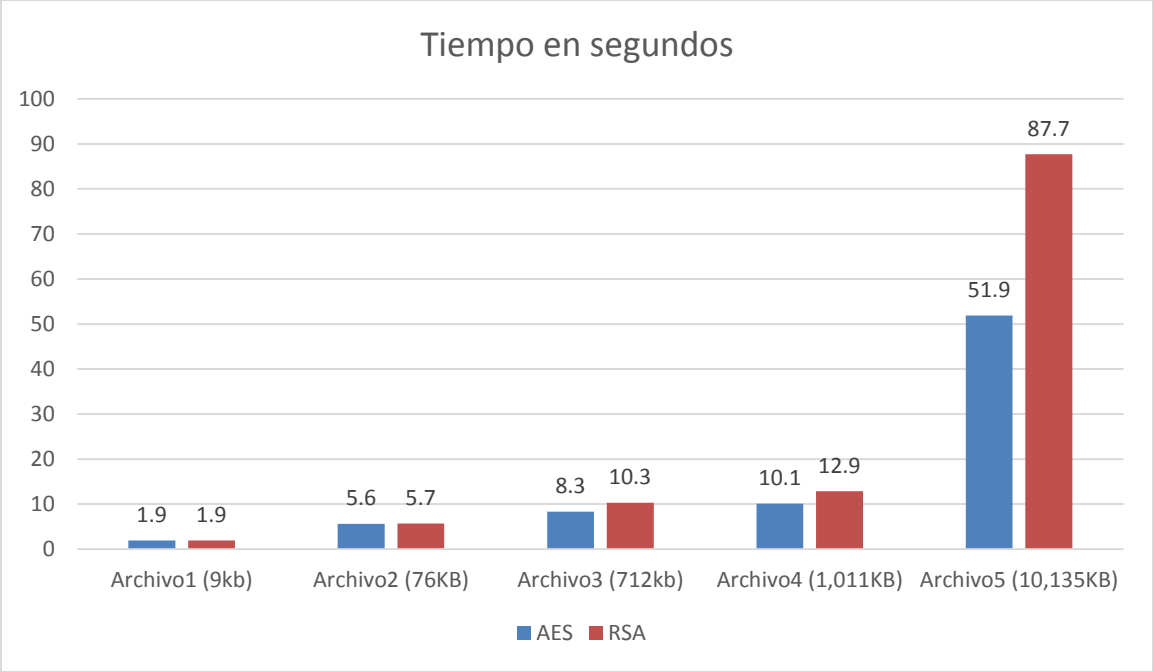

Figura2.- Resultados de la simulación en JCryptool, tiempo en segundos.
Fuente: Elaboración propia, basada en la simulación con el programa JCryptool.

El segundo índice o parámetro de evaluación es el uso de memoria, véase Figura3, de acuerdo a los resultados se puede observar que en la simulación de cifrado de todos los archivos, la encriptación con el algoritmo RSA utiliza una mayor cantidad de memoria, por lo que se deduce que este algoritmo requiere de mayor utilización de los recursos informáticos al momento de encriptar la información.

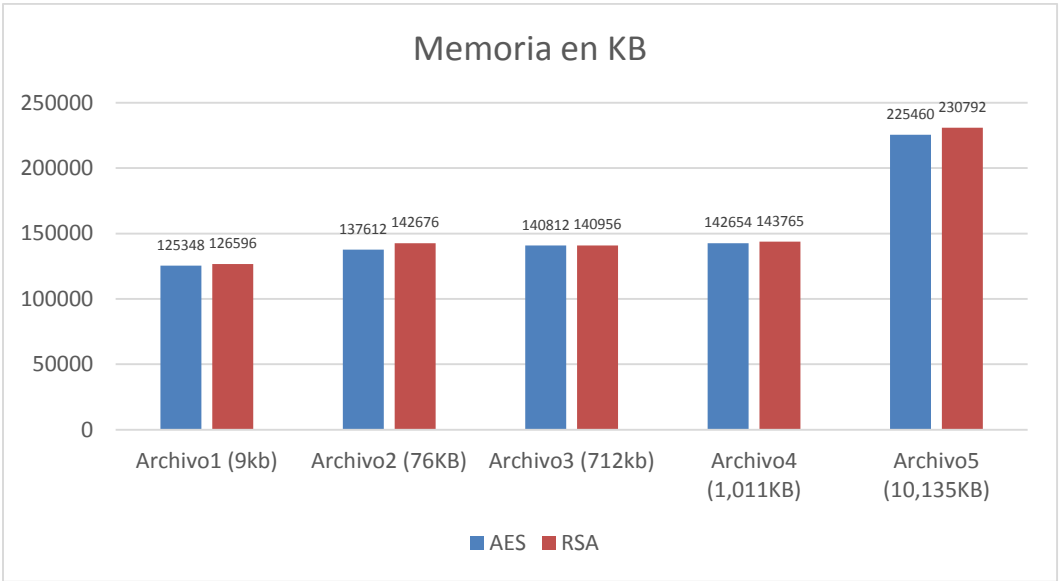

Figura3.- Resultados de la simulación en JCryptool, memoria en KB
Fuente: Elaboración propia, basada en la simulación con el programa JCryptool.

El tercer índice o parámetro de evaluación es el tamaño del archivo de salida, véase Figura4, de acuerdo a los resultados se puede observar que, al igual que en la evaluación del uso de memoria, en la simulación de cifrado de todos los archivos, la encriptación con el algoritmo RSA genera una archivo de salida de mayor tamaño que el algoritmo AES, por lo que se deduce que este algoritmo requiere de mayor espacio en disco para poder almacenar la información encriptada.

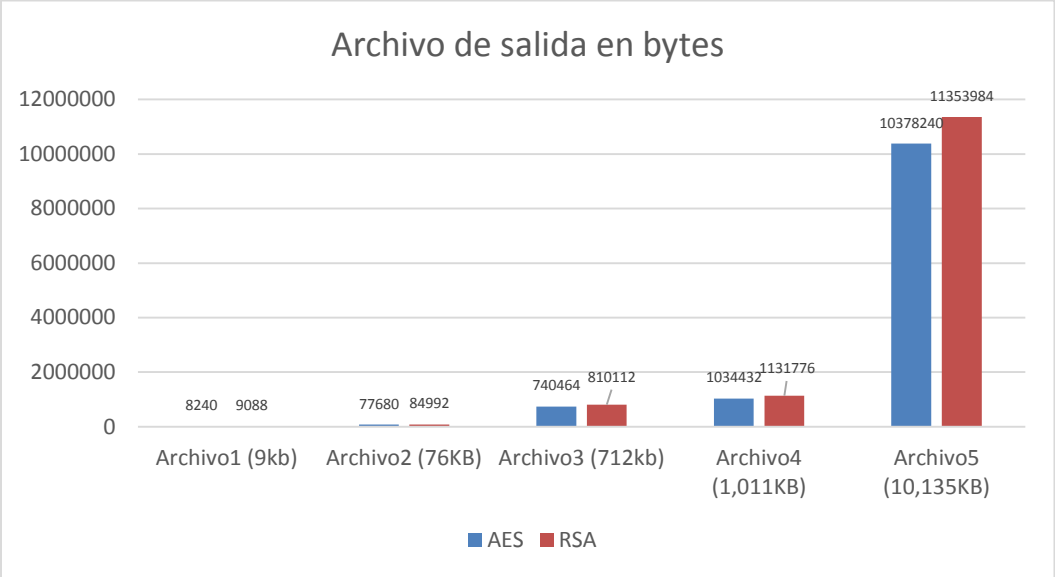

Figura4.- Resultados de la simulación en JCryptool, archivo de salida en bytes.
Fuente: Elaboración propia, basada en la simulación con el programa JCryptool.

CONCLUSIONES

Como resultado de la investigación es posible determinar que la criptografía es considerada uno de los mecanismos de seguridad más recomendados para salvaguardar la información, por lo cual es necesario investigar y ampliar el conocimiento en cuanto a la eficiencia y funcionamiento de los algoritmos criptográficos que puedan ser utilizados en cualquier organización.

Para lo cual, en esta investigación se detalla la historia, estructura, componentes, características y funcionamiento de dos algoritmos criptográficos, AES y RSA, considerados los más utilizados, estableciendo similitudes y diferencias entre ellos. Por un lado AES es un algoritmo de clave simétrica, es decir, que utiliza una clave privada para cifrar cualquier texto plano a un texto ilegible, el cual solo podrá ser descifrado por la persona que posea dicha clave.

Por otro lado, RSA es un algoritmo criptográfico de clave asimétrica donde cada participante tiene una clave pública y una privada, y todas las claves públicas de todos los participantes pueden ser compartidas, de tal forma que el remitente pueda encriptar el mensaje con la clave pública del receptor para que éste sea el único que pueda descifrar el mensaje.

De modo que, este estudio permitió realizar una simulación de cifrado de cinco archivos de texto de diferentes tamaños, utilizando los algoritmos seleccionados, a través de un software de uso libre llamado JCryptool, lo cual permitió verificar el comportamiento de los mismos, basado en la observación, medición e interpretación cuidadosa de los resultados, obtenidos de la evaluación de los siguientes parámetros: tiempo de cálculo, uso de memoria y bytes de salida.

Basándose en los resultados de la simulación se establece que el tiempo de cálculo del algoritmo RSA es mayor comparado con el tiempo del algoritmo AES en los archivos de tamaño 76 KB, 712 KB, 1011 KB, 10135 KB, lo cual no sucede en el archivo de 9 KB, ya que el tiempo de cálculo de ambos algoritmos es el mismo, esto es, que el tiempo de cifrado utilizado por el algoritmo RSA incrementa, conforme va aumentando el peso del archivo o el volumen de la información.

Lo mismo acontece con los otros parámetros de evaluación, en donde el uso de memoria es mayor al momento de cifrar los archivos con el algoritmo RSA, en comparación con el uso de memoria al cifrarlos con el algoritmo AES. De la misma manera, la cantidad de bytes aumenta en los archivos de salidas cuando son encriptados mediante el algoritmo RSA, mientras que con el AES, disminuye.

Por lo tanto, de acuerdo a los resultados obtenidos en esta simulación y a los estudios previos, se concluye que las fortalezas del algoritmo AES, es su velocidad, su bajo uso de memoria y de espacio en disco, en comparación con el algoritmo RSA, por lo tanto, AES tiene un mejor rendimiento y puede garantizar una mejor seguridad, para ser implementado en la institución de Guayaquil, objeto de este estudio.

De esta manera, este trabajo de investigación cumple con su objetivo propuesto, realizar una comparación entre los algoritmos seleccionados y demostrar sus fortalezas, pero puede ser referente para trabajos futuros que podrían analizar la relación entre rendimiento y seguridad, tomando en consideración aspectos con mayor complejidad, como por ejemplo, analizar qué algoritmo contiene rondas más complejas y en mayor cantidad, para determinar el algoritmo más seguro. Además, se puede incluir simulaciones con archivos de imágenes y audio, lo cual abarcará un mayor alcance y se enfocará en analizar y mejorar el tiempo de cifrado y tiempo de descifrado.

A pesar de todo, este trabajo también presentó sus limitaciones y es que a pesar de todas las pruebas establecidas, todavía existen algunos investigadores que son escépticos a las simulaciones, puesto que consideran que muchas veces el ambiente de prueba en el que se realizan las simulaciones no cumple con los requisitos necesarios para asemejarse al ambiente de producción, por lo que los investigadores a menudo prefieren los enfoques descriptivos de las experiencias pasadas, a los métodos que prueban teorías o hipótesis a partir de una simulación. Por lo que se sugiere continuar con los trabajos futuros detallados anteriormente, para que este escepticismo disminuya.

Finalmente, se concluye que todas las organizaciones deben considerar la criptografía como una de las herramientas esenciales para asegurar la información y establecer más estudios y análisis para entender el funcionamiento, estructura y características de los algoritmos que puedan utilizar.

También es necesario establecer campañas de difusión e investigación para mejorar en el conocimiento de los algoritmos criptográficos, para que puedan escoger y administrar correctamente las funcionalidades y aprovechar los beneficios y ventajas que éstos ofrecen, al momento de su implementación.

Referencias Bibliográficas

Ahmad Milad, A., & Zaiton Muda, H. (2012). Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack). Journal of Computer Science, 91-97.

Asole, P. S., & Mundada, M. S. (2013). A Survey on Securing Databases From Unauthorized Users. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 228-230.

Bellare, M., & Rogaway, P. (2005). Introduction to Modern Cryptography. San Diego: University of California at San Diego.

Bhanot, R., & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications, 289-306.

Bisht, N., & Sapna, S. (2015). A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms. International Journal of Innovative Research in Science, Engineering and Technology, 1028-1031.

Blaze, M. (1996). Cryptography Policy and the Information Economy. Murray Hill: AT and T Labs Research.

Brocade Communications Systems, Inc. (2013). Encryption Solution Design and Deployment Considerations. ADX.

Calderbank, M. (2007). The RSA Cryptosystem: History, Algorithm, Primes. Chicago: math.uchicago.edu.

CERT Australia. (5 de 12 de 2015). CERT Australia. Obtenido de CERT Australia: https://www.cert.gov.au/system/files/614/691/2015-ACSC-Cyber-Security-Survey-Major-Australian-Businesses.pdf

Dankhe, G. (1986). Investigación y comunicación. México D.F.: McGraw Hill.

Darwish, H. (2015). Cryptographic Algorithms (AES, RSA). Pomona: California State Polytechnic University.

Deshpand, A. (2012). eDBCrypto: A Database Encryption System using Query Level Approach. International Journal of Computer Applications (0975 – 8887), 27-32.

Diffie, W., & Hellman, M. (1976). Nueva dirección en criptografía. Nueva dirección en criptografía.

Goldwasser, S., & Bellare, M. (2008). Lecture Notes on Cryptography. San Diego: D'Ippolito.

Grofig, P., Hang, I., Harterich, M., & Kerschbaum, F. (2012). Privacy By Encrypted Databases. Karlsruhe, Germany.

Gupta, V. (2012). Advance cryptography algorithm for improving data security. International Journal of Advanced Research in Computer Science and Software Engineering, 1-5.

Hakan, H., Balakrishna, R. I., & Sharad, M. (2004). Effcient execution of aggregation queries over encrypted relational databases. DASFAA.

Hernández, R., Fernández, C., & Baptista, P. (2010). Metodología de la Investigación. Ciudad de México: McGraw Hill.

IBM. (15 de diciembre de 2016). IBM Security. Obtenido de IBM Security: http://www-03.ibm.com/security/data-breach/

Jackson, J. (19 de Agosto de 2011). PCWorld. Obtenido de AES proved vulnerable by Microsoft researchers: http://www.pcworld.idg.com.au/article/397769/aes_proved_vulnerable_by_microsoft_researchers/

K.U. Leuven. (2011). K.U. Leuven E-NEWSLETTER. Obtenido de Researchers identify first flaws in the Advanced Encryption Standard: http://www.kuleuven.be/english/newsletter/newsflash/encryption_standard.html

Karule, K., & Nagrale, N. (2016). Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security. International Journal of Scientific Engineering and Applied Science, 495-498.

Kaur, P., & Arora, N. (2015). A Comprehensive Study of Cryptography and Digital

Signature. International Journal of Computer Science Engineering and Technology(IJCSET), 1-5.

Kayarkar, H. (2012). Classification of Various Security Techniques in Databases and their Comparative Analysis. Navi, Bumbai: College of Engineering and Technology.

Kolhe, N., Raza, N., & Patheja, P. (2013). A New Approach of Cryptography for Database SecurityA New Approach of Cryptography for Database SecurityA New Approach of Cryptography for Database Security A New Approach of Cryptography for Database Security A New Approach of Cryptography for Database S. International Journal of Emerging Technology and Advanced Engineering, 226-229.

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security, 14-22.

Makhmali, A., & Mat Jani, H. (2013). Comparative Study On Encription Algorithms. International Journal of Scientific & Technology Research, 42-48.

Marcella, A. (2014). Encryption Essentials. Internal Auditor, 55-59.

Martínez, S., Mateu, V., Tomás, R., & Valls, M. (2007). Criptografía ordenable para bases de datos. Universitat de Lleida.

McDonald, N. G. (2009). PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION. Utah: University of Utah.

Mehrotra, S., & Mishra, R. (2011). Comparative Analysis Of Encryption Algorithms For Data Communication. IJCST, 292-294.

Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

Miklau, G., & Suciu, D. (2012). Controlling Access to Published Data Using. Seattle: University of Washington.

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2000). Report on the Development of the Advanced Encryption Standard (AES). National Institute of Standards and Technology.

NIST. (1997). Proceso de selección de un algoritmo de cifrado de clave simétrica. Proceso de selección de un algoritmo de cifrado de clave simétrica.

NIST. (1998). Aceptación de quince algoritmos candidatos. Aceptación de quince algoritmos candidatos.

NIST. (26 de 11 de 2001). AES. AES.

nuBridges, Inc. (2008). Best Practices in Encryption Key Management & Data Security. Atlanta: U.S. HEADQUARTERS - EMEA HEADQUARTERS.

Padmavathi, B., & Ranjitha, S. (2013). A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique. International Journal of Science and Research (IJSR), 170-174.

Paraskevo, Z., & Gianna, N. (2013). Database Security & Cryptography. Athens: University of Athens.

Pawar, S., Tandel, L., Zeple, P., & Sonawane, S. (2015). Survey of Cryptography Techniques for Data Security. International Journal of Computer Science Engineering and Technology(IJCSET), 27-30.

Peltier, T. R. (2013). Information Security Fundamentals, Second Edition. CRC Press.

Pita, S. (1996). Correlación frente a causalidad. JANO, 59-60.

Prajapati, P., Patel, N., & Macwan, R. (2014). Comparative Analysis of DES, AES, RSA Encryption Algorithms . International Journal of Engineering and Management Research, 132-134.

Princy, M. (2007). Secure Database Access and Transfer Using Public Key Cryptography. International Journal on Recent and Innovation Trends in Computing and Communication, 674 – 678.

PWC. (6 de 12 de 2015). PWC. Obtenido de PWC: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

Rafiq, M. (2014). Database Security Threats and Its Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 183-192.

Rivest, R., Shamir, A., & Adleman, L. (1976). RSA. RSA.

Robling Denning, D. E. (1983). Cryptography and Data Security. Addison-Wesley Reading .

Saranya, V., & Phani Krishna, C. (2013). A Study on Encoding and Security in the Databases. International Journal of Emerging Science and Engineering (IJESE), 52-57.

Singh, J. (2013). A Database Encryption Technique to Enhance Security Using Hill Cipher Algorithm. International Journal of Engineering and Advanced Technology (IJEAT), 660-664.

Stallings, W. (2011). Cryptography and Network Security Principles and Practice. New York: Pearson.

Vellaiyan, P., Alagarsamy, J., & Krishnan, K. (2012). Comparative Analysis of Performance Efficiency and Security Measures of some encryption algorithms. International Journal of Engineering Research and Applications (IJERA), 3033-3038.

Verizon . (1 de Diciembre de 2016). Verizon Enterprise Solutions. Obtenido de Verizon Enterprise Solutions: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Verma, A., Guha, P., & Mishra, S. (2016). Comparative Study of Different Cryptographic Algorithms. International Journal of Emerging Trends & Technology in Computer Science, 58-63.

Vinda, E. (2013). Algoritmo AES. Ciudad de Panamá: Universidad Tecnológica de Panamá.

Zulkifli, M. Z. (17 de Enero de 2007). Evolution of Cryptography. Obtenido de Evolution of Cryptography: https://idazuwaika.files.wordpress.com/2008/06/evolution_of_cryptorgarphy.pdf