MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Análisis y comparación de dos algoritmos de cifrado simétrico en plataformas Windows

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

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Thruman Wladimir CARRERA ALBÁN.

Bajo la dirección de:
Rayner Stalyn DURANGO ESPINOZA.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Febrero del 2016

Análisis y comparación de dos algoritmos de cifrado simétrico en plataformas Windows.

Analysis and comparison of two symmetric encryption algorithms on Windows platforms.

Thruman Wladimir CARRERA ALBÁN[1]
Rayner Stalyn DURANGO ESPINOZA[2]

Resumen

El objetivo principal que guía el diseño de cualquier algoritmo de cifrado debe ser la seguridad contra ataques no autorizados. Sin embargo, para todas las aplicaciones prácticas, el rendimiento y la velocidad también son preocupaciones importantes. Estas son las dos características principales que diferencian un algoritmo de cifrado de otro. Este documento proporciona la comparación de rendimiento entre dos de los algoritmos de cifrado más utilizados: AES (Rijndael) y Blowfish. La comparación se ha realizado mediante la ejecución del cifrado para procesar varios tamaños de archivos y evaluar la velocidad de cifrado/descifrado del algoritmo en diferentes versiones de la plataforma Windows para estaciones de trabajo. La simulación se ha realizado utilizando una herramienta de cifrado de archivos que nos permite elegir entre los algoritmos AES y Blowfish en máquinas virtuales de sistemas operativos Windows 7, Windows 8.1 y Windows 10, determinando así la influencia del sistema operativo en la velocidad de cada uno de los algoritmos elegidos, se ha concluido que Windows 10 acelera significativamente el cifrado y descifrado de archivos ya sea con AES o Blowfish.

Palabras clave: | Criptografía, Algoritmos, AES, Blowfish.

Abstract

The main purpose guiding the design of any encryption algorithm should be security against unauthorized attacks. However, for all practical applications, performance and speed are also important concerns. These are the two main features that differentiate one encryption algorithm from another. This document provides the performance comparison between two of the most commonly used encryption algorithms: AES (Rijndael) and Blowfish. The comparison has been made by running encryption to process various file sizes and evaluating the encryption / decryption speed of the algorithm in different versions of the Windows platform for workstations. The simulation was done using a file encryption tool that allows us to choose between AES and Blowfish algorithms in virtual machines operating systems Windows 7, Windows 8.1 and Windows 10, thus determining the influence of the operating system on the speed of each of the algorithms chosen, it has been concluded that Windows 10 significantly accelerates the encryption and decryption of files with either AES or Blowfish.

Key words | Cryptography, Algorithms, AES, Blowfish.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail tcarrera@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. E-mail: rdurango@uees.edu.ec.

1.- INTRODUCCIÓN

Hoy en día la privacidad es un aspecto muy importante para usuarios de estaciones de trabajo. Y es que debemos estar preparados para las veces en que los delincuentes informáticos se apoderan de nuestra información privada y puedan manipularla y/o divulgarla sin consentimiento del usuario. Motivo por el cual los usuarios se vuelven más interesados en proteger esa información usando algún método tecnológico como el caso del cifrado de archivos, evitando el acceso a su información aunque haya sido sustraída.

De esta manera, muchas herramientas de cifrado son ampliamente disponibles y se utilizan en la seguridad de la información, tal como lo hace uno de los sistemas operativos más comunes en nuestro entorno como lo es Windows en cada una de sus versiones de la última década. Estas herramientas utilizan los algoritmos más utilizados y eficientes hasta la actualidad ya sean simétrico (llave privada) o el cifrado asimétrico (llave pública). En el cifrado de clave simétrico o cifrado de clave secreta, sólo se utiliza una clave para cifrar y descifrar datos.

Las llaves juegan un papel importante al cifrar los datos. La fuerza de cifrado de clave simétrica depende del tamaño de la clave utilizada, es decir una clave pequeña es considerada una llave débil y fácil de descifrar, mientras que una clave más grande es difícil de romper que la realizada con la clave más pequeña. Hay muchos ejemplos de claves fuertes y débiles de algoritmos de criptografía como RC2, DES, 3DES, RC6, Blowfish, y AES.

Cualquier persona con una potente herramienta de ataque, puede penetrar en un sistema y apoderarse de nuestros archivos, y si no se ha optado por cifrarlos, los delincuentes informanticos no sólo se apoderaran de estos archivos, sino también de la información que contengan dentro. La elección del tipo de algoritmo de cifrado será entonces una elección de compromiso entre velocidades de cifrado, seguridad ofrecida y tipo de dato a cifrar (entre otras cosas), por ejemplo un cifrado seguro suele consumir más recursos de la CPU que un cifrado menos seguro.

En este artículo se realiza un análisis comparativo de Blowfish y AES en diferentes plataformas Windows, cabe recalcar que a partir de Windows Vista, todas las siguientes versiones cuentan con sus propias herramientas de cifrado. En este análisis se muestra el algoritmo más adecuado en el entorno mediante herramientas que calculan el tiempo de cifrado en segundos de cada algoritmo con un mismo tipo archivos de video. La medida de rendimiento de los esquemas de cifrado se llevará a cabo en términos de cambio de versión del sistema operativo, utilizando varios tamaños de paquetes y la clave para los algoritmos criptográficos seleccionados.

Trabajos relacionados

Existen diversos estudios de investigación que comparan entre el rendimiento de los algoritmos de cifrado comunes, entre ellos DES, Triple DES, AES, RC5, Blowfish, TWOFISH, Threefish e IDEA son algoritmos de cifrado de clave simétrica. Estos trabajos están basados en diferentes parámetros y los compararon para elegir el mejor algoritmo de cifrado de datos. Han descubierto que cada algoritmo tiene sus propias ventajas de acuerdo con los diferentes parámetros (Ruangchaijatupon & Krishnamurthy, 2001).

Un estudio realizado se lleva a cabo para diferentes algoritmos de clave secreta populares como DES, AES y Blowfish (Nadeem A. , 2006). Se comparó el rendimiento mediante el cifrado de archivos de entrada de diferentes contenidos y tamaños (Hirani, 2003).

Además, se ha realizado una comparación entre algoritmos de cifrado (AES, DES, 3DES y, RC2, Blowfish, RC6) en diferentes configuraciones con diferentes tamaños de bloques de datos de diferentes tipos de datos, tiempo de CPU, y diferente tamaño de la clave. Los algoritmos fueron probados en dos plataformas de hardware diferentes (Abd Elminaam, Abdual Kader, & Hadhoud, 2010).

En Nadeem (2005) se implementaron los algoritmos de claves secretas populares, incluyendo DES, 3DES, AES (Rijndael), Blowfish, y su rendimiento se comparó mediante el cifrado de archivos de entrada de diferentes contenidos y tamaños. Los algoritmos se implementaron en un lenguaje uniforme (Java), utilizando sus especificaciones estándar, y se probaron en dos plataformas de hardware diferentes para comparar su rendimiento.

2.- MARCO TEÓRICO

El cifrado es el proceso de convertir el texto sin formato "descubierto" en un texto críptico "oculto" para protegerlo contra los ladrones de datos.

Criptografía

La criptografía es el arte y la ciencia de la codificación de datos para que pueda viajar a cualquier lugar sin la amenaza de robo en el camino. Según Joux (2009) en la criptografía, la función básica de cifrado es la codificación de un mensaje (texto sin formato) en otro mensaje (texto cifrado) difícil de entender si es interceptado por entidades no autorizadas.

Esta ciencia se clasifica básicamente en dos categorías: simétrica y asimétrica. La criptografía simétrica es para codificar y decodificar datos con la misma llave única, mientras que la criptografía asimétrica funciona con un par de llaves, una llave codifica los datos y con la otra se puede decodificar. Los sistemas de cifrado simétrico son de dos tipos: Bloque y Flujo. Los cifrados en bloque cifran un bloque fijo de bits a la vez y los cifrados de flujo lo hacen poco a poco. En Schneier (2003.), se menciona que los cifrados de bloque son fundamentales en la construcción para los sistemas criptográficos.

Ciclo de vida

El ciclo de vida de la criptografía simétrica se inicia principalmente con DES (Data Encryption Standard). En 1977, la presentación de IBM Lucifer (Feistel), adoptado como DES (Diffie & Hellman, 1977) por NBS (National Bureau of Standards) ahora NIST (Instituto Nacional de Estándares y Tecnología). Desde su evolución, muchos criptoanalistas han intentado romperlo y finalmente fue roto en solo 22 horas en el año 1998.

Por otra parte existía la necesidad de un nuevo estándar de cifrado, entonces NIST realizó un concurso y fueron seleccionados 15 algoritmos como finalistas en la primera ronda, CAST fue uno de ellos. En la segunda ronda fueron 5 finalistas, uno era Twofish que es el descendiente de Blowfish. Por último, Rijndael ganó la competencia convirtiéndose en el algoritmo AES (Advanced Encryption Standard) en 2001 (Daemen & Rijmen, 1999).

El secreto de la fuerza del algoritmo de cifrado se basa en la clave, la longitud de la clave, el vector de inicialización, y la forma en que todos trabajan juntos (Abd Elminaam, Abdual Kader, & Hadhoud, 2010). Supongamos que si la llave se puede romper en tres horas utilizando un procesador de doble núcleo, se debe tener en cuenta que el cifrado no es fuerte en lo absoluto, pero si la llave se rompió con miles de sistemas de multiprocesamiento en muchos años, entonces el cifrado es considerablemente fuerte.

Cifrado de bloque

En criptografía, un cifrado de bloque es un cifrado de clave simétrica que opera en grupos de longitud fija de bits, denominados bloques, con una transformación invariable. Durante el cifrado, un cifrado de bloques podría tomar (por ejemplo) un bloque de 128 bits de texto plano como entrada, y emite un bloque de 128 bits de texto cifrado. La transformación exacta es controlada utilizando una segunda entrada - la clave secreta (Aos, Naji, Hameed, Othman, & Zaidan, 2009). El descifrado es similar: el algoritmo de descifrado que contenga en este ejemplo, un bloque de 128 bits de texto cifrado junto con la clave secreta, obteniendo el bloque de 128 bits original de texto plano.
Para cifrar los mensajes más largos que el tamaño del bloque (128 bits en el ejemplo anterior), se utiliza el modo de operación. Los cifrados en bloque puede ser contrastados

con cifras de flujo; un cifrado de flujo opera en dígitos individuales a la vez y la transformación varía durante el cifrado. La distinción entre los dos tipos no siempre es clara: un cifrado de bloques, cuando se utiliza en ciertos modos de operación, actúa efectivamente como un cifrado de flujo.

Blowfish

Fue diseñada en 1994 por Bruce Schneier, que funciona en unidades de 64 bits con longitudes de clave de 32 bits hasta 448 bits (Schneier, 1995). Cada bloque de 64 bits se divide en dos de 32 bits, cifrando cada bloque mediante la realización de 16 rondas de cifrado. Básicamente, el algoritmo consta de dos partes: una parte de clave de expansión y una parte de cifrado de datos.

Una clave de expansión convierte una clave de máximo 448 bits en varias matrices de subclave con un total de 4168 bytes. El proceso de generación de sub-claves tiempo-consumido añade una complejidad considerable para un ataque de fuerza bruta. Las sub-claves son demasiado largas para ser almacenadas en una cinta masiva, por lo que tendrían que ser generados por una máquina de formación de grietas como se requiere por fuerza bruta.

La búsqueda exhaustiva del espacio de claves podría ser la forma eficaz de romper, porque el propio diseñador admite la existencia de claves débiles. Pero hasta ahora nadie ha tenido éxito en la resistencia a la rotura completa del cifrado con Blowfish. Blowfish es patentado y de licencia libre, y está disponible gratuitamente para todos los usos. A pesar de que sufre de problema llaves débiles, ningún ataque es conocido por ser exitoso en contra de ella (Schneier, 1996) (Nadeem, 2005).

AES

El Advanced Encryption Standard (AES), también conocido como Rijndael (Daemen & Rijmen, 2003), es una especificación para el cifrado de datos electrónicos establecidos por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) en el 2001. AES se basa en el cifrado Rijndael desarrollado por dos criptógrafos belgas,
Joan Daemen y Vincent Rijmen, quienes presentaron una propuesta al NIST durante el proceso de selección de AES (Daemen & Rijmen, 2003).
Se basa en un principio de diseño conocido como una red de permutación de sustitución, combinación de sustitución y permutación, y es rápido tanto en software como en hardware. A diferencia de su predecesor DES, AES no utiliza un Feistel. AES es una variante de Rijndael que tiene un tamaño de bloque fijo de 128 bits y un tamaño de clave de 128, 192 o 256 bits. Por el contrario, la especificación de Rijndael por sí se especifica con tamaños de bloque y clave que pueden ser cualquier múltiplo de 32 bits, ambos con un mínimo de 128 y un máximo de 256 bits (Schneier, y otros, 2000).

Durante el proceso de cifrado - descifrado, el sistema AES va a través de 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits, y 14 rondas para llaves de 256 bits con el fin de entregar el texto cifrado final o para recuperar el texto sin formato original (Mr. Singh, Mr. Singla, & Mr. Sandha, 2011)

AES ha sido adoptada por el gobierno de los Estados Unidos y ahora se utiliza en todo el mundo. Sustituye a Data Encryption Standard (DES), que fue publicado en 1977 (Westlund, 2002). El algoritmo descrito por AES es un algoritmo de clave simétrica, lo que significa que la misma clave se utiliza para cifrar y descifrar los datos.

Hay muchas trampas para evitar cuando se implementa el cifrado, y se generan las claves. Es necesario asegurarse de todos y cada una de las implementaciones de seguridad, pero es difícil ya que requiere un cuidadoso examen por los expertos. Un aspecto importante de la evaluación de cualquier aplicación específica es determinar que dicho examen se ha realizado, o puede ser llevado a cabo (Naji, y otros, 2009), (Hamdan, Hamnid, Zaidan, & Zaidan, 2010).

Cifrando datos en los sistemas operativos

En una computadora aislada, el sistema operativo puede determinar de manera fiable quienes son el emisor y el receptor de todas las comunicaciones e interprocesos, ya que el sistema operativo controla todos los canales de comunicaciones de la computadora. La protección de la información en un sistema operativo mejora notablemente con el sistema de cifrado ya incorporado en algunas versiones de Windows.

Cifrando los archivos en Windows

Si lo que se desea es tener cada uno de los archivos cifrados de forma individual, se puede utilizar el Sistema de Archivos de Cifrado (EFS) incluido en la plataforma Windows. El sistema de archivos de cifrado es una de las muchas nuevas características a partir del sistema operativo Windows 2000 (Microsoft, 2006). EFS trabaja utilizando una inteligente mezcla de cifrado simétrico y asimétrico.

Ambas tecnologías de cifrado tienen sus fortalezas y debilidades. Microsoft intenta sacar provecho de los puntos fuertes al tiempo que hace que las debilidades sean irrelevantes. En este sentido Microsoft a partir de las versiones de Windows 7 y Windows Server 2008 R2, indica que *"EFS es compatible con los algoritmos de cifrado estándar del sector incluido el Estándar de cifrado avanzado (AES), el algoritmo hash seguro (SHA), el cifrado de curva elíptica (ECC), el cifrado basado en tarjetas inteligentes y otras características."* (Microsoft, 2010)

Cifrado completo de Disco en Windows

Microsoft con la versión Windows Vista incorpora la tecnología BitLocker como parte de un enfoque estratégico para asegurar datos móviles a través de la tecnología de cifrado. Los datos de una computadora perdida o robada son vulnerables al acceso no autorizado, ya sea ejecutando una herramienta de ataque de software contra ella o transfiriendo el disco duro de la computadora a otra computadora. BitLocker ayuda a mitigar el acceso a datos no autorizados en equipos perdidos o robados antes de que el sistema operativo se inicie, cifrando nuestro disco duro completamente así como también cualquier partición o unidad extraíble USB (Bitlocker To Go) (Microsoft, 2014). Además, BitLocker admite dos niveles de fuerza de cifrado: BitLocker con 128 bits y 256 bits. Ambos utilizan el Advanced Encryption Standard (AES) para realizar el cifrado.

Las claves de cifrado más largas proporcionan un mayor nivel de seguridad y tienen menos probabilidades de ser atacadas con éxito por el uso de métodos de fuerza bruta. Sin embargo, las claves más largas pueden causar un cifrado y descifrado más lento de los datos. En algunos equipos, el uso de claves más largas podría resultar en una notable degradación del rendimiento. Puede utilizar Directiva de grupo (Group Policy) de Active Directory para cambiar la longitud de la clave de cifrado utilizada por BitLocker.

Además, BitLocker admite un algoritmo difusor para ayudar a proteger contra los ataques de manipulación de cifrado, una clase de ataques en los que se realizan cambios en los datos cifrados en un intento de descubrir patrones o debilidades. De forma predeterminada, BitLocker utiliza cifrado AES con claves de cifrado de 128 bits y un algoritmo difusor (Microsoft, 2009). También puede seleccionar cifrado sin un algoritmo difusor mediante la directiva de grupo siempre y cuando la organización cumpla con el Estándar Federal de Procesamiento de Información (FIPS).

3.- METODOLOGÍA.

Para este trabajo se toma como referencia los trabajos relacionados y mencionados en la introducción, para lo cual se aplica un análisis cuantitativo y así establecer los factores determinantes que serán considerados para la propuesta de análisis comparativo. Se pretende analizar y comprobar el rendimiento de los algoritmos de cifrado simétrico AES y BLOWFISH en las versiones de la plataforma Windows de la última década.

Para el experimento, se utiliza una computadora portátil I7 de 2,50 GHz, en la que se crean tres máquinas virtuales cada una con un espacio de 20GB de disco duro, 8 GB de RAM, las cuales acogerán a tres sistemas operativos de 64 bits respectivamente como Windows 7, Windows 8.1 y Windows 10, donde se recopilan datos de rendimiento. En los experimentos, cada máquina virtual cifra un mismo tipo de archivo de video (.MKV) pero con un rango de tamaño de archivo diferente. Se consideraron los siguientes tamaños de archivo de video: 11,867 KB; 51,291 KB; 103,278 KB; 512,800 KB y 1051,988 KB. El tamaño de archivo incrementa para tener una mejor apreciación del tiempo de cifrado y descifrado.

Existe una gran cantidad de herramientas de cifrado, pero no todas cumplen con las características solicitadas para la simulación, y para efecto, se experimenta con la herramienta criptográfica Kruptos 2 Profesional en su versión Trial, ya que este software nos permite bloquear, cifrar y descifrar archivos y carpetas sensibles y/o privadas, permitiendo elegir entre los algoritmos simétricos AES y Blowfish, con un tamaño de cifrado de 256 bits (Kruptos 2, 2017).

Se recolecta los datos de dos variables: una métrica de rendimiento como el Tiempo de cifrado, equivalente al tiempo que tarda en cifrar el archivo por medio del algoritmo seleccionado a partir de un archivo sin formato y el sistema operativo Windows en las versiones antes mencionadas. El tiempo de cifrado se utiliza para calcular el rendimiento de un esquema de cifrado. Indica la velocidad de cifrado (Tamimi, 2008).

Se realiza una comparación entre los resultados de los diferentes esquemas de cifrado y descifrado seleccionados en términos de tiempo.
Se realiza un estudio sobre el efecto que causa el cambiar la versión del Sistema Operativo al momento de cifrar o descifrar un archivo.

Simulación

Los datos de cifrado y descifrado obtenidos de los archivos de video en cada uno de los Sistemas Operativos Windows. El comportamiento de los algoritmos de cifrado simétrico son analizados por separado. En la Tabla 1, Tabla 2 y Tabla 3, podemos apreciar que el tiempo de cifrado de AES y Blowfish, varían según el sistema operativo utilizado.

Tamaño	AES	Blowfish
11,867	0,22	0,34
51,291	0,97	1,67
103,278	3,44	3,23
512,800	16,2	30,27
1051,988	55,47	33,53

Tabla 1. Cifrado en Windows 7

Tamaño	AES	Blowfish
11,867	0,67	0,44
51,291	1,53	1,39
103,278	2,08	2,78
512,800	13,58	16,41
1051,988	38,08	40,86

Tabla 2. Cifrado en Windows 8.1

Tamaño	AES	Blowfish
11,867	0,42	0,20
51,291	1,08	1,64
103,278	3,03	3,78
512,800	16,77	19,97
1051,988	32,02	34,47

Tabla 3. Cifrado en Windows 10

El descifrado de estos archivos de video anteriormente cifrados, también sufren un incremento en su proceso. Tabla 4, Tabla 5 y Tabla 6.

Tamaño	AES W7	Blowfish W7
11,867	0,13	0,22
51,291	0,47	0,73
103,278	1,50	1,45
512,800	4,56	7,42
1051,988	10,97	15,09

Tabla 4. Descifrado en Windows 7

Tamaño (KB)	AES (seg.)	Blowfish (seg.)
11,867	0,13	0,20
51,291	0,45	0,73
103,278	1,06	1,64
512,800	6,00	9,03
1051,988	13,22	19,45

Tabla 5. Descifrado en Windows 8.1

Tamaño	AES	Blowfish
11,867	0,13	0,19
51,291	0,50	0,77
103,278	0,91	1,47
512,800	5,08	7,84
1051,988	11,98	15,55

Tabla 6. Descifrado en Windows 10

4.- ANÁLISIS DE RESULTADOS

Resultados de rendimiento con Windows 7

El primer conjunto de experimentos se realizó utilizando el sistema operativo Windows 7, los resultados se muestran en la figura 1. Estos resultados muestran la superioridad del algoritmo AES sobre Blowfish en términos del tiempo de procesamiento. También muestra que AES consume más tiempo de procesamiento cuando el tamaño del bloque de datos es relativamente grande.

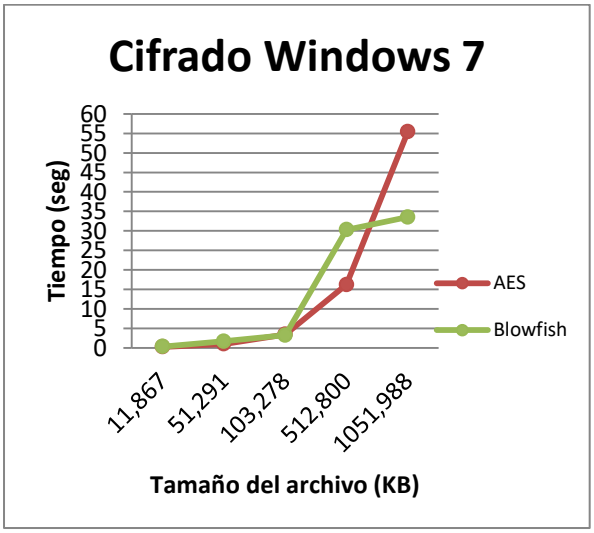

Figura 1: Resultados de Rendimiento con Windows 7

Resultados de rendimiento con Windows 8.1

Los segundos conjuntos de experimentos se realizaron usando el sistema operativo Windows 8.1, los resultados se muestran en la figura 2.

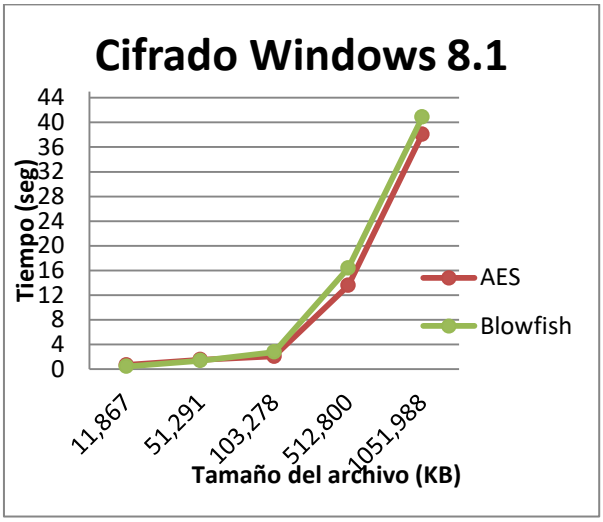

Figura 2: Resultados de Rendimiento con Windows 8.1

Como se esperaba, Windows 8.1 requiere menos tiempo de procesamiento que Windows 7 debido al consumo de recursos de estas plataformas. Los resultados indican que el tiempo adicional añadido no es significativo para muchas solicitudes, conociendo que Windows 8.1 es mucho más eficiente que Windows 7 en términos de inicio rápido (Microsoft, 2017), procesos de cifrado, entre otros (Ed Bott, 2013). La diferencia entre los dos modos es difícil de ver a simple vista porque es relativamente pequeña. Una vez más los resultados muestran la superioridad del algoritmo AES sobre Blowfish en términos del tiempo de procesamiento.

Resultados de rendimiento con Windows 10

El tercer conjunto de experimentos se llevó a cabo utilizando la plataforma Windows 10, los resultados se muestran en la figura 3. Como se esperaba Windows 10 requieren menos tiempo de procesamiento que Windows 7 y Windows 8.1. Los resultados indican que el Windows 10 es mejor que sus antecesores versiones en términos de tiempo de

procesamiento. La diferencia entre los tres sistemas operativos es difícil de ver a simple vista porque es relativamente pequeña. Se corrobora la superioridad del algoritmo de AES sobre Blowfish en términos del tiempo de procesamiento.

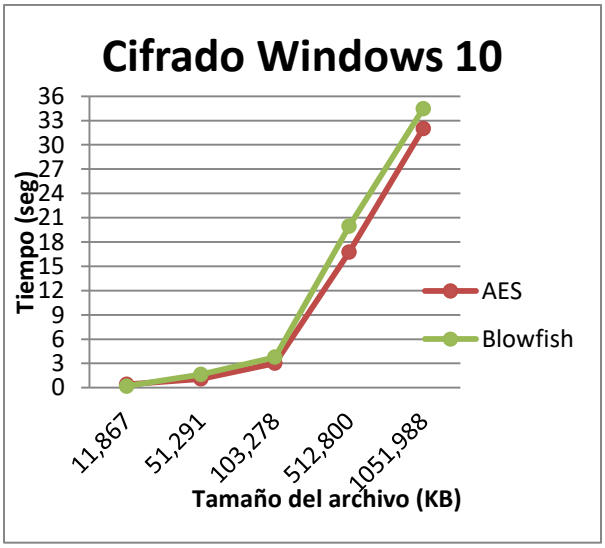

Figura 3: Resultados de Rendimiento con Windows 10

Todo lanzamiento de un nuevo sistema operativo de Microsoft, es para mejorar su rendimiento en cualquier proceso que le asignemos como se menciona en (Microsoft, 2015). El proceso de cifrado y descifrado de archivos con algoritmos simétricos no es la excepción.

5.- CONCLUSIONES Y RECOMENDACIONES

Los resultados de simulación presentados mostraron que AES tiene un mejor rendimiento que Blowfish en tiempos de procesamiento. Blowfish mostró resultados de bajo rendimiento en comparación con AES ya que requiere más potencia de procesamiento. El uso del sistema operativo Windows 7 ha añadido un tiempo de procesamiento adicional, pero en general fue relativamente insignificante, especialmente para ciertas aplicaciones que requieren un cifrado más seguro para bloques de datos relativamente grandes que afectaron al algoritmo simétrico AES. Windows 10 muestra un mejor desempeño que Windows 7 y Windows 8.1 al obtener tiempos menores a los 35 segundos con archivos de hasta 1000,000 KB.

Esta investigación ayudará analizar los tiempos que se pueden usar cuando se cifra grandes cantidades de archivos como son los ISO o también conocidos como imagen o copia de CD, DVD o Blu-Ray dentro de hipervisores, teniendo en cuenta el tipo de procesador a usarse para optimizar los tiempos cuando se lleva a cabo el cifrado y descifrado de los archivos.

En posteriores investigaciones, este análisis se puede implementar en plataformas Linux, teniendo en cuenta las diferentes distribuciones de este sistema operativo, como es el caso de Ubuntu, Centos, KDE Neon entre otros, logrando poder medir su rendimiento en el tiempo. Esto ayudaría a poder comparar datos entre diferentes plataformas de sistemas operativos.

Como índice estadístico se sugiere aplicar el Coeficiente de Correlación Intraclase (ICC) y así poder medir el nivel de concordancia para poder realizar una mejor inferencia de las mediciones asociadas a las variables cuantitativas continuas.

REFERENCIAS BIBLIOGRÁFICAS

Abd Elminaam, D. S., Abdual Kader, H. M., & Hadhoud, M. M. (2010). Evalution the Performance of Symmetric Encryption Algorithms. *International Journal of Network Security,*, 213-219.

Aos, A. Z., Naji, A. W., Hameed, S. A., Othman, F., & Zaidan, B. B. (2009). Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File. *International Conference on IACSIT Spring Conference (IACSIT-SC09)* (págs. 425-429). Advanced Management Science (AMS).

Coppersmith, D. (1994). The Data Encryption Standard (DES) and Its Strength Against Attacks. *I BM Journal of Research and Development*, 243-250.

Daemen, J., & Rijmen, V. (1999). AES Proposal: Rijndael.

Daemen, J., & Rijmen, V. (2001). Rijndael: The Advanced Encryption Standard. *Dr. Dobb's Journal*, 137-139.

Daemen, J., & Rijmen, V. (2003). AES Proposal: Rijndael. *National Institute of Standards and Technology.* .

Diffie, W., & Hellman, M. (1977). “Exhaustive cryptanalysisof the NBS data encryption standard” . En *Computer* (págs. 74-78).

Ed Bott. (2013). *Introducing Windows 8.1 for IT Professionals Technical Overview.* Washington: Microsoft Press.

El-Fishawy, N. (2007). Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms. *International Journal of Network Security*, 241–251.

Hamdan, A., Hamnid, J., Zaidan, A. A., & Zaidan, B. B. (2010). NewFrame Work of Hidden Data with in Non Multimedia File. *International Journal of Computer and Network Security*, 46-54.

Hardjono. (2005). Security In Wireless LANS And MANS. . *Artech House Publishers* .

Hirani, S. (2003). Energy Consumption of Encryption schemes in wireless device Thesis. *University of Pittsburgh*.

Joux, A. (2009). Algorithmic cryptanalysis. *CRC Press series on cryptography and network security*.

K. McKay. (2005). 'Trade-offs Between Energy and Security in Wireless Networks Thesis. *Worcester Polytechnic Institute*.

Kruptos 2. (2017). *Kruptos 2 Software*. Obtenido de Kruptos 2 profesional, Encript and Secure: http://www.kruptos2.co.uk/index.html

Microsoft. (Junio de 2006). *TechNet Magazine*. Obtenido de Microsoft: https://technet.microsoft.com/en-us/library/2006.05.howitworks.aspx

Microsoft. (30 de octubre de 2009). *Microsoft*. Obtenido de How Strong Do You Want the BitLocker Protection?: https://technet.microsoft.com/en-us/library/ee706531(v=ws.10).aspx

Microsoft. (enero de 2010). *Microsoft*. Obtenido de Cambios en EFS: https://technet.microsoft.com/es-es/library/dd630631(v=ws.10).aspx

Microsoft. (26 de marzo de 2014). *Microsoft*. Obtenido de BitLocker Countermeasures: https://technet.microsoft.com/en-us/library/dn632176(v=ws.11).aspx

Microsoft. (2015). *Windows 10*. Obtenido de Microsoft: https://www.microsoftstore.com/store/msmx/es_MX/cat/Windows/categoryID.70036100

Microsoft. (2017). *Compara versiones de Windows*. Obtenido de Microsoft: https://www.microsoft.com/es-cl/windows/compare

Mr. Singh, G., Mr. Singla, A., & Mr. Sandha, K. (2011). Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion

Detection System. *International Journal of Multidisciplinary Research*, 143-151.

Murgi. (2006). Cifrado Simétrico y Asimétrico con GPG. *Explotación de Sistemas Informáticos*.

Nadeem. (2005). A Performance Comparison of Data Encryption Algorithms. *IEEE*.

Nadeem, A. (2006). A performance comparison of data encryption algorithms. *IEEE information and communication technologies*, 84-89.

Naji, A. W., Hameed, S. A., Zaidan, B. B., Al-Kha, W. F., Khalifa, O. O., Zaidan, A. A., & Gunawan, T. S. (2009). Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advanced Encryption Standard and Distortion Techniques. *International Journal of Comput*.

Ruangchaijatupon, & Krishnamurthy, P. (2001). Encryption and Power Consumption in Wireless LANs-N. *The Third IEEE Workshop on Wireless LANs*.

Salama, D., Kader, H. A., & Hadhoud, M. (2011). Studying the Effect of Most Common Encryption Algorithms. *International Arab Journal of e-Technology*.

Schneier, B. (1995). The blowfish encryption algorithm-one year later. *Dr. Dobb 's Journal*.

Schneier, B. (1996). Applied Cryptography. *John Wiley & Sons*.

Schneier, B. (2003.). Practical Cryptography. *Wiley*.

Schneier, B. (2004). *The Blowfish Encryption Algorithm*. Obtenido de Schneier on Security: http://www.schneier.com/blowfish.html

Schwartz , J. (2000). U.S. Selects a New Encryption Technique". *New York Times*.

Stallings, W. (2005). Cryptography and Network Security 4th Ed. *Prentice Hall*, 58-309.

Tamimi, A.-K. A. (2008). Performance Analysis of Data Encryption .

Westlund. (2002). NIST reports measurable success of A dvanced Encryption Standard. *Journal of Research of the National Ins titute of Standards and Technology*.