ANÁLISIS DE LOS MECANISMOS DE ENCRIPTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN EN REDES DE COMUNICACIONES

ANALYSIS OF THE MECHANISMS OF ENCRYPTION FOR SECURITY INFORMATION IN COMMUNICATION NETWORKS

(Entregado 04/03/2016 – Revisado 03/03/2017)

PAOLA MARITZA VELASCO SÁNCHEZ

Ingeniera en Electrónica e Instrumentación de la Escuela Politécnica del Ejército, Diplomado en Didáctica de la Educación Superior de la Universidad Técnica de Cotopaxi, Magister en Redes de Comunicaciones de la Pontificia Universidad Católica del Ecuador. Docente de la Carrera de Ingeniería Eléctrica de la Universidad Técnica de Cotopaxi de 2005 a 2015. Actualmente Docente Ocasional del Departamento de Eléctrica y Electrónica de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

MARÍA SOLEDAD JIMÉNEZ JIMÉNEZ

Ingeniera en Electrónica y Telecomunicaciones de la Escuela Politécnica Nacional, Master of Science in Electrical Engineering de la Universidad de Texas & Arlington – USA. Profesora a tiempo completo en la Facultad de Ingeniería Eléctrica y Electrónica de la Escuela Politécnica Nacional desde 1988 hasta la presente fecha, docente de la Maestría en Redes de Comunicaciones de la Pontificia Universidad Católica del Ecuador.

GUSTAVO XAVIER CHAFLA ALTAMIRANO

Doctor en Telecomunicaciones – Coordinador del Programa de Maestría en Redes de Comunicaciones y Profesor Principal de la PUCE en la Facultad de Ingeniería. Actualmente vinculado a varios proyectos de Investigación ligados al Desarrollo de las Telecomunicaciones y sus diferentes aplicaciones.

Universidad de las Fuerzas Armadas – Ecuador
pmvelasco1@espe.edu.ec

Escuela Politécnica Nacional – Ecuador
maria.jimenez@epn.edu.ec

Pontificia Universidad Católica del Ecuador
gxchafla@puce.edu.ec

Resumen

Las tecnologías de la información y las comunicaciones (TIC) son cada vez más utilizadas en todos los ámbitos de la sociedad –educación, salud, comercio, investigación–. Sin embargo, la interacción entre usuarios a través de Internet, el avance tecnológico y el uso de los medios de comunicación masiva, hacen que la información que circula por la red esté expuesta a diferentes formas de ataques informáticos –suplantación de identidad, falsificación y alteración de documentos, hurto o destrucción de información–. El presente trabajo hace un análisis de los mecanismos de encriptación para garantizar la confidencialidad e integridad de la información que se transmite en las redes de comunicaciones. Dicho análisis examina el estado del arte y los

trabajos relacionados con el tema de seguridad informática, criptografía, protocolos y algoritmos criptoFiguras, normas y estándares internacionales.

Palabras Claves: *seguridad, criptografía, protocolos, algoritmos*

Abstract

Information and communication technologies (ICT) are increasingly used in all areas of society –education, health, trade, research–. However, the interaction between users on Internet, high-technological advancement and the use of the mass media, have made the information that flows through the network will be exposed to different forms of cyber-attacks –identity theft, falsification and alteration of documents, theft or destruction of information–. This paper investigates the encryption mechanisms to ensure the confidentiality and integrity of information transmitted in communication networks, and it presents a literature review and looks at some of the relevant research studies in the area of computing security, cryptography, protocols and cryptographic algorithms, international norms and standards.

Keywords: *security, cryptography, protocols, algorithms*

1. Introducción

A medida que se expanden las redes de comunicaciones, la inseguridad en los sistemas informáticos también aumenta, por lo que el término seguridad, se ha convertido en una prioridad para garantizar la transmisión de la información a través de Internet, que es el medio que ha permitido esta interconectividad. Se establece en la seguridad informática, que la criptografía es la ciencia encaminada a procurar la confidencialidad, autenticación, integridad y no repudio en la transmisión de la información, la misma que se fundamenta en las matemáticas discretas y la teoría de la información; y, tiene como objetivo proteger la información almacenada y la que se transmite por un medio de comunicación (Escrivá Gascó, Romero Serrano, & Ramada, 2013). En este trabajo se realizó una revisión teórica y bibliográfica sobre la seguridad informática y específicamente sobre los algoritmos criptoFiguras ; y, a partir de ella un análisis comparativo de los algoritmos de criptografía simétrica y asimétrica, en cuanto a velocidad de procesamiento, robustez, rendimiento y tamaño de clave, tiempo requerido para romper una clave, complejidad ciclomática, etc., para a partir de los resultados de pruebas realizadas y del análisis identificar los algoritmos de mejor desempeño y poder establecer los mecanismos de encriptación más idóneos para seguridad en redes de comunicaciones, contrastando con los resultados de la literatura técnica.

2. Materiales y métodos

Para realizar el análisis de los mecanismos de encriptación, se utilizó la revisión sistémica de la seguridad informática, criptografía, mecanismos de seguridad, aplicaciones de algoritmos de encriptación, pues de esta forma es posible identificar, evaluar, interpretar y sintetizar la información referente al tema de investigación. Además se incluyen criterios de elegibilidad al momento de presentar un análisis de rendimiento de los algoritmos de criptografía simétrica,

aplicando las herramientas de software *OpenSSL, TrueCrypt y DiskCrypt*, para la recolección de datos de la velocidad de proceso de encriptación y desencriptación de los algoritmos.

Seguridad Informática

La seguridad informática se constituye en el conjunto de políticas y mecanismos que permitan proteger los recursos de un sistema. Es así que la Unión Internacional de Telecomunicaciones (UIT-T), elaboró la recomendación *X.800* para arquitectura de sistemas abiertos; y, ha venido trabajando conjuntamente con la Organización Internacional de Estándares (ISO) en el desarrollo de nuevas recomendaciones, que permitan abordar los servicios y mecanismos de seguridad en otras arquitecturas. De acuerdo a la recomendación UIT-T. 805, se establecen 8 dimensiones de la seguridad: control de acceso, autenticación, no repudio, confidencialidad de los datos, seguridad de la comunicación, integridad de los datos, disponibilidad y privacidad (Zhao, 2006).

Seguridad en Redes Inalámbricas

Las redes inalámbricas de área local (WLAN), debido a su potencial acceso han alcanzado estándares de popularidad a nivel mundial. Sin embargo, en cuanto a seguridad se refiere, una gran mayoría son vulnerables y están expuestas a plagio por personas no autorizadas. La presencia de puntos de acceso (AP) inalámbrico en la red tiene ciertas implicaciones negativas en términos de seguridad para una determinada empresa o compañía, es decir, una persona puede fácilmente de manera intencional o no obtener información exclusiva (Andreu, Pellejero, & Lesta, 2006).

Criptografía

Etimológicamente proviene del griego κρυπτο (**Kryptos)** = secreto y ΓΡΑΦΕΙΑ (**Graphos)** = escribir, y se traduce como el arte de escribir de manera secreta. Los autores Menezes, Van Oorschot y Vanstone, manifiestan: "*La criptografía es el estudio de técnicas matemáticas relacionadas con los aspectos de la seguridad de la información tales como la confidencialidad, la integridad de datos, la autenticación de entidad y de origen. La criptografía no comprende solo a los medios para proveer seguridad de información, sino a un conjunto de técnicas"* (Menezes, Oorschot, & Vanstone, 1996).

Algoritmos criptoFiguras.- Son funciones matemáticas estructuradas como un conjunto finito de pasos, que permiten encriptar y desencriptar datos, se basan en tres principios: teoría de la información, teoría de los números y teoría de la complejidad. (Maiorano, 2009).

Criptografía simétrica.- Consiste en la distribución de una misma clave para la comunicación entre el emisor y el receptor, la clave asignada se utiliza para encriptar y desencriptar el mensaje (Buendía, 2013). Las vulnerabilidades están en mantener secreta la clave asignada a las partes, al existir mayor número de destinatarios del mensaje todos deberán conocer la clave secreta, un inconveniente es el resguardo de tantas claves, pudiendo existir problemas como: suplantación de identidad, falsificación, entre otras.(Vivas, Huerta, Zambrano, Clotet, & Satizábal, 2008). Los

algoritmos de criptografía simétrica más representativos son: DES (*Data Encryption Standard)*, TripleDES, AES (*Advanced Encryption Standar)*, IDEA (*International Data Encryption Algorithm)*, Blowfish y Twofish, RC4.

Criptografía asimétrica.- Usa dos claves (pública y privada) para el envío de mensajes. La clave pública se puede entregar a cualquier persona, la clave privada únicamente a la persona autorizada. El emisor usa la clave pública del destinatario para encriptar el mensaje, y solo la clave privada del receptor podrá desencriptarlo. (Maiorano, 2009)**.** Dentro de los algoritmos de criptografía asimétrica se tienen: RSA, El Gamal, DSA, Diffie-Hellman, Curvas Elípticas.

Herramientas de software y hardware

Para realizar una comparación entre los algoritmos de criptografía simétrica, se han aprovechado las herramientas de código abierto que cuentan con la posibilidad de analizar la velocidad de proceso en la encriptación y desencriptación a través de un *benchmark* entre los algoritmos (Alfaro, 2014; Olsson, 2012). Las mismas que se detallan a continuación:

1. *OpenSSL*[1].- Es una implementación de los protocolos SSL (Seccure Sockets Layer) y TLS (Transport Layer Security), utiliza lenguaje de programación C. Tiene versiones disponibles para los sistemas operativos Linux y Microsoft Windows, y los algoritmos criptoFiguras que implementa son: AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, TDES, GOST 28147-89, RSA y DSA.
2. *TrueCrypt*[2].- Es una aplicación disponible para los sistemas operativos Linux y Windows. Permite crear archivos encriptados a los que se puede acceder si se conoce la contraseña y/o clave que se utilizó para su creación. Trabaja con los siguientes algoritmos: Twofish, AES y Serpent –es un algoritmo de cifrado simétrico de bloques, utiliza un tamaño de bloque de 128 bits, tamaños de llave de 128, 192 y 256 bits y consta de 32 rondas–, y las posibles combinaciones entre ellos.
3. *DiskCryptor*[3].- Soporta algoritmos de encriptación AES, Twofish, Serpent, y las combinaciones entre ellos. Realiza un *benchmarking* de la velocidad de encriptación de los algoritmos. Disponible para los sistemas operativos Windows.

Para la elección del *hardware*, en el cual se instaló cada una de las herramientas, se realizó una prueba entre tres computadores, aplicando el *software OpenSSL*, que tiene un mayor número de algoritmos para procesar; y, de esta forma comparar el rendimiento entre los equipos, que poseen sistema operativo Windows 7 de 64 bits, y las siguientes características:

Tabla 1
Características de los equipos

	Computador 1	**Computador 2**	**Computador 3**
Procesador	Intel Core i7 2.1GHz	Intel Core i5 2.67GHz	Intel Core i3 1.89 GHz
Memoria RAM	8.00 GB	4.00GB	4.00GB

[1] https://www.openssl.org/
[2]https:// www.truecrypt.org/dowloads
[3] https://diskcryptor.net/

Una vez ejecutada la prueba se obtuvo como resultado que para todos los tamaños de bloque (16, 64, 256, 1024 y 8192 bytes) que se compararon, el rendimiento del computador 1 fue el mejor. En la figura 2 se muestra la evaluación de los algoritmos para un tamaño de bloque de 8192 bytes en función de las tres computadoras.

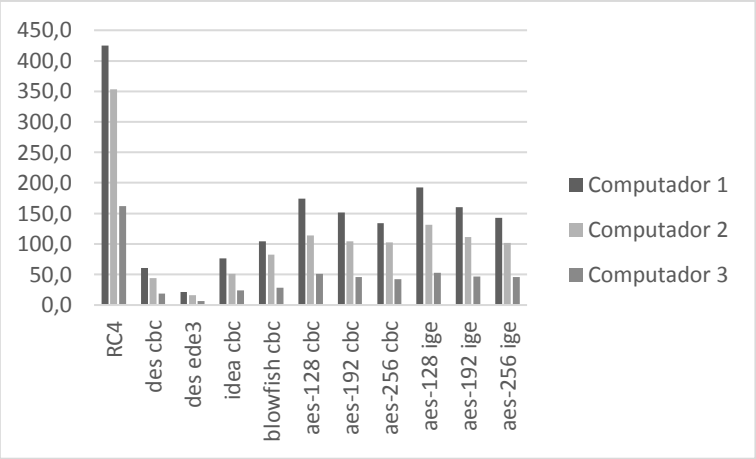

Figura 1: Rendimiento de los tres computadores utilizando OpenSSL

Es así como se determinó que debido al tiempo de ejecución en el procesamiento, la evaluación de los algoritmos se debía realizar en el computador 1, el mismo que tiene memoria RAM de 8 GB y procesador de 2,1 GHz.

3. Resultados y discusión

Análisis de los algoritmos de criptografía simétrica

Evaluación de los algoritmos de encriptación utilizando *OpenSSL*

Para realizar esta evaluación se utilizó el comando *speed* del *software*, con el cual el sistema hace una prueba de la velocidad de encriptación en megabytes por segundo (MB/s) de cada algoritmo en diferentes modos de operación (cbc, ige), variando el tamaño del bloque (16, 64, 256, 1024 y 8192 bytes) que se va a encriptar; y, en algunos casos el tamaño de la clave (AES 128, 192 y 256 bits). Con este software se comparó los algoritmos: RC4, DES, IDEA, Blowfish y AES. Los resultados son presentados en la tabla 2 y de manera gráfica en la figura 2.

Tabla 2

Velocidad de proceso en MB/s para diferentes tamaños de bloques utilizando OpenSSL

Algoritmo	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
RC4	493,3	431,8	416,4	357,4	425,1
des cbc	58,1	59,6	60,2	58,9	60,3
des ede3	22,0	20,8	21,1	21,3	21,2
idea cbc	72,7	74,6	75,5	76,7	76,0
blowfish cbc	96,4	100,7	102,8	104,0	104,4
aes-128 cbc	155,5	169,0	171,8	175,8	174,1
aes-192 cbc	139,3	147,8	149,6	150,1	151,6

aes-256 cbc	124,5	131,6	133,6	134,0	134,2
aes-128 ige	172,4	182,9	185,6	185,1	192,4
aes-192 ige	151,8	161,6	155,8	158,1	160,2
aes-256 ige	133,7	140,0	140,0	140,7	142,8

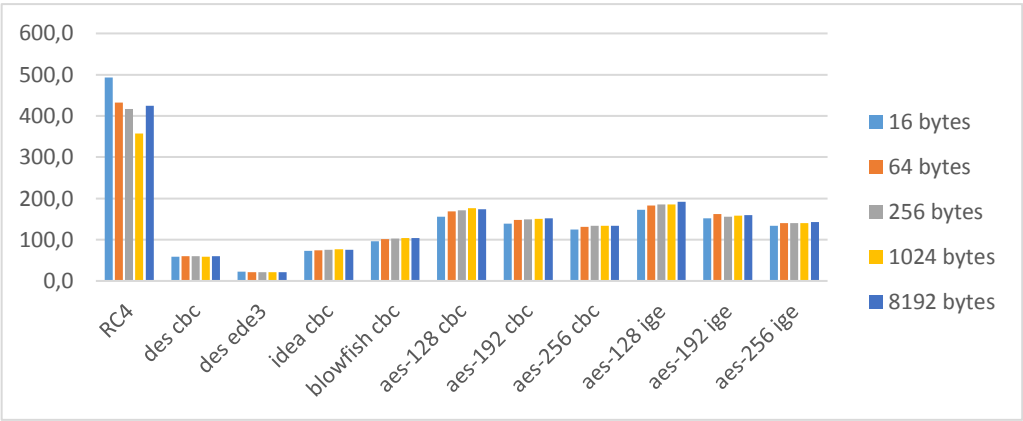

Figura 2: Velocidad de proceso en MB/s para diferentes tamaños de bloques utilizando OpenSSL

De los resultados obtenidos se puede establecer que independientemente del tamaño de bloque, el algoritmo RC4 tiene un tiempo de ejecución mayor que los otros algoritmos. En segundo lugar se encuentra AES en modo de operación ige y con tamaño de clave de 128 bits, seguido de AES en modo cbc y clave de 128 bits. En tercer lugar se encuentra Blowfish en modo cbc.

3.1.2 Evaluación de los algoritmos de encriptación utilizando TrueCrypt

El *software TrueCrypt* permite generar un *benchmark* con los algoritmos que contiene y las combinaciones entre ellos. En esta comparación se puede elegir el tamaño del *buffer* a encriptar; y, presenta las velocidades en el proceso de encriptación y desencriptación en gigabytes por segundo (GB/s) y megabytes por segundo (MB/s), además del promedio entre ellas. Para esta evaluación se consideró los algoritmos AES, *Twofish* y *Serpent* y se varió el tamaño de *buffer*. En la tabla 3 se presentan los resultados obtenidos en la evaluación de los algoritmos para tamaños de *buffer* de: 100KB, 500KB, 1MB, 50MB, 200MB, y gráficamente en la figura 3.

Tabla 3

Promedio en MB/s para diferentes tamaños de buffer utilizando TrueCrypt

Algoritmo	100 KB	500 KB	1 MB	50 MB	200 MB
AES	68,9	78,9	79,5	174	177
Twofish	67,1	71	71,4	157	159
Serpent	37,4	39,3	41,3	91,3	93,6

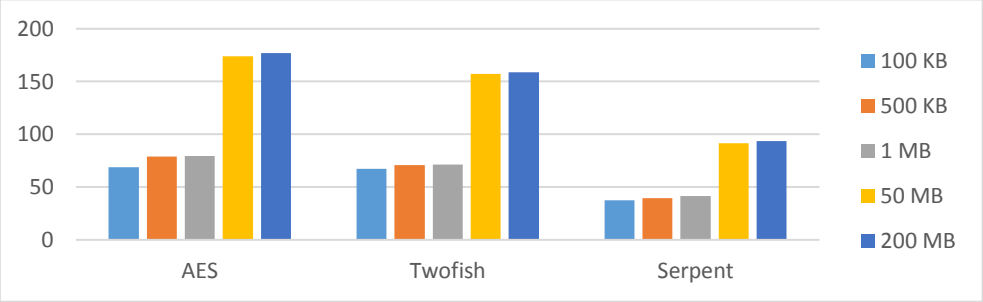

Figura 3: Velocidad promedio en MB/s para diferentes tamaños de buffer utilizando TrueCrypt

De los resultados se determina que el algoritmo AES tiene una mayor velocidad de proceso de encriptación y desencriptación para cualquiera de los tamaños de *buffer* comparados, seguido por Twofish y finalmente Serpent. Se puede diferenciar que cuando el tamaño del *buffer* está entre 100 KB y 1 MB, los valores de la velocidad no sobrepasan los 80 MB/s, mientras que cuando el tamaño está entre 50 MB y 200 MB, la velocidad se incrementa notablemente.

3.1.3 Evaluación de los algoritmos de encriptación utilizando *DiskCryptor*

Este *software* presenta entre sus herramientas un *"Encryption Benchmark*", este proceso permite determinar la velocidad de encriptación y desencriptación en megabytes por segundo (MB/s) de los algoritmos disponibles AES, Twofish y Serpent y las combinaciones entre ellos. Ya que en esta prueba no es factible manipular otra variable para la comparación, lo que se realizó es un *benchmark* con las unidades de disco. Para la evaluación se comparó cada uno de los algoritmos con el tamaño de las unidades de disco (C: 243 GB, disco D: 454 GB, disco E: 2.03MB, I: 7.2GB). Los resultados obtenidos se muestran en la tabla 4 y de forma gráfica en la figura 4.

Tabla 4
Velocidad en MB/s para diferentes tamaños de unidad de disco utilizando DiskCryptor

Algoritmo	243 GB	454 GB	2.03 MB	7.2 GB
AES	130,55	141,16	137,54	138,66
Twofish	111,29	122,32	118,92	116,07
Serpent	85,04	91,16	94,45	93,24

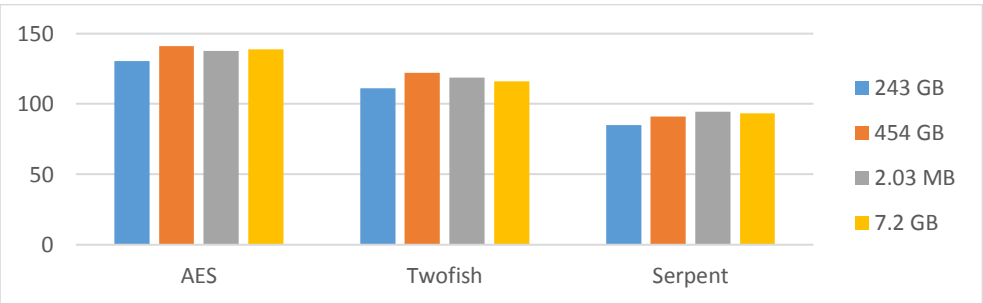

Figura 4: Velocidad en MB/s para diferentes tamaños de unidad de disco utilizando DiskCryptor

Con los resultados obtenidos, se puede observar que en este caso AES es el algoritmo con mayor velocidad de encriptación y desencriptación para todas las unidades de disco, seguido por *Twofish* y *Serpent*.

3.1.4 Análisis de la Robustez de los algoritmos

Una vez establecido que los algoritmos RC4 y AES, son los que poseen mejores características respecto a la velocidad de proceso en la encriptación y desencriptación, se realiza una comparación respecto al nivel de seguridad en la encriptación de datos en función de la robustez del algoritmo. En el caso de RC4, éste es utilizado como mecanismo de seguridad WEP, se ha determinado que las claves son descubiertas con facilidad, por lo que es considerado como un sistema de criptografía simétrica inseguro, y aceptado para usuarios domésticos y aplicaciones no críticas (Lehembre, 2006).

El algoritmo AES es utilizado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA), para el resguardo de información *"Secret"* con una longitud de clave de 128 bits; y, *"Top Secret"*, con claves de 192 o 256 bits, consideradas suficientemente seguras (Pousa, Sanz, & De Giusti, 2011). Así también, en el año 2011 descubrieron una vulnerabilidad en el algoritmo, no obstante ésta no tiene relevancia práctica debido a que es necesaria una estructura computacional que permita probar 10 millones de claves por segundo. Por lo que es un algoritmo de criptografía simétrica que garantiza un alto nivel de seguridad (Alfaro, 2014).

3.2 Análisis de los algoritmos de criptografía asimétrica

Para este análisis se han considerado, los estudios, aplicaciones e investigaciones realizadas respecto a la comparación de algoritmos de criptografía asimétrica de Carbonell (2007), Maldonado (2009), Bonilla (2012) y Alfaro (2014). Exponiendo diferentes parámetros que permitan seleccionar al algoritmo de encriptación asimétrico con mejores características de desempeño y seguridad.

3.2.1 Tamaño de la clave

El *National Institute of Standards and Technology* (NITS), muestra una tabla comparativa entre el tamaño de la clave de los algoritmos asimétricos de Curvas Elípticas (ECC) y RSA; y, el algoritmo simétrico AES. Esto debido a que en las aplicaciones se utilizan los dos tipos de algoritmos en el intercambio de claves y luego en la encriptación de la información (Carbonell, Díaz, & Mejías, 2007).

Tabla 5
Comparación entre el tamaño de clave de los algoritmos de Curva Elíptica, RSA y AES

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Fuente: *Certicom* - http://www.*certicom*.com

En la tabla 5 se muestra la relación que existe entre el tamaño de la clave en ECC y en RSA, y se puede observar una amplia diferencia entre ellas. Además se observan datos respecto a la relación de tamaño de la clave (*key size ratio)*. Por ejemplo si en AES se requiere una clave de 192 bits para el resguardo de información, se puede alcanzar el mismo nivel de seguridad usando ECC con clave de 384 bits, o RSA con clave de 7680 bits, teniendo una proporción de 1:20 entre el tamaño de ambas.

i. Rendimiento y tamaño de clave

La empresa *Certicom*[4] ha desarrollado investigaciones respecto al algoritmo ECC, a continuación se muestra una comparación respecto al tiempo de respuesta de un servidor que utiliza algoritmos RSA (con claves de 1024 y 2048 bits) y ECC (con claves de 160 y 224 bits) expresado en milisegundos (ms), las operaciones por segundo, el *ratio* –relación– de *performance* –rendimiento– y el *ratio* de tamaño de clave (Carbonell et al., 2007).

Tabla 6
Comparación de performance de RSA y ECC

	ECC-160	RSA-1024	ECC-224	RSA-2048
Tiempo (ms)	3.69	8.75	5.12	56.18
Operaciones/seg	271.3	114.3	195.5	17.8
Ratio de Performance	2.4 : 1		11 : 1	
Ratio de tamaño de clave	1 : 6.4		1 : 9.1	

Fuente: *Certicom* - http://www.*certicom*.com

De los datos expuestos en la tabla 6 se puede establecer que el algoritmo ECC tiene tiempos de respuesta y número de operaciones por segundos mejores que los presentados para RSA. Se observa que al relacionar los tamaños de las claves, ECC sigue siendo mejor que RSA, puesto que el tiempo de respuesta de un RSA-1024 es de 8.75 ms, mientras que ECC-160 tiene una respuesta de 3.69 ms. En el caso del *performance* se aprecia una mayor diferencia cuando RSA-2048 realiza 17.8 operaciones/seg; y, ECC-224 ejecuta 195.5 operaciones/seg.

ii. Tamaño de textos encriptados

Certicom presenta un análisis entre los algoritmos ECC, ElGamal y RSA, respecto al tamaño del texto encriptado considerando para el proceso un mensaje de tamaño de 100 bits (Belingueres, 2000).

Tabla 7
Tamaño de textos encriptados

Algoritmo	Tamaño de texto encriptado (bits)
RSA	1024
ElGamal	2048
ECC	321

Fuente: *Certicom* - http://www.*certicom*.com

[4] *Certicom principal empresa comercial de algoritmos de Curvas Elípticas ECC* - http://www.*certicom*.com

Esta comparación permite determinar que el algoritmo ECC tiene el tamaño de texto encriptado menor al del algoritmo ElGamal, lo que se refleja en un ahorro de ancho de banda utilizado al momento de la transmisión de mensajes encriptados.

3.2.4 Tiempo requerido para romper una clave

Respecto a los niveles de seguridad, *Certicom* presenta una curva de respuesta donde se compara dicho parámetro entre ECC, RSA y DSA

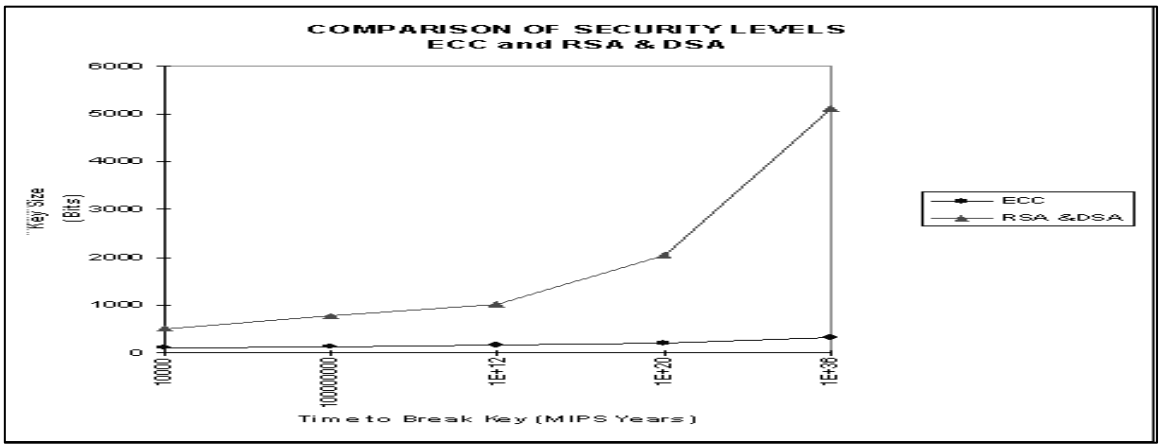

Figura 5: Comparación de los niveles de seguridad entre ECC, RSA y DSA
Fuente: *Certicom* - http://www.certicom.com

La figura 5 muestra una curva de respuesta que relaciona el tiempo requerido para romper una clave (medido en MIPS[5] años) y el tamaño de la clave de los algoritmos. El nivel de seguridad aceptable para romper una clave es aproximadamente 10^{12} MIPS-años. Según la gráfica, el algoritmo ECC es más seguro en relación a RSA y DSA (Carbonell et al., 2007).

3.2.5 Complejidad Ciclomática

La complejidad ciclomática, facilita una medición cuantitativa de la complejidad lógica de un algoritmo, en la figura 6 se muestra la comparación de tres algoritmos de encriptación ECC, RSA y AES (Maldonado López, 2009)

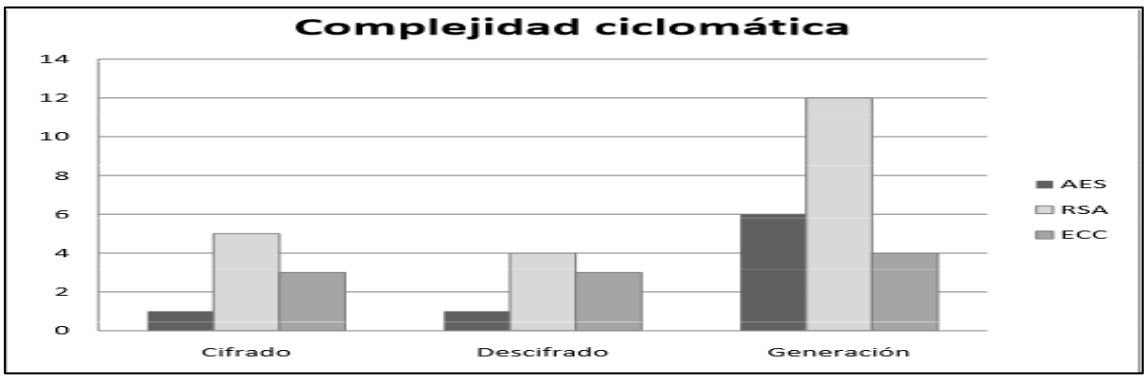

Figura 6: Comparación de la complejidad de AES, RSA y ECC

[5] MIPS representa un tiempo de cálculo de un año en una máquina capaz de realizar un millón de instrucciones por segundo.

La complejidad lógica del algoritmo RSA es mayor que ECC, tanto en la generación como en el cifrado (encriptación) y descifrado (desencriptación), esto se debe al proceso matemático que ejecuta al seleccionar números primos grandes y realizar una operación compleja. AES tiene una complejidad menor, por ser un algoritmo de criptografía simétrica y su proceso matemático consiste en elaboración de tablas de sustitución, mezcla de columnas e intercambio de matrices (Maldonado López, 2009).

3.2.6. Ataque de canal lateral

En el año 2014, un grupo de investigadores, entre quienes se destaca Adi Shamir – uno de los creadores del algoritmo RSA –, presentaron una investigación sobre un ataque para romper el algoritmo de encriptación en base a sonidos. Utilizan técnicas de criptoanálisis acústico para deducir la clave privada a partir del ruido que hace el computador cuando desencripta un mensaje (Genkin, Shamir, & Tromer, 2014). Con este tipo de ataques denominados de canal lateral, ya no es relevante el tamaño de la clave, puesto que al ser un ataque a nivel de señales eléctricas existen más posibilidades de detectarlas.

4. Conclusiones

- En base al análisis de velocidad de encriptación, se determinó que los algoritmos AES de criptografía simétrica y el de Curvas Elípticas ECC de criptografía asimétrica, son idóneos para utilizarlos como algoritmos de encriptación en mecanismos de seguridad en redes de comunicaciones.
- La comparación de la velocidad de proceso de los algoritmos simétricos, es un parámetro disponible en el software de encriptación que permite realizar una evaluación para establecer el algoritmo a seleccionar para una aplicación. Sin embargo, se ha demostrado que existen otros parámetros que influyen al momento de decidir entre uno u otro algoritmo.
- Otro aspecto de este análisis es que las investigaciones en los últimos años, han abierto la posibilidad de que los ataques se hagan a través de canales laterales y no únicamente desde la estructura matemática del algoritmo.
- Antes de elegir un algoritmo de encriptación es necesario establecer si se puede aplicar en cualquier tipo de dispositivo y así facilitar la migración de tecnología cuando sea necesario.

5. Recomendaciones

- Se recomienda difundir el algoritmo asimétrico de Curvas Elípticas pues posee características altamente seguras en robustez y tamaño de clave. Además de un significativo ahorro en el ancho de banda requerido, debido a que los tiempos de procesamiento son más bajos los de otros algoritmos.
- Se recomienda que al seleccionar algún mecanismo de encriptación, se considere que los algoritmos de criptografía asimétrica no reemplazan a los de criptografía simétrica, puesto que la aplicación de éstos dependerá del tipo de seguridad que requiera la red.

- Al momento de aplicar criptografía asimétrica es recomendable aprovechar las ventajas que presentan algoritmos como el de curvas elípticas y analizar la implementación de éste en los software de encriptación de código abierto.

6. Referencias Bibliográficas:

Alfaro, D. E. M. R. P. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles.

Andreu, F., Pellejero, I., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN*: Marcombo.

Belingueres, G. (2000). Introducción A Los Criptosistemas de Curva Elíptica. *Obtenido en la Red Mundial el, 5*.

Carbonell, C., Díaz, R., & Mejías, P. (2007). *Eficiencia de la Criptografia de Curva Elíptica y RSA para enfrentar los nuevos requerimientos de Seguridad en Internet.* Universidad Central de Chile, Santiago de Chile. Retrieved from www.criptored.upm.es/guiateoria/gt_m103a.htm

Escrivá Gascó, G., Romero Serrano, R. M., & Ramada, D. J. (2013). *Seguridad informática*: Macmillan Iberia, S.A.

E. d. i. d. E. Latinoamérica. (2014) Tendencias 2014: El desafío de la privacidad en Internet. Available: http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

E. Bonilla Palencia, "Implementación del algoritmo AES sobre arquitectura ARM con mejoras en rendimiento y seguridad," 2012.

Genkin, D., Shamir, A., & Tromer, E. (2014). RSA key extraction via low-bandwidth acoustic cryptanalysis *Advances in Cryptology–CRYPTO 2014* (pp. 444-461): Springer.

J. Cano, *Inseguridad de la Información*. Bogotá: Alfaomega, 2013.

J. M. Luaces Novoa, "Seguridad en redes inalámbricas de área local (WLAN)," 2013.

J. F. Roa Buendía, *Seguridad informática*. España: McGraw-Hill España, 2013.

Lehembre, G. (2006). Seguridad Wi-Fi–WEP, WPA y WPA2. *Recuperado el, 9*(10).

L. E. Hernández, C. Carreto, R. Menchaca, E. S. de Cómputo, and D. México, "Modelo de Seguridad para Redes Aplicado a Dispositivos Móviles," *RISCE Revista Internacional de Sistemas Computacionales y Electrónicos,* p. 21, 2012.

Maiorano, A. (2009). *Criptografía. Técnicas de desarrollo para profesionales* (1 ed. ed.). Buenos Aires: Alfaomega Grupo Editor.

Maldonado López, F. A. (2009). Modelo de seguridad para datos y servicios de telecomunicaciones sobre redes de distribución de energía eléctrica - PLT.

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

Olsson, R. (2012). Performance differences in encryption software versus storage devices.

Pousa, A., Sanz, V. M., & De Giusti, A. E. (2011). *Análisis de rendimiento de un algoritmo de criptografía simétrica sobre arquitecturas multicore.* Paper presented at the XVII Congreso Argentino de Ciencias de la Computación.

A. Sánchez-Henarejos, J. L. Fernández-Alemán, A. Toval, I. Hernández-Hernández, A. B. Sánchez-García, and J. M. C. de Gea, "Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria," *Atención Primaria*, vol. 46, pp. 214-222, 2014.

U. I. d. T. (UIT). (2014). *Índice de Desarrollo de las TIC*. Available: http://www.itu.int/net/pressoffice/press_releases/2014/68-es.aspx#.VSvg_5N1LcY

Vivas, T., Huerta, M., Zambrano, A., Clotet, R., & Satizábal, C. (2008). *Aplicación de Mecanismos de Seguridad en una Red de Telemedicina Basados en Certificados Digitales.* Paper presented at the IV Latin American Congress on Biomedical Engineering 2007, Bioengineering Solutions for Latin America Health.

Zhao, H. (2006). La seguridad de las telecomunicaciones y las tecnologías de la información.