ISSN 0798 1015

REVISTA ESPACIOS

HOME | Revista ESPACIOS | ÍNDICES / Index | A LOS AUTORES / To the AUTHORS

Vol. 39 (Nº 32) Año 2018 • Pág. 3

Diseño e implementación de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web

Design and implementation of a new symmetric cryptographic algorithm for instant messaging in a web environment

Ana Lucila CUSHPA Guamán 1; Pablo Martí MÉNDEZ Naranjo 2; Diego Gustavo CAIZA Méndez 3; Henry Mauricio VILLA Yánez 4; Andrés Santiago CISNEROS Barahona 5

Recibido: 22/02/2018 • Aprobado: 15/04/2018

Contenido

RESUMEN:

La presente investigación permite realizar el diseño e implementación de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web, con la finalidad de incrementar la seguridad de la información, utilizando la criptografía. El algoritmo criptográfico base fue el AES (Advanced Encryption Standard), seleccionado de acuerdo a los parámetros de comparación con otros algoritmos simétricos generando el Prototipo I, esto permitió el desarrollo de un nuevo algoritmo criptográfico que incorpora nuevas funciones que generando el Prototipo II. El software utilizado fue Netbeans como IDE de desarrollo en Java de los prototipos de escritorio con los cuales se realizan las pruebas de entropía de los mensajes cifrados por cada uno de ellos y utilizando R Stadistical se obtuvieron datos estadísticos de las pruebas realizadas para la validación del algoritmo propuesto y su respectiva incorporación en los prototipos web aplicados en un chat con el apoyo postgreSQL como motor de base de datos. Con la implementación de los Prototipos I y II se realizó la comparación de los resultados obtenidos del análisis de las características de los algoritmos y por medio de la herramienta Cryptool se realizaron las pruebas de

ABSTRACT:

The present investigation allows the design and implementation of a new symmetric cryptographic algorithm for instant messaging in a web environment, in order to increase the security of information, using cryptography. The base cryptographic algorithm was the AES (Advanced Encryption Standard), selected according to the parameters of comparison with other symmetric algorithms generating the Prototype I, this allowed the development of a new cryptographic algorithm that incorporates new functions that generate the Prototype II. The software used was Netbeans as IDE of Java development of the desktop prototypes with which entropy tests were performed on the messages encrypted by each of them and using R Stadistical, statistical data were obtained from the tests carried out for the validation of the proposed algorithm and its respective incorporation in web prototypes applied in a chat with postgreSQL support as a database engine. With the implementation of Prototypes I and II the comparison of the results obtained from the analysis of the characteristics of the algorithms was made and through the Cryptool tool the cryptanalysis tests were performed for the measurement and

criptoanálisis para la medición y comparación de los indicadores que fueron considerados en las variables. Con la aplicación de la estadística descriptiva e inferencial en la comprobación de la hipótesis se concluye que el nuevo algoritmo propuesto incrementó el nivel de seguridad en un 53% al compararlo con el algoritmo simétrico AES base debido a que presenta mayor difusión en el cifrado de mensajes.
Palabras-Clave: Advanced Encryption Standard (AES); criptoanálisis; mensajería instantánea, R Stadistical.

comparison of the indicators that were considered in variables. With the application of descriptive and inferential statistics in the verification of the hypothesis, it is concluded that the proposed new algorithm increased the security level by 53% when compared to the symmetric AES base algorithm because it has a greater diffusion in message encryption.
Keywords: Advanced Encryption Standard (AES); cryptanalysis; instant messaging, R Statistical.

1. Introducción

En la actualidad, proteger los datos es una tarea desafiante debido a que la información es el activo más importante y desempeña un papel vital en todos los aspectos de la vida humana, ya sea personal o profesional. (Panday & Pandey, 2016)

La criptografía viene de palabras griegas que significan "escritura oculta", es el arte o la ciencia que abarca los principios y métodos de transformar un mensaje inteligible en uno que es ininteligible (cifrados) y luego retransformar ese mensaje de nuevo a su forma original. Sólo aquellos que poseen una clave secreta pueden descifrar el mensaje en texto plano. No es utilizado únicamente en las comunicaciones telefónicas, fax, correo electrónico, transacciones bancarias, cuentas bancarias, PIN, contraseñas y transacciones de tarjetas de crédito en la web, también se utiliza en otros ámbitos de seguridad de la información, incluyendo firmas electrónicas, que se utilizan para demostrar quién envió un mensaje. (Nikita & Kaur, 2014)

El Algoritmo AES es un cifrado de clave simétrica en el que tanto el remitente como el receptor utilizan la misma clave para el cifrado y el descifrado. El bloque de datos es de tamaño fijo de 128 bits, la longitud de clave puede variar desde 128.192.256 bits. El algoritmo AES es un algoritmo iterativo. Cada iteración se llama ronda. El número de rondas varía de 10, 12, 14 depende del tamaño de la clave 128, 192, 256, respectivamente. El bloque de imagen de 128 bits se divide en hasta 16 bytes. Estos bytes se asignan en los arrays 4x4 llamados estados. Todas las operaciones internas del algoritmo AES se realizan en los estados. En cifrado y descifrado AES cada ronda consta de cuatro transformaciones. La transformación realizada en el estado es similar entre todas las versiones, pero el número de rondas de transformación depende de la longitud de la clave de cifrado. Las AES finales difieren ligeramente de las primeras rondas Nr-1, ya que tiene una transformación menos realizada en el estado. Las principales funciones del Algoritmo AES son: sub bytes, shift rows, mix columns y add roundkey. (Kumar & Singh, 2011)

El criptoanálisis es el estudio de textos cifrados y criptosistemas con el objetivo de encontrar fallas en ellos que eventualmente permitan la recuperación del texto sin cifrar, sin revelar necesariamente muchos detalles sobre la clave o el algoritmo utilizado para el cifrado (Kalubandi, Vaddi, Ramineni, & Loganathan, 2016). El criptoanálisis permitirá verificar el nivel de seguridad de la propuesta, del algoritmo AES en comparación con el algoritmo AES base.

En la investigación realizada por Patil y Kobsa (2010), plantean la mensajería instantánea (IM) como una herramienta útil para el trabajo colaborativo. Sin embargo, las características de conciencia y comunicación de IM proyectan una tensión con los deseos de privacidad. Realiza entrevistas y una encuesta por Internet para entender actitudes y prácticas de privacidad en el uso de mensajería instantánea. Basándose en los hallazgos de estos estudios, diseña un complemento de mensajería instantánea para mejorar el soporte para la gestión de la privacidad en los sistemas actuales de mensajería instantánea. El complemento detecta conflictos en las preferencias de privacidad, notifica a las partes involucradas y permite la negociación de una resolución.

En la investigación realizada por Kumar y Rana (2016), presentan una modificación al algoritmo AES, aumentando el número de rondas (Nr) en el proceso de cifrado y descifrado del algoritmo, obteniendo como resultado mayor seguridad para el sistema que proporciona

alta velocidad, así como una menor transferencia de datos a través de los canales no seguros.

La investigación realizada por Mathur y Bansode (2016), consideran que la seguridad de los datos tiene un papel importante en el desarrollo del sistema de comunicación, donde más aleatorización en las claves secretas aumenta la seguridad, así como la complejidad de los algoritmos de criptografía. La criptografía juega un papel vital en el sistema de seguridad de la información contra varios ataques. Versiones más eficientes y nuevas de las técnicas de criptografía pueden ayudar a reducir esta amenaza de seguridad. En este trabajo, se utiliza un algoritmo AES mejorado para cifrar el texto sin formato y el algoritmo ECC se aplica para cifrar la clave AES, aumentando así la seguridad general del sistema mediante la implementación de contramedidas basadas en software para evitar posibles vulnerabilidades planteadas por el ataque de canal de tiempo. Para aumentar aún más la eficiencia del cifrado de datos, se implementa su orden de AES con el tamaño de clave de 192 bits y con 12 rondas de iteraciones en comparación con el modelo AES básico que tiene 128 bits y 10 rondas de iteraciones.

---

2. Metodología

La presente investigación es de tipo cuasi-experimental ya que se basa en las características definidas en el estudio para elegir un algoritmo simétrico base que sirve como base para la creación del nuevo algoritmo, que se incorpora en una aplicación web de mensajería instantánea, con los que se realiza pruebas en escenarios a través del uso de prototipos. Los instrumentos utilizados son: Netbeans (Netbeans, 2016) como IDE de desarrollo en Java, Cryptool (Cryptool, 2015) para realizar las pruebas de criptoanálisis a los mensajes cifrados, PostgreSQL *(PostgreSql, 2010)* es un sistema de gestión de bases de datos objeto-relacional, de código abierto. Utiliza un modelo cliente/servidor y multiprocesos para garantizar la estabilidad del sistema, R Stadistical es un lenguaje y un entorno para la informática estadística y los gráficos, es un proyecto GNU, proporciona una amplia variedad de modelos estadísticos y técnicas gráficas, y es muy extensible (R-Project, 2016).

Para la presente investigación, se realizaron las siguientes actividades: se determinó e implementó el algoritmo criptográfico simétrico base AES, se creó e implementó la propuesta de mejora del algoritmo criptográfico simétrico, se integró los algoritmos en una aplicación web de mensajería instantánea.

2.1. Determinación e implementación del algoritmo criptográfico simétrico base

Basado en la investigación realizada por Mathur y Kerwani (2013), se selecciona como algoritmo criptográfico simétrico base el algoritmo AES debido a las ventajas que posee en comparación con otros algoritmos, entre las principales: tamaño de bloque variable, tamaños de clave variables de 128 bits, 192 bits y 256 bits, tamaño de bloque, número de rondas dependiendo del tamaño de la clave, resistencia a criptoanálisis, resistencia contra ataques de fuerza bruta. Por lo que se lo implementa con sus funciones AddroundKey, SubByte, MixColumns, ShiftRows.

2.2. Creación e implementación de la propuesta de mejora del algoritmo criptográfico simétrico

Para la propuesta de mejora del algoritmo criptográfico se ha considerado el algoritmo AES como base. Con la finalidad de mejorar la seguridad e incrementar la difusión del mensaje, se proponen las siguientes modificaciones del algoritmo criptográfico:

Utilizar una nueva función que se ejecute en la ronda inicial y en la ronda final denominado MIXDIAGONAL. En el nuevo método en se realizan desplazamientos cíclicos de manera diagonal en la matriz de estado.

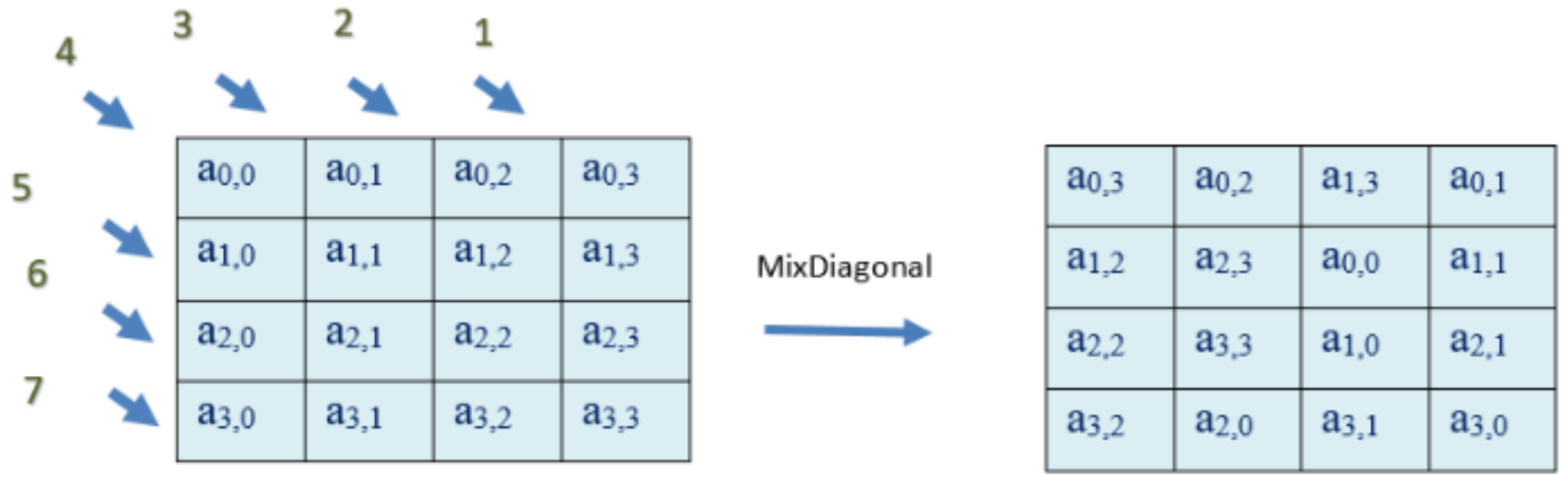
Se inicia desde la diagonal de la parte superior derecha hasta la diagonal principal, luego se

continúa por la diagonal izquierda hasta completar toda la matriz de estado.

Los datos se van colocando en la nueva matriz llenando la primera fila, después la segunda fila hasta llenar la matriz.

En la figura 1 se muestra la función MIXDIAGONAL propuesta:

Figura 1
Proceso de la función MixDiagonal



Implementar un ciclo secundario luego de las rondas principales que incluye las funciones subBytes, ShiftRows y mixColumns con Nr/2 número de vueltas, que permita hacer el texto más difuso e incomprensible para terceras personas.

2.3. Implementación de los algoritmos criptográficos

Se desarrollan dos prototipos que utilizan los algoritmos criptográficos.

PROTOTIPO I

Se emplea el algoritmo criptográfico AES base.

PROTOTIPO II

Se emplea el nuevo algoritmo criptográfico propuesto que incrementa funciones. El proceso de cifrado se muestra en la Figura 2 y el proceso de descifrado se muestra en la Figura 3

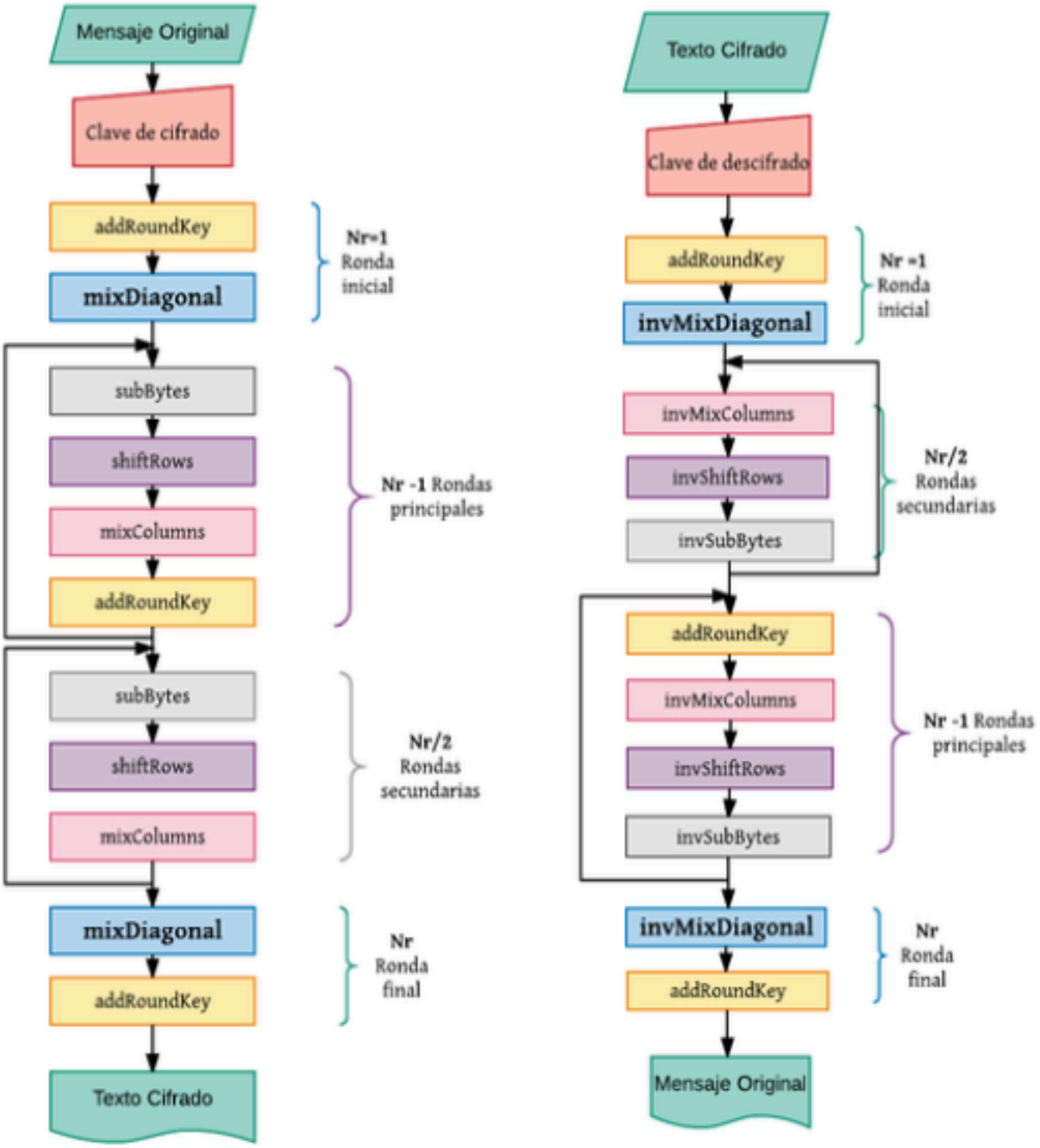


Figura 2 Proceso de cifrado nuevo algoritmo

Figura 3 Proceso de descifrado nuevo algoritmo

COMPARACIÓN DE MENSAJES CIFRADOS

Se utiliza el programa Cryptool para realizar la comparación de los mensajes cifrados pos los Prototipos I y II, realizando pruebas de criptoanálisis.

2.4. Validación del nuevo algoritmo criptográfico

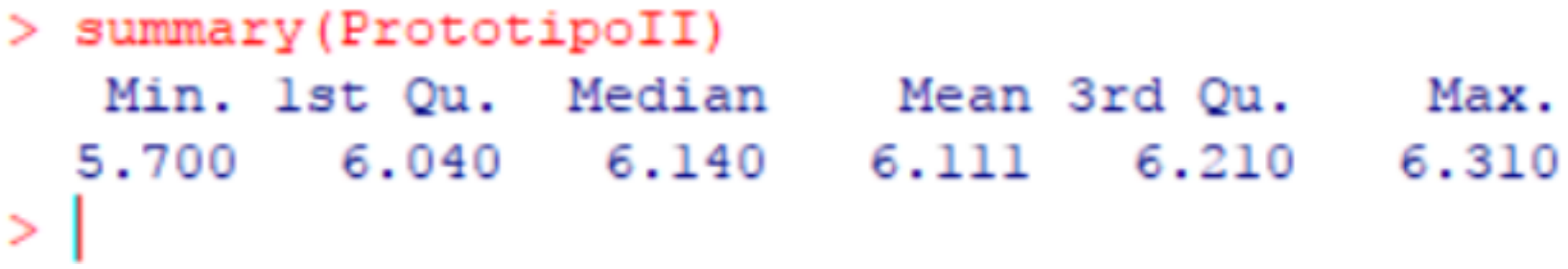
Para validar la implementación del nuevo algoritmo criptográfico se realizan pruebas de entropía a los mensajes cifrados por los prototipos I y II, que se analizan con la herramienta R stadistical como se muestran en las Figuras 4 y 5:

Figura 4
Proceso de descifrado nuevo algoritmo

```
> summary(PrototipoI)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
  5.650   6.010   6.090   6.056   6.150   6.280
```

Los datos están posicionados entre 6.010 (Primer cuartil) y 6.150 (tercer cuartil) con una media de 6.056.

Figura 5
Proceso de descifrado nuevo algoritmo



Los datos están posicionados entre 6.040 (Primer cuartil) y 6.210 (tercer cuartil) con una media de 6.310.

2.5. Ambiente de pruebas

Se establece un ambiente de pruebas en dos escenarios, en el primer escenario con el prototipo I y en el segundo escenario con el prototipo II. Las condiciones del ambiente de pruebas para los 2 escenarios son:

- Entropía
- Histogramas
- Autocorrelación
- Fuerza bruta

Escenario 1

Se utiliza el Prototipo I, que implementa el algoritmo AES base,

Escenario 2

Se utiliza el Prototipo II, que implementa el nuevo algoritmo criptográfico que incluye nuevas funciones propuestas para mejorar la seguridad.

---

3. Resultados

Para los procesos de cifrado y descifrado se utilizaron los siguientes datos:

Clave (128 bits): LDG2w:Qxmll+]vN(

Clave (192 bits): LDG2w:Qxmll+]vN(LDG2w:Qx

Clave (256 bits): LDG2w:Qxmll+]vN(LDG2w:QxLDG2w:Qx

Mensaje: Los sistemas de cifrado simétrico utilizan una misma clave para cifrar y descifrar un documento. El problema de seguridad se da en el intercambio de claves entre el emisor y el receptor. Por lo que es necesario que el canal de comunicación sea también seguro para el intercambio de claves.

Los mensajes han sido cifrados con el Prototipo I y con el Prototipo II utilizando claves de 128 bits, 192 bits y 256 bits cuyo resultado incluye caracteres imprimibles y no imprimibles como se muestra en la Tabla I.

Tabla 1
Mensajes cifrados por el Prototipo I y Prototipo II

Prototipo	Clave	Mensajes cifrados
Prototipo I	128 bits	Ä¤É□ýGÎàëÒü□À□)P'□òïti□ÇJB□>^gë ¬4Ü□àõ□0¤Ó□×I 5ñ4ÀôÎ®TqÎBªôÖmïV)□□*vëÎ:Ñn□÷□¸ö□□□ý□¬ç)hÓýµ°¢°¢Å]@ß □Ñ*°NV(□□òG□Ú§i9D_%,□ÿ¹¦PÀþA»□ ,
	192 bits	iîc¢□E□ V♠ "□+ÇÂhºã□¦ÃMÁ-Ë□□ÃÕ_á°®tâ·¶Ä¯□v!ùTöóð%S□Ê_□o¤'p□£ÜÃ □¤½DèWx□J¹ãM-oSF¬Õð§ÃÂ.cÿ□Àæ □_Ò□Ûm□ÊY± þò@ùsï¢□□ d7s□Ö!c□¬x□A□Nu+_□□Ý°=f□À□]□)ì□□□□~Ê □□□□□iªxÁ-?¦æ□Ù¦ì}□□F□Üñé□ >¤ÃUøú□¼Â'□?}□□□÷□/Ð´ÛÒ¥□□□.Ð□Äéç%·©?□W/Ó$□ t]□KCà£ú□lÂ□□ðe®| Ä]õ□ã°HL□KI□¿□□¦ Ä¬Ü_´96å}Õ□□Ñ'eÞ;Th□Ã¸RH_tEÓÎ-)@Ø□□ð`rFÏ□□=æ3□1
	256 bits	]Mit-D(sF×XU|´YÂjs` □□□ÅÁ¢;pU×Óö□ ¬õ□)3Û¼XT7□□a;¸â□xÂn2xT□□´°:d¶Ü□)♠□ □□¢t□õÃ¹Î^□x□â»Ã>?□»D□§ÿ¬A□¤¿² :TN□¸□"xì□¯#□A1Ô¹□F$□□®Ô|ö7nûi*□¤ÄvüÈh¾□¨Û] □þkµ8à □ºº□□y□8)dSPÈã□g□þc□□ªÛKKC9]}2ráe□□j□¼□åqG× Fðø♠□BWlÁfà□ÜÙ□*óN□si□³3a ¢□£ºÌ□ªH¬□x¢□□â ^¸□ð$]ÝFÞ
Prototipo II	128 bits	□$È_□Xñ¿r□□□8V□□©V□=á□ gÝ□§E□§□□$□□Ïv³□¯È□iÅ□Q□;-□Þ□□&03□Ãé)□å□òs□t°□ □□Ëù¥.□□□pY°Û¢h□Ò`ðÇ□[¸#x1□3g□Q²è¥d□□ºz□@ïö□µ^% □ÎÑh4Mÿ□w<#O□z□)□_{Â®Û□×X□`Â5Û♠□.cTq d□¶□□□°ü□ :$« ðr□ç:□Àq□□□□¤1èÙìc03Öù¿Ìl□□□Á□«□tYÀA©□úá"-`ø\□ E□D4¤Í.TJ□!□□&□ê□□uç3Ü2·HM%Ñé□N□ ±□ºÏ□_ □´J □mg□á□□ÛÄ□□ßÈ□ëÓ
	192 bits	-□kÔ3ãÛÈ£·V2Ç□½·µ□¹L□iûß□s^Ð÷□rE□□s□□□Ïæÿßêl □ð>¼øºTu □¬ÌÑ <?¨ËU=º>+³%¨ÉÞÃ□Ä°□□4ö[%Ìò2a □9♠ p□Y:`) ùJ`µú□ 2ÜvÃP□□ZP_À□]ÃK□À|Á□□|>,ó¶_□□±RÌ-ì÷ È- "i$DymäÝ ¢□□□-¹i□□)4ñ2□:FñÙr□+□g=Á¹P□Ós□pàÃ_♠ ^□□â~§àõ©]□`úFÇgî¨¯Í£uÿ□{îrË□=ü□´w M à}Î9«□□ È'þí□□÷□□V□ é¶Ïnþ>□Wy&□ÌB6À□□ò5□¯#ê1=üZ□^(Â□%ø~Á□?l □ì□_Ó□(b¹Ì□G~ÿïK9□□º
	256 bits	□¥3Ç□°¾µÃxÍÎÅ \¹□□¸pÛ□□{0Àþ□B«ÅOåÍí□U□ ÍÜ□ôt '□□Õôo□ g□])□Ð□?¶ê□îÎ□ö©¿ò□Rú □+□È!¸Ù□ □□□□#GÛ¤®yXÉ7b<*¥□ w¢¿!UU%@5DÙ□ñ□□KN÷ìwú□ªÙË#□ Ë□Q=¾Ï□ço3□|wh=□×+-²é¦□L}□□i□Ø±□ïËJÔÄ□µ □RÅy k□'□,Ñ□ÿeD»¹T□¾Ç"ÕÁ□#6¶□úJ$□ûZrÛÒV□□@c·M□©□□CÃº □ÿo®{â□GTÂ□□s/=È?äÇ~èÄ.ó□

3.1. Comparación de resultados

Se realiza la comparación de los mensajes criptográficos con el Prototipo I y el Prototipo II utilizando criptoanálisis con los indicadores de entropía, histogramas, n-gramas, autocorrelación y fuerza bruta, para lo cual se utiliza la herramienta cryptool.

Entropía

El análisis de entropía permitió medir el nivel de desorden de los mensajes cifrados con el Prototipo I y Prototipo II, el cual es directamente proporcional a la seguridad del mensaje, como se muestra en la Tabla 2.

Tabla 2
Entropía de los mensajes cifrados con el Prototipo I y Prototipo II

Prototipo	Clave	Caracteres diferentes	Entropía máxima	Valor
	128 bits	6,61	6,61	5,79
Prototipo I	**192 bits**	65	6,61	5,82
	256 bits	69	6,61	5,92
	128 bits	65	6,61	5,91
Prototipo II	**192 bits**	73	6,61	5,85
	256 bits	75	6,61	6,01

Histogramas

El análisis de histogramas permitió evaluar la cantidad de caracteres que conforman los mensajes cifrados con el Prototipo I y Prototipo II, el mismo que es directamente proporcional a la seguridad del mensaje, como se muestra en la Tabla 3.

Tabla 3
Histogramas de los mensajes cifrados con el Prototipo I y Prototipo II

Prototipo	Clave	Caracteres diferentes
	128 bits	106
Prototipo I	**192 bits**	109
	256 bits	105
	128 bits	112
Prototipo II	**192 bits**	130
	256 bits	120

Fuerza bruta

El análisis de fuerza bruta permitió medir el tiempo que sería necesario para encontrar la clave con la que fueron cifrados los mensajes, utilizando fuerza bruta realizando varias combinaciones, con el objetivo de determinar los mensajes cifrados con el Prototipo I y Prototipo II, el cual es directamente proporcional a la seguridad del mensaje, como se muestra en la Tabla VI.

Tabla 4

Tiempo para descifrar los mensajes cifrados con el Prototipo I y Prototipo II

Prototipo	Clave	Tiempo descifrar (años)
	128 bits	1,7e+ 025 años
Prototipo I	**192 bits**	3,8+044 años
	256 bits	1e+064 años
	128 bits	2,2e +025 años
Prototipo II	**192 bits**	4,4e+044 años
	256 bits	1,2e+064 años

4. Conclusiones

Se utilizó el algoritmo criptográfico AES, debido a que es el más apropiado por sus ventajas que permite utilizar claves de 128 bits, 192 bits y 256 bits, tamaños del bloque variables, resistente a criptoanálisis diferencial, lineal y tiene resistencia contra fuerza bruta, por lo que es más seguro y resistente.

La incorporación de la función propuesta en las rondas del algoritmo y el incremento de rondas, permitió que el mensaje cifrado se difumine más en comparación con el algoritmo AES base, logrando mayor seguro.

Los mensajes cifrados con el Prototipo II poseen mayor entropía, utilizan mayor cantidad de caracteres y se requiere un mayor tiempo para obtener la clave y con ella el mensaje original utilizando fuerza bruta en comparación a los mensajes cifrados con el Prototipo I.

Referencias bibliográficas

Cryptool. (2015). *About CrypTool 1.* Obtenido de https://www.cryptool.org/en/cryptool1

Kalubandi, V., Vaddi, H., Ramineni, V., & Loganathan, A. (2016). A novel image encryption algorithm using AES and visual cryptography. *Next Generation Computing Technologies (NGCT)* (págs. 808-812). IEEE.

Kumar, A., & Singh, J. (2011). Novel secure technique using visual cryptography and advanced AES for images. *International Journal of Knowledge Management & e-Learning, 3*(1), 29-34.

Kumar, P., & Rana, S. (2016). Developmente of modified AES algorithm for data security. *Inernational Journal for light and electron optics*, 2341-2345.

Mathur, N., & Bansode, R. (2016). AES Based Text Encryption Using 12 Rounds with dynamic key selection. *Procedia Computer Sciencie*, 1036-1043.

Netbeans. (2016). *NetBeans IDE - The Smarter and Faster Way to Code*. Obtenido de https://netbeans.org/features/index.html

Nikita, & Kaur, R. (2014). A survey on secret key encryption technique. *IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET), 2*(5), 7-14.

Panday, R., & Pandey, V. (2016). Cryptography & security implementation in network computing environments. *3rd Computing for Sustainable Global Development (INDIACom)* (págs. 3136-3140). IEEE.

Patil, S., & Kobsa, A. (2010). Enhancing privacy management support in instant messaging. *Interacting with computers*, 206-217.

PostgreSql. (2 de octubre de 2010). Recuperado el 5 de enero de 2017, de http://www.postgresql.org.es/sobre_postgresql

R-Project. (2016). *Introduction to R.* Obtenido de https://www.r-project.org/about.html

---

1. Profesional orientado a las Redes de computadoras. Ecuador. Ingeniero en Sistemas Informáticos. Magíster en Interconectividad y Redes. anitacg25@hotmail.com

2. Profesor y profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. pmendez@unach.edu.ec

3. Profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Electrónica Telecomunicaciones y Redes. Magíster en Seguridad Telemática. diegomix07@hotmail.com

4. Profesor y profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. hvilla@unach.edu.ec

5. Profesor y profesional orientado a las telecomunicaciones y redes. Director Departamento de Evaluación y Acreditación. Universidad Nacional de Chimborazo. Ecuador. Investigador CIMOGSYS - Escuela Superior Politécnica de Chimborazo. Ecuador. Ingeniero en Electrónica y Computación. Magíster en Interconectividad y Redes. ascisneros@unach.edu.ec

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 39 (Nº 32) Año 2018

[Índice]