ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DISEÑO E IMPLEMENTACIÓN DE UN NUEVO ALGORITMO CRIPTOGRÁFICO SIMÉTRICO PARA MENSAJERÍA INSTANTÁNEA EN UN ENTORNO WEB

ANA LUCILA CUSHPA GUAMÁN

Trabajo de Titulación modalidad: Proyectos de investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN INTERCONECTIVIDAD DE REDES

RIOBAMBA - ECUADOR

MARZO 2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo** titulado "DISEÑO E IMPLEMENTACIÓN DE UN NUEVO ALGORITMO CRIPTOGRÁFICO SIMÉTRICO PARA MENSAJERÍA INSTANTÁNEA EN UN ENTORNO WEB", de responsabilidad de la Ing. Ana Lucila Cushpa Guamán, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Juan Mario Vargas Guambo; M.Sc	
PRESIDENTE	FIRMA
Ing. Pablo Martí Méndez Naranjo; M.Sc.	
DIRECTOR	FIRMA
Ing. Diego Gustavo Caiza Méndez; M.Sc.	
MIEMBRO	FIRMA
Ing. Henry Mauricio Villa Yánez; M.Sc.	
MIEMBRO	FIRMA

Riobamba, Marzo 2018

DERECHOS INTELECTUALES

Yo, Ana Lucila Cushpa Guamán, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación modalidad **Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior politécnica de Chimborazo.

_____

060334378-1

DECLARACIÓN DE AUTENTICIDAD

Yo, Ana Lucila Cushpa Guamán, declaro que el presente Trabajo de Investigación, es de mi autoría y que los resultados expuestos son auténticos y originales. Los textos constantes en el documento que proceden de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

_____

Ana Lucila Cushpa Guamán
060334378-1

DEDICATORIA

Con mucho cariño a mi esposo e hijos, quienes son el motor de mi vida y el apoyo incondicional durante todo el proceso, con su paciencia y confianza están siempre presentes en la construcción de mis objetivos.

A mis padres por enseñarme que con esfuerzo, dedicación y trabajo todo es posible.

Anita

AGRADECIMIENTO

Agradezco a Dios porque siempre está presente en mi vida y en mi familia y por darme fortaleza en los momentos más difíciles.

Gracias a mi familia por apoyarme siempre y por sus palabras que me confortan para seguir adelante.

A la Escuela Superior Politécnica de Chimborazo, por ser parte de mi formación académica.

Un agradecimiento sincero al Ing. Pablo Méndez, quién como director del presente proyecto de investigación ha sido una guía y apoyo constante durante todo el desarrollo de este trabajo.

A los docentes y Miembros del Tribunal del Trabajo de Titulación: al Ing. Diego Caiza y al Ing. Henry Villa, que han sabido orientarme y asesorarme para culminar el presente proyecto.

Anita

ÍNDICE DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

El objetivo fue el diseño e implementación de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web, para incrementar la seguridad de la información que es transmitida a través de canales inseguros de información utilizando la criptografía. Se realizó una revisión de las características que presentan los algoritmos criptográficos simétricos más utilizados que permitió determinar el algoritmo simétrico AES (Advanced Encryption Standard) como algoritmo base 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. En la implementación se utilizó Netbeans como ambiente de desarrollo en 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 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. La modificación de las funciones que ejecuta el algoritmo o el incremento de nuevas funciones ayudan a difuminar más el mensaje.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA > , <SEGURIDAD INFORMÁTICA> , <CRIPTOGRAFÍA> , <ESTÁNDAR DE ENCRIPTACIÓN AVANZADA (AES)> , <CRIPTOANÁLISIS> , <MENSAJERÍA INSTANTÁNEA> , <R STADISTICAL>

ABSTRACT

The objective was the design and implementation of a new symmetric cryptographic algorithm for instant messaging in a web environment, to increase the security of information that is transmitted through insecure channels of information using cryptography. A review of the characteristics of the most used symmetric critical algorithms was made, this allowed the determination of the symmetric algorithm Advanced Encryption Standard (AES) as base algorithm according to the comparison parameters with other symmetric algorithms generating the Prototype I, this allowed the development of a new cryptographic algorithm that incorporates new functions that generated the Prototype II. In the implementation, NetBeans was used as a development environment in the desktop prototypes with which the entropy tests of the messages encrypted by each of them were performed and using Statistical R, statistical data were obtained from the tests performed for the validation of the algorithm proposed and their respective incorporation in the 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 device the cryptanalysis tests were carried out for the measurement and comparison of the indicators that were considered in the variables. With the application of descriptive and inferential statistics in the verification of hypotheses, it is concluded that the proposed new algorithm increased the security level by 53% when compared with the symmetric AES base algorithm because it has a greater diffusion in message encryption. The modification of the functions that the algorithm executes or the increase of new functions help to spread the message further.

KEYWORDS: <TECHNOLOGY AND ENGINEERING SCIENCES >, <COMPUTER SECURITY >, <CRYPTOGRAPHY>, <ADVANCE ENCRYPTION STANDARD (AES)>, <CRYPTANALYSIS>, <INSTANT MESSAGING>, <STADISTICAL R>

CAPITULO I

INTRODUCCIÓN

En este Capítulo se realiza la identificación del problema de estudio, justificación, objetivos e hipótesis a comprobar con el desarrollo de la investigación.

1.1. Planteamiento del problema / antecedentes

1.1.1. Problematización

El surgimiento de redes de comunicación, en particular de Internet, ha abierto nuevas posibilidades para el intercambio de información. Al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite, dado que los mensajes enviados generalmente por una persona suelen viajar por canales o infraestructura externa, como internet, en texto plano (plain text), es decir en archivos formados exclusivamente por texto (sólo caracteres), sin ningún formato; no requieren ser interpretados para leerse, por lo que son susceptibles a ser interceptados, causando daños o perjuicios inevitables.

La seguridad de la información es el conjunto de medidas preventivas de los sistemas tecnológicos que permiten proteger la información buscando custodiar la confidencialidad, la disponibilidad e integridad de los datos.

Es necesario entonces, crear diferentes mecanismos, dirigidos a garantizar la privacidad y autenticidad, resguardando los documentos y datos que circulan en las redes locales y en internet, para ello se utilizará la ***Criptografía***.

La criptografía es la técnica utilizada para cifrar mensajes que contienen información; ha sido denominada también escritura secreta, ya que el cifrado supone un nivel de ocultamiento para evitar el descifrado por personas ajenas a los receptores originales del mensaje. (**SGARRO**, 1990, pág. p. 22)

Background Check publicó una infografía que permite visualizar de forma muy clara cuál es la situación actual de la seguridad de la información en las empresas. Durante 8 años se realizó un seguimiento a más de 2000 brechas de seguridad y fueron investigados más de mil millones de registros sobre sistemas comprometidos. Según los estudios realizados, el 97% de los incidentes ocurridos podrían haber sido evitados con controles de niveles simples o intermedios (**E-VOLUTION**, 2012, págs. http://e-volution.cc/2012/06/04/eset-informa-estudio-sobre-el-estado-de-la-seguridad-de-la-informacion-corporativa/comment-page-1/).

La comunicación vía web es insegura, debido a que la información viaja a través de un canal inseguro y puede ser obtenido por terceras personas, por lo que es necesario proteger dicha

información con técnicas de cifrado que utiliza la criptografía.

Los algoritmos criptográficos actuales no son completamente seguros, su seguridad se basa en la cantidad de tiempo de cómputo que con la tecnología actual, llevaría descifrar las claves criptográficas, por lo que, juegan un papel importante los algoritmos que cubran una o varias características básicas de seguridad, la presente propuesta busca mejorar el nivel de seguridad con la implementación de un nuevo algoritmo criptográfico con ***mejores características*** de acuerdo a factores analizados en la investigación realizada por Mathur y Kesawani (2013) como por ejemplo: tipo de clave, tamaño del bloque, número de rondas, criptoanálisis, entre otras.

1.1.2. Formulación del problema

¿Cuál sería el nivel de mejora en la seguridad al diseñar e implementar un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web?

1.1.3. Sistematización del problema

- ¿Cuáles son las características, de los algoritmos criptográficos simétricos existentes?
- ¿Cómo mejorar la seguridad de un algoritmo criptográfico simétrico existente?
- ¿Cómo implementar un algoritmo criptográfico simétrico para mensajería instantánea en un entorno web?
- ¿Cómo medir el nivel de mejora de la seguridad de un algoritmo criptográfico simétrico y probar que la información cifrada tiene mayor seguridad?

1.2. Justificación

El trabajo de investigación propone con ayuda de la criptografía aplicar técnicas que incrementen la seguridad cuando se transmita información sensible, que no sea obtenida fácilmente por terceros ya que se encontrará cifrada, enmarcado en el objetivo 11 del Plan Nacional del Buen Vivir: "Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológicas", 11.3 "Democratizar la prestación de servicios públicos de telecomunicaciones y de tecnologías de información y comunicación (TIC), incluyendo radiodifusión, televisión y espectro radioeléctrico, y profundizar su uso y acceso universal" y 11.3.l "Fortalecer la seguridad integral usando TIC". La investigación enmarcada desde el punto vista de la Maestría de Interconectividad de Redes, a la seguridad informática: Análisis de algoritmos criptográficos, dentro de la ESPOCH a las tecnologías de la información, comunicación, procesos industriales y biotecnológicos, dentro del Programa de desarrollo de la seguridad en la gestión de la información.

Con estos antecedentes la presente propuesta plantea la creación de un nuevo algoritmo criptográfico simétrico con el objetivo de incrementar el nivel de seguridad de la información para mensajería instantánea en un entorno web; en el supuesto caso de que la información sea

interceptada y extraída por los atacantes, esta no pueda ser leída o alterada ya que se encuentra cifrada, mejorando así la seguridad.

La validación del nuevo algoritmo criptográfico simétrico planteado se lo realizará en base al *análisis de complejidad* de los algoritmos, en función del orden de complejidad para obtener el nivel de eficiencia del mismo, en comparación con el algoritmo criptográfico simétrico base.

Las pruebas se efectuarán en dos escenarios, en el primero se utilizará el algoritmo criptográfico simétrico base y el en segundo se utilizará el nuevo algoritmo criptográfico simétrico implementado en una aplicación para mensajería instantánea en un entorno web.

Posteriormente se comparará el nuevo método implementado con el algoritmo base, con el fin de demostrar el incremento de la seguridad.

1.3. Objetivos

1.3.1. General

- Diseñar e implementar un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web.

1.3.2. Específicos

- Analizar los algoritmos criptográficos simétricos más conocidos, para seleccionar uno como base en función de sus características.
- Diseñar el nuevo algoritmo criptográfico simétrico, tomando como base el algoritmo seleccionado.
- Implementar los prototipos para mensajería instantánea en un entorno web: uno con el algoritmo criptográfico simétrico base y el otro con el nuevo algoritmo criptográfico simétrico.
- Probar los prototipos implementados para mensajería instantánea en un entorno web para verificar el nivel de seguridad en los escenarios.

1.4. Hipótesis

La implementación de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web mejorará el nivel de seguridad de la información.

CAPITULO II

MARCO DE REFERENCIA

En este Capítulo, se analiza el estado del arte acerca del tema, objeto de estudio y se establece el algoritmo que servirá de base para la crear el nuevo algoritmo criptográfico.

2.1. Antecedentes y estudios previos

Entre las principales investigaciones, se citan las siguientes:

"Development of modified AES algorithm for data security" (KUMAR & RANA, 2016, págs. 2341-2345)**.**

El proyecto surge de la necesidad de proveer una comunicación segura a través de un procesamiento criptográfico eficiente para un buen rendimiento del sistema, utilizando una herramienta básica de la seguridad de la información. Este documento presenta la compresión de los datos con el estándar de cifrado AES, en la investigación se incrementa el número de rondas (Nr) a 16 para el proceso de cifrado y descifrado del algoritmo AES, que dan como resultado mayor seguridad al sistema.

El proceso realizado en el estudio es el siguiente:

- Determinación los parámetros AES que dependen de su tamaño de clave
- Desarrollo del algoritmo propuesto con el incremento a 16 rondas.
- Ejecución de pruebas sobre la base del rendimiento para los diferentes tamaños de archivo.
- Análisis de resultados obtenidos.
- Definición de conclusiones.

A continuación, se muestra la propuesta de modificación del algoritmo AES.

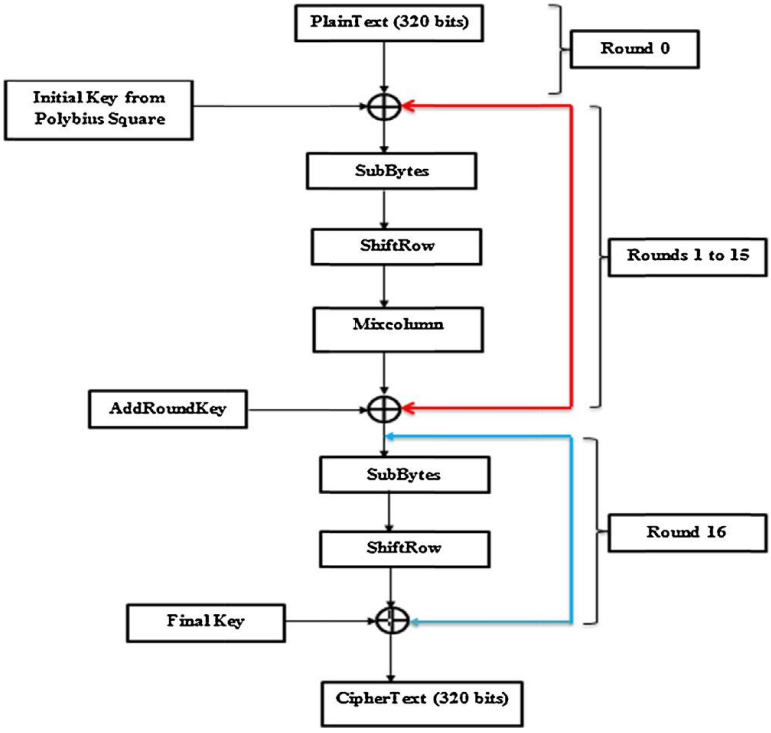


Figura 1-2: Propuesta del proceso de encriptación AES
Fuente: (KUMAR & RANA, 2016)

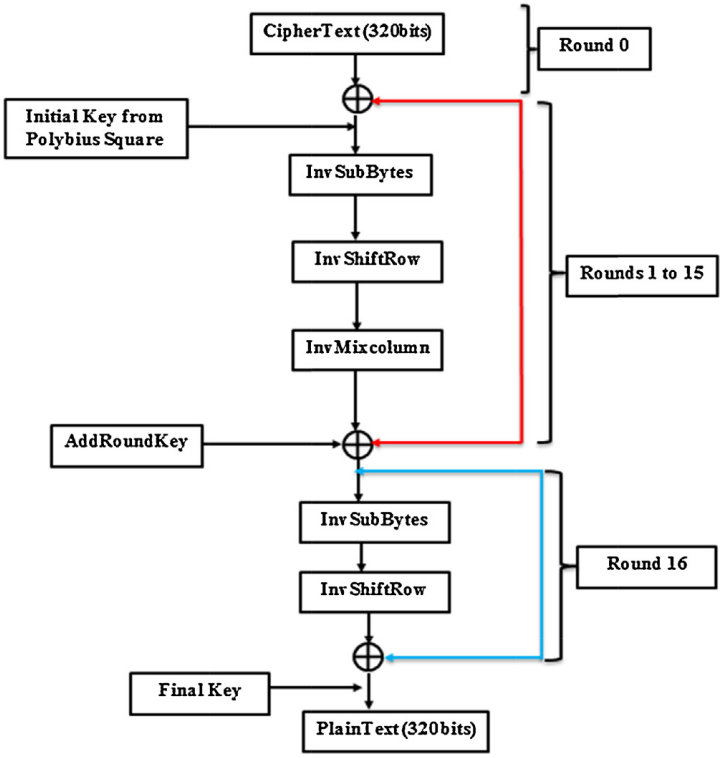


Figura 2-2: Propuesta del proceso de descifrado AES
Fuente: (KUMAR & RANA, 2016)

En las pruebas realizadas el proceso de cifrado AES en lugar de 10 rondas se incrementa el número de rondas a 16. La clave inicial se ha generado a partir de la plaza Polybius. El proceso de cifrado experimenta las operaciones Subytes, ShiftRows, MixColumns y AddRound Key. En el Proceso de descifra se somete a InvSubBytes, InvShiftRows, InvMix-Columns y AddRoundKey El proceso de generación de claves Polybius Square se utiliza la clave con matriz 6X6.

El tiempo computacional de cifrado puede definirse como el tiempo que toma el algoritmo para la conversión de texto claro en texto cifrado.

Este tiempo de cifrado se puede utilizar para calcular el rendimiento de cifrado de los algoritmos. El parámetro de rendimiento incluye el tiempo que toma el algoritmo para el cifrado y descifrado del tamaño del archivo de entrada que es el tiempo de cifrado computacional y el tiempo de descifrado computacional usado para procesar el archivo.

Tiempo para el tamaño de archivo diferente En este tamaño de archivo de entrada de 15 KB es el tiempo de ejecución de cifrado para DES, TDES, AES y algoritmo propuesto que son como 20, 22, 21, 23 s, respectivamente.

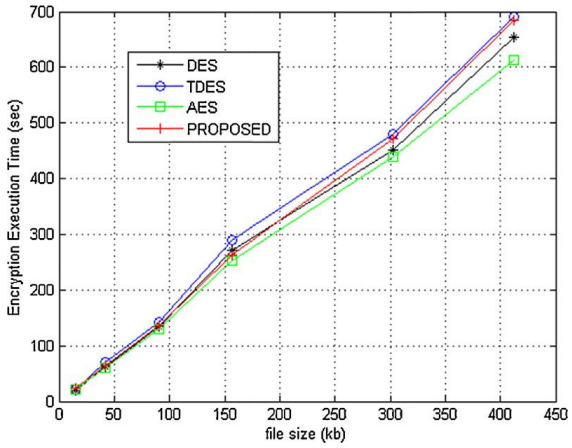


Figura 3-2: Tiempo de ejecución de cifrado de diferentes tamaños de archivo.
Fuente: (KUMAR & RANA, 2016)

La Figura 3-2 muestra cómo el tiempo de ejecución del cifrado depende del tamaño del archivo, se observa que el algoritmo propuesto consume más tiempo para todos los tamaños de los archivos, lo que aumenta la seguridad del sistema.

Por lo que se concluye, el algoritmo propuesto es más rápido.

"AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection" (MATHUR & BANSODE, 2016, págs. 1036-1043)**.**

La investigación considera que la criptografía juega un papel vital en el sistema de seguridad de la información contra varios ataques, por lo tanto, el desarrollo de nuevas técnicas de criptografía puede ayudar a reducir esta amenaza de seguridad. Este documento propone una extensión de un criptosistema de clave pública para soportar un criptosistema de clave privada que es una combinación de Advanced Encryption Standard y ECC, plantea un esquema híbrido para aumentar la competencia y minimizar los inconvenientes.

El proceso realizado en el estudio es el siguiente:

- Determinación de los parámetros para desarrollar un modelo de cifrado mixto basado en ECC y AES, utilizando ECC para cifrar y transferir la clave AES y por lo tanto AES cifra los datos de comunicación.
- Implementación del algoritmo de cifrado híbrido, que es una mezcla de Advanced Encryption Standard (AES) y criptografía de curva elíptica con claves cifradas para el intercambio seguro de claves y una mayor seguridad de texto cifrado.
- Ejecución de pruebas sobre la base del rendimiento para los diferentes tamaños de archivo.
- Análisis de resultados obtenidos.
- Definición de conclusiones.

Algoritmo hibrido propuesto:

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 prevenir posibles vulnerabilidades planteadas por el ataque de canal de tiempo. Para mayor eficiencia del cifrado de datos, se implementa un orden superior de AES que tenga 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.
El bloque de datos que el usuario desea enviar está encriptado por razones de seguridad.

- El algoritmo utilizado para el cifrado de los datos es AES.
- La clave AES generada se codifica adicionalmente con Criptografía de Curva Elíptica (ECC).
- La clave generada se proporciona al usuario que se utilizará para descifrar el bloque de teclas AES en el momento del descifrado.
- Se calcula y se almacena el tiempo total de cifrado del bloque de datos.

- Después de descifrar la clave AES, los datos cifrados son descifrados por el bloque de teclas AES en su formato original para que el usuario pueda acceder a él.
- El módulo atacante calculará el tiempo de respuesta de la salida cifrada del servidor utilizando varias teclas aleatorias junto con una clave válida.
- En el programa de correlación del módulo atacante se realiza la comparación de los detalles de tiempo para ambos casos y se genera el posible espacio de clave de acuerdo con los detalles de tiempo que se utilizarán para determinar la combinación de teclas correcta.

Los resultados que se muestran a continuación incluyen el cifrado realizado en un documento de texto como entrada utilizando Advanced Encryption Standard 192-bit en el que la clave ha sido dada por el usuario y el número de las iteraciones utilizadas para AES son 12. La siguiente imagen muestra la salida del cifrado en la ronda.

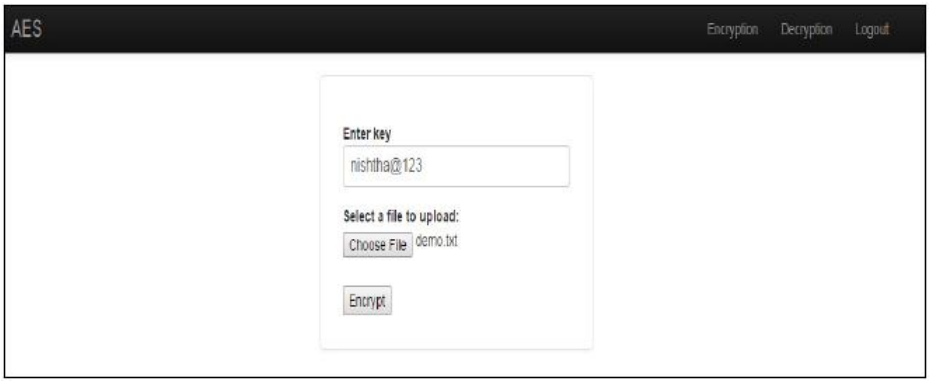


Figura 4-2: Salida del cifrado
Fuente: (MATHUR & BANSODE, 2016)

Como conclusión de la investigación define que AES, que es un algoritmo de cifrado simétrico utiliza una serie de tablas de look ups para aumentar su eficiencia de rendimiento. Dado que estas tablas no ocupan completamente la memoria caché, los accesos y fallos de caché son comunes durante el proceso de cifrado, lo que provoca varios tiempos de búsqueda y tiempos de cifrado que cambian según el texto de entrada y la clave de cifrado. El ataque de sincronización de caché correlaciona los detalles de sincronización para el cifrado utilizando una clave conocida y también con una clave desconocida para inferir la clave desconocida. En este trabajo, se utiliza un algoritmo AES mejorado para cifrar el texto sin formato y el algoritmo ECC se aplicará para cifrar la clave AES, aumentando así la seguridad general del sistema mediante la implementación de contramedidas basadas en software para prevenir posibles vulnerabilidades planteadas por el ataque de canal de tiempo. Para aumentar aún más la eficiencia del cifrado de datos, se implementará un orden superior de AES que tenga 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.

"Comparison Between DES, 3DES, RC2, RC6, BLOWFISH AND AES" (MATHUR & KESARWANI, 2013, págs. 143-148)**.**

En la investigación se considera que la confidencialidad de la información tiene un alto valor y debe ser protegida. El cifrado es la ciencia del cambio de datos para que sea irreconocible e inútil para una persona no autorizada. El descifrado lo cambia de nuevo a su forma original. Este trabajo presenta la comparación en el desempeño de los seis algoritmos más útiles: DES, 3DES, AES, RC2, RC6 y BLOWFISH. El rendimiento de diferentes algoritmos es diferente según las cargas de datos.

El proceso realizado por la investigación es el siguiente:

- Definición de los conceptos de criptografía
- Determinación de las características principales de los algoritmos: DES, 3DES, RC2, RC6, BLOWFISH AND AES.
- Comparación entre los algoritmos considerando varios criterios de evaluación como: seguridad, rendimiento de software y hardware, idoneidad en entornos de espacio restringido, resistencia al análisis de potencia y otros ataques de implementación, entre otros.
- Análisis de resultados de la simulación de los diferentes algoritmos considerando varios criterios.
- Análisis de resultados.
- Definición de las conclusiones.

Los resultados de la simulación se muestran en las siguientes figuras para los seis algoritmos de cifrados seleccionados con diferentes métodos de codificación. La Figura 5-2 muestra los resultados en la codificación de la base 64 mientras que la Figura 6-2 da los resultados de la codificación de la base hexadecimal. Se puede notar que no hay diferencia significativa en ambos métodos de codificación.

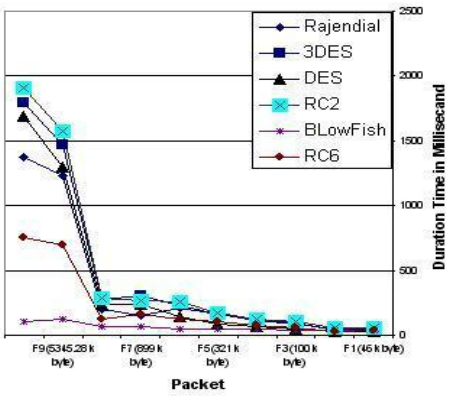


Figura 5-2: Consumo de tiempo del algoritmo de cifrado (codificación de base 64)
Fuente: (MATHUR & KESARWANI, 2013)

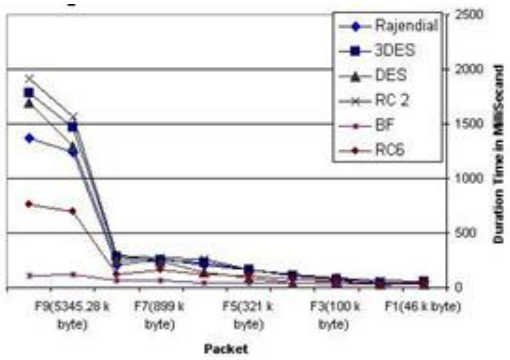


Figura 6-2: Consumo de tiempo del algoritmo de cifrado (Codificación hexadecimal)
Fuente: (MATHUR & KESARWANI, 2013)

Los resultados de tiempos de ejecución comparativos (en milisegundos) de algoritmos de cifrado con diferentes tamaños de paquete se muestran a continuación:

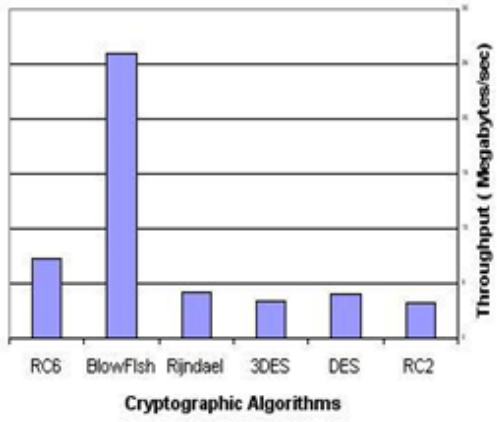


Figura 7-2: Rendimiento de cada algoritmo de cifrado (Megabit/Seg)
Fuente: (MATHUR & KESARWANI, 2013)

Se observa la superioridad del algoritmo de Blowfish sobre otros algoritmos en términos del tiempo de procesamiento, RC6 requiere menos tiempo que todos los algoritmos excepto Blowfish,

AES tiene una ventaja sobre otros 3DES, DES y RC2 en términos de consumo de tiempo y rendimiento, 3DES tiene un bajo rendimiento en términos de consumo de energía y rendimiento cuando se compara con DES. Requiere siempre más tiempo que DES debido a sus características de cifrado de triple fase. Finalmente, se encuentra que RC2 tiene bajo rendimiento y bajo rendimiento cuando se compara con otros cinco algoritmos a pesar del tamaño de clave pequeño utilizado.

Este trabajo presenta una evaluación del rendimiento de algoritmos de cifrado simétricos seleccionados. Los algoritmos seleccionados son AES, DES, 3DES, RC6, Blowfish y RC2. Varios puntos Puede deducirse de los resultados de la simulación.

- No hay diferencia significativa cuando los resultados se muestran en codificación de base hexadecimal o en codificación de base 64.
- En el caso de cambiar el tamaño del paquete, se llegó a la conclusión de que Blowfish tiene un mejor rendimiento que otros algoritmos de cifrado común utilizados, seguido de RC6.
- En el caso de cambiar tipo de datos como imagen en lugar de texto, se encontró que RC2, RC6 y Blowfish tiene desventaja sobre otros algoritmos en términos de consumo de tiempo.
- 3DES todavía tiene un bajo rendimiento en comparación con el algoritmo DES.
- Finalmente, en el caso de cambiar el tamaño de la llave se puede determinar que la aplicación de un tamaño de llave más alto conduce a un cambio claro en el consumo de batería y tiempo.

2.2. Criptología

La criptología viene del griego *krypto* y *logos*, estudio de lo oculto, lo escondido es la rama que trata los problemas teóricos respectivos con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones (TRAYNO, 2016).

En su clasificación dentro de las ciencias, la criptología proviene de una rama de las matemáticas, denominada: “Teoría de la Información” (GRANADOS P, 2006).

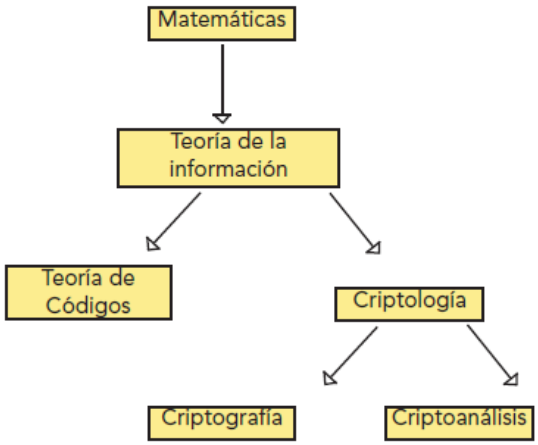


Figura 8-2: Origen de la criptografía
Fuente: (GRANADOS P, 2006)

Según la RedIRIS (Red académica y de investigación española) esta ciencia está dividida en dos grandes ramas: **criptoanálisis y criptografía** (ESPAÑOLA, 2016)**.**

2.2.1. Criptoanálisis

El criptoanálisis es el arte de tomar lo que se conoce y convertirlo en algo que se conoce, en este caso, tomando un mensaje encriptado y convirtiéndolo en uno no encriptado, texto en claro. Para descubrir el significado de un mensaje cifrado tiene que haber una comprensión de qué método de cifrado se utilizó. Y así nos quedamos con dos problemas, descubrir cómo fue cifrado un mensaje y descubrir el valor de cifrado (IEE OCC CyberSecurity SIG, 2016).

El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado; se supone por el contrario que los algoritmos siempre son conocidos (LUCENA, 2010).

2.2.2. Criptografía

La palabra criptografía proviene del griego Kripto=oculto, Graphos=escribir, lo que significaría escritura oculta. La finalidad principal de la criptografía es la de proteger la privacidad y confidencialidad de la información, es decir que la información sea accesible únicamente para el personal debidamente autorizado (GARCÍA, 2013).

Objetivos de la criptografía

Cada sistema de seguridad según Medina y Miranda (2015), debe proporcionar un conjunto de funciones de seguridad que pueden asegurar el secreto del sistema. Estas funciones se refieren generalmente como los objetivos del sistema de seguridad.

Estos objetivos pueden ser listados bajo las siguientes cinco categorías principales:

Autenticación

- Probar la identidad de uno. Esto significa que antes de enviar y recibir datos utilizando el sistema, la identidad del receptor y el remitente debe ser verificada.

Privacidad/confidencialidad:

- Asegurar que nadie puede leer el mensaje, excepto el receptor previsto. Por lo general, esta función es como la mayoría de la gente se identifica un sistema seguro. Esto significa que sólo las personas autenticadas son capaces de interpretar el contenido del mensaje y de nadie más.

Integridad

- Asegurar al receptor que el mensaje recibido no ha sido alterado de ninguna manera de la original. La forma básica de la integridad es paquete de suma de comprobación en los paquetes IPv4.

No repudio

- Probar que el remitente realmente envió este mensaje. Significa que ni el emisor ni el receptor puedan falsamente negar que hayan enviado un mensaje determinado.

Servicio fiabilidad y disponibilidad

- Asegurar la información contra intrusos, que pueden afectar la disponibilidad y el tipo de servicio a sus usuarios. Estos sistemas proporcionan a sus usuarios la calidad de servicio que esperan.

2.2.2.1. Criptografía asimétrica

La criptografía asimétrica o de clave pública establece a cada extremo un par de llaves, una llave pública que cualquiera puede conocer y/o solicitar, y la otra llave privada, donde la seguridad es fundamental para el éxito de la codificación (PADILLA, 2012).

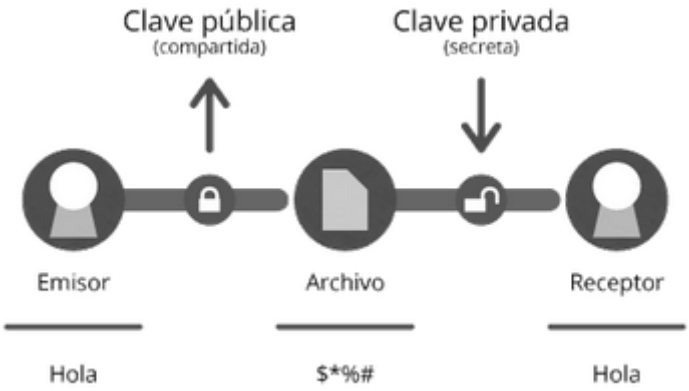


Figura 9-2: Criptografía asimétrica
Fuente: *https://www.genbetadev.com/seguridad -informatica/tipos -de-criptografia-simetrica-asimetrica-e-hibrida*

Los algoritmos asimétricos se basados en funciones matemáticas que son fáciles de resolver en un sentido, pero también son muy complicadas realizarlas en un sentido inverso, salvo que se conozca la llave. Las claves públicas y privadas son generadas simultáneamente y están ligadas la una a la otra (DE LUZ, 2010).

La criptografía asimétrica presenta las siguientes ventajas y desventajas: (COMUNIDAD ECURED, 2016)

VENTAJAS

- La repartición de claves es más fácil y ofrece mayor seguridad, ya que la clave que se distribuye es la pública conservando la privada para el uso especial del propietario.

DESVENTAJAS

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- El mensaje que se encuentra cifrado presenta más espacio ocupado que el mensaje original.

2.2.2.2. Criptografía simétrica

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave secreta para cifrar y descifrar un documento, como se muestra en la Figura 1 (GRANADOS, 2006).

Figura 10-2: Criptografía simétrica
Fuente: *Granados G.*

Este tipo de criptografía sólo utiliza una llave para cifrar y descifrar, esto es: si se cifra un mensaje *m* con una llave secreta *k* entonces el mensaje cifrado resultante m' únicamente se lo podrá descifrar con la misma llave k. Este tipo de llave conocida como secreta se debe de compartir entre las personas que se desea que vean los mensajes.

Con este tipo de criptografía se puede garantizar la confidencialidad porque únicamente quien posea la llave secreta será capaz de ver el mensaje.

Entre las principales ventajas y desventajas de los algoritmos de criptografía simétrica están los siguientes: (MATAMALA, 2012)

VENTAJAS

- Alta velocidad.
- El tamaño del mensaje no se incrementa.

DESVENTAJAS

- Es necesario que el receptor tenga conocimiento de la clave que se va a utilizar.
- Cuando se tiene un número de m personas que requieren comunicarse entre sí, se requieren m/2 claves distintas por cada pareja de personas que necesitan comunicarse de forma privada.

Principales algoritmos de clave simétrica

Los algoritmos de clave simétrica definidos entre los principales se mencionan los siguientes:

- 3DES (Triple Data Encryption Standard)
- RC6
- BLOWFISH
- AES (Advanced Encryption Standard)

2.2.2.2.1. Triple Data Encryption Standard (3DES)

Fue desarrollado por IBM en 1978, creado con la finalidad de mejorar el cifrado DES, escogido con la finalidad de ampliar la clave sin que sea necesario cambiar el algoritmo de cifrado (ROMERO & ALVARADO, 2016).

Está basado en la aplicación del algoritmo DES, tres veces, la clave posee una longitud de 128 bits. Si el mismo bloque de datos es cifrado dos veces con dos llaves distintas (de 64 bits), el tamaño de la clave se incrementa. El 3DES se inicia con una llave de 128 bits, que se divide en dos llaves, A y B. Cuando recibe los datos, se emplea el algoritmo DES con una llave A, luego se repite con la llave B y después otra vez con la llave A (de nuevo). 3DES acrecienta de forma significativa la seguridad del método DES, pero también requiere el aumento de recursos del ordenador (AGUIRRE, 2006).

Las partes más importantes del algoritmo3DES son: (ROMERO & ALVARADO, 2016)

1. La segmentación del texto en bloques de 64 bits (8 bytes)
2. Una permutación preliminar de los bloques,
3. El fraccionamiento de los bloques en dos partes: izquierda y derecha, que se denominan I y D en el orden respectivo,
4. Las fases de permutación y de sustitución que se repiten 16 veces (que se denominan rondas),
5. La reconexión de las partes izquierda y derecha, luego de la permutación inicial inversa.

A continuación, se presenta el funcionamiento de una de las variantes más simple del algoritmo 3DES:

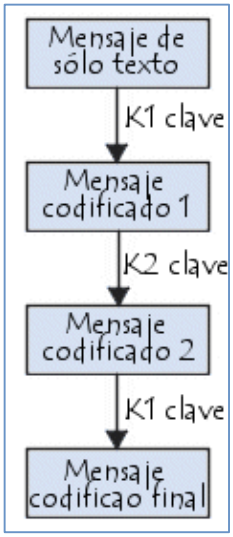


Figura 11-2:. Proceso 3DES
Fuente: http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion1.html

Donde para cifrar el mensaje se utiliza las claves DES: k1, k2 y k3 de forma respectiva. En la tercera variante 3TDES las tres claves son diferentes; en la segunda variante 2TDES, la primera y tercera clave son similares.

Por lo general, se tienen distintos tipos de cifrado 3DES: (ROMERO & ALVARADO, 2016)

- DES-EEE3: Cifrado triple DES que consta con 3 claves diferentes,
- DES-EDE3: Consta de una clave diferente para cada operación de triple DES (cifrado, descifrado, cifrado),
- DES-EEE2 y DES-EDE2: Consta de una clave distinta para la segunda operación (descifrado).

2.2.2.2.2. RC6

RC6 es un algoritmo de cifrado de bloques que usa llaves simétricas que tienen longitud máxima de 256 bits y también un tamaño de bloque cifrado de 128 bits. Fue creado por Ron Rivest, Ray Sidney, y Yiqun Lisa Yin para RSA que cumple con las exigencias de AES.

Enfatiza la sencillez en sus mecanismos de cifrado, descifrado y en la generación de sub-llaves, también tiene una alta velocidad de cifrado y descifrado. Pero su seguridad ha estado grandemente cuestionada (CASTANEDO, 2007).

RC6 es muy similar a RC5 en estructura, usando rotaciones dependientes de datos, adición modular y operaciones XOR; De hecho, RC6 podría ser visto como entrelazar dos procesos de cifrado RC5 paralelos. Sin embargo, RC6 utiliza una operación de multiplicación extra que no está presente en RC5 para hacer que la rotación dependa de cada bit en una palabra, y no sólo los menos significativos pocos bits (MATHUR & KESARWANI, 2013)

El cifrador de bloque RC6 en sí consta de: (CASAS, 2010)

- Una transformación inicial, denominada entrada.
- 20 rondas de mezcla
- Una transformación final, denominada salida

.

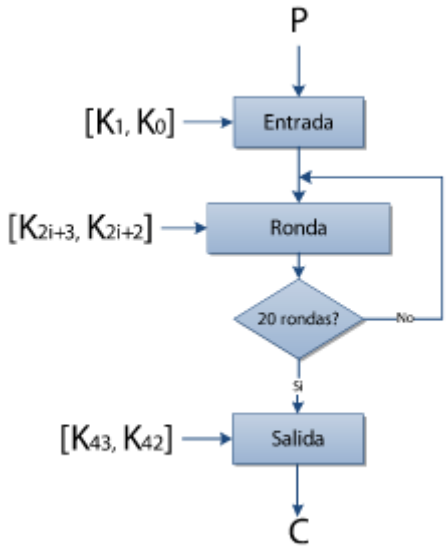


Figura 12-2: Algoritmo de cifrado RC6
Fuente: (CASAS, 2010)

Donde la entrada consiste en realizar dos sumas entre dos de las palabras que conformas el texto plano y dos de las subclaves $K_{i.}$

Luego el cifrador RC6 ejecuta 20 rondas donde 128 bits de datos se combinan utilizando 2 subclaves K_i en cada iteración. En la salida se efectúan dos sumas entre dos de las palabras que conforman el texto que va cifrado y dos de las subclaves $K_{i.}$ El proceso de descifrado es el mismo en forma inversa.

2.2.2.2.3. BLOWFISH

Es un algoritmo de cifrado por bloques de 64 bits que fue desarrollado por Scheiner, es de tipo Feistel y cada rotación radica en una permutación que requiere de la clave y de una sustitución y también depende de la clave y los datos. Las operaciones se fundan en o-exclusivas sobre palabras de 32 bits. La clave posee tamaño variable (siendo el máximo de 448 bits) y se utiliza para generar vectores de subclaves. Este algoritmo se creó para máquinas de 32 bits y es más rápido que el DES. El algoritmo se considera seguro pero se han descubierto algunas claves débiles. (CASTANEDO, 2007).

Blowfish utiliza claves de longitud variable, que van desde 32 a 448 bits, cuya planificación de claves incluye la generación de cajas S y P (utilizadas en la red Feistel) que dependen directamente de la clave. El mensaje en claro se divide en bloques de 64 bits, los cuales entran a la red de cifrado en bloques de 32 bits para combinarse con las subclaves P mediante XOR, y en la red Feistel sustitución por medio de sumas modulares entre las salidas de las cajas (JIMENEZ, 2013).

La Figura13-2 muestra el cifrado Blowfish:

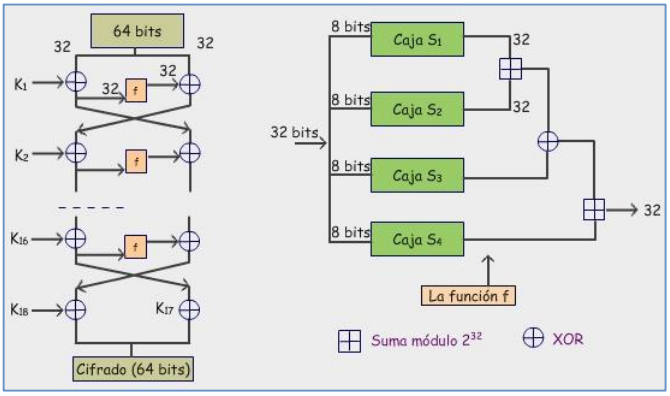


Figura 13-2: Cifrado Blowfish
Fuente: *http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/4-criptografia-simetrica-o-de-clave-secreta/41-introduccion-a-la-criptografia-simetrica/413-principales-algoritmos-simetricos?showall=&start=2*

Los primeros bloques de datos se dividen en 2 grupos de igual tamaño (32 bits), éstos se procesan en 16 rondas, manejando en cada iteración una subclave P (se utilizan 28 en total). Se manejan dos operaciones básicas, la XOR y la adición.

En la función F se integra una serie de 32 bits la cual se divide en 4 bloques de 8 bits, se procede a sustituir S-Box, después se realiza una suma entre el resultado de la S-Box 1 y S-Box 2 y una operación XOR entre el resultado anterior y el resultado de la S-Box 3 y se ejecuta el mismo procedimiento con el resultado de S-Box 4.

2.2.2.2.4. Advanced Encryption Standard (AES)

Es un algoritmo de cifrado simétrico. Fue desarrollado por Joan Daeman y Vicent Rijment, ambos de origen belga, bajo el nombre Rijndael (GUTIÉRREZ, 2009).

AES es un sistema de cifrado por bloques, diseñado para manejar longitudes de clave y de bloque variables, ambas comprendidas entre los 128 y 256 bits. Realiza varias de sus operaciones internas a nivel de byte, interpretando éstos como elementos de un cuerpo de Galois GF(2^8) el resto de operaciones se efectúan en términos de registros de 32 bits. Es resistente frente a ataques de tipo lineal y diferencial (LUCENA, 2010).

Al contrario de su predecesor DES, AES es una red de sustitución-permutación, no tiene una estructura tipo Feistel. AES es rápido con respecto a software y hardware, relativamente más fácil para implementar y necesita poca memoria (GUTIÉRREZ, 2009).

La estructura del algoritmo AES está formado por un conjunto de rondas, las mismas que está formadas por varias iteraciones de cuatro funciones matemáticas que son diferentes e invertibles. Se basa en la aplicación de un número específico de rondas a una información que se encuentra

en claro para generar una información cifrada. La información que se genera por cada función es un dato intermedio, que se define como Estado o Estado Intermedio (VÁZQUEZ, 2007).

Características

El algoritmo AES presenta las siguientes características: (BLANCO, 2010)

- 4 funciones matemáticas diferentes y que pueden ser reversibles.
- 4 filas por bloque.
- El tamaño del bloque podrá ser incrementado o disminuido en múltiplos de 4 bytes (32 bits).
- El número de columnas está dado por la fórmula Nk= *tamaño_bloque_en_bits/32.*
- Para la subclave, el tamaño de bloque dependerá de la fórmula Nb= *tamaño_clave_en_bits/32.*
- El número de rondas está determinado por la siguiente expresión Nr= *max(Nk, Nb) +6*, donde *max* devolverá el valor de la variable más grande. Es decir, *Nr* = 10 para una longitud de clave de 128 bits, *Nr* = 12 para 192 bits y *Nr* = 14 para 256 bits.

El estado se representa con una matriz rectangular de bytes, que consta de cuatro filas y de Nb columnas. Por ejemplo, si nuestro boque tiene 128 bits, Nb = 128/32 = 4 columnas, quedando la siguiente matriz:

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Figura 14-2:. Matriz de Estado
***Fuente**: https://www.iit.comillas.edu/pfc/resumenes/46ea7511774d8.pdf*

La clave consta de una estructura análoga a la del Estado y está representada por una tabla de cuatro filas y Nk columnas. Si se tiene una clave de 128 bits, Nk= 128/32=4 columnas. Se representa con la Figura 15-2.

k_{00}	k_{01}	k_{02}	k_{03}
k_{10}	k_{11}	k_{12}	k_{13}
k_{20}	k_{21}	k_{22}	k_{23}
k_{30}	k_{31}	k_{32}	k_{33}

Figura 15-2: Algoritmo de clave
Fuente: *https://www.iit.comillas.edu/pfc/resumenes/46ea7511774d8.pdf*

En todas las rondas salvo en la última, el algoritmo ejecuta una serie de operaciones que van modificando la matriz de estado, contribuyendo con difusión al mensaje a cifrar (BONILLA, 2012).

Proceso de cifrado

Las operaciones que se aplican en el proceso de cifrado son:

- SubByte o sustitución de bytes.
- ShiftRows o desplazamiento de filas
- MixColumns etapas de mezcla de columnas
- AddRoundKey etapa de adición de claves.

La Figura 16-2 muestra cómo se distribuyen las operaciones que se realizan en el proceso de cifrado durante las 10 rondas necesarias para una clave de 128 bits.

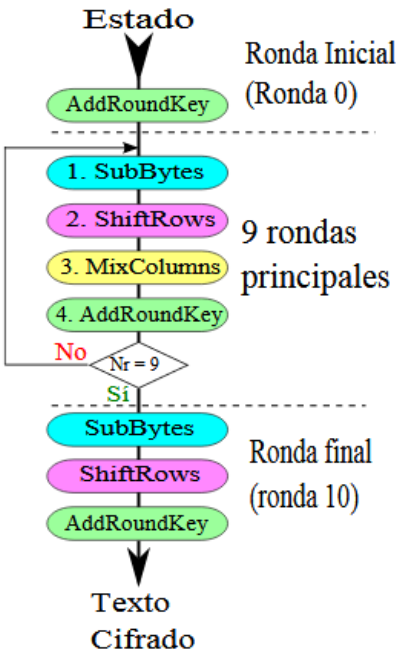


Figura 16-2: Proceso de cifrado AES
Fuente: *https://core.ac.uk/download/pdf/30046976.pdf*

En primer lugar, se realiza una ronda inicial en la que solo se aplica una operación AddRoundKey. Luego se realizan 9 rondas principales con las cuatro operaciones y, por último, se realiza una ronda final en la que se aplica las operaciones SubByte, ShiftRows y AddRoundKey para conseguir así el texto cifrado.

Calculo de subclaves

De acuerdo con el principio de la criptografía moderna, donde determina que la seguridad de un algoritmo sólo debe depender de la clave, se usan distintas subclaves Ki, tanto en el cifrado como en el descifrado para que de esta forma el resultado que genera el algoritmo dependa de una información externa al procedimiento, es decir la clave del usuario. Las subclaves proceden de la clave principal K por medio del uso de dos funciones: de expansión y de selección.

Por lo tanto, el número de claves que sean generadas depende del número de rondas que se emplee (Nr).

Función AddRoundkey

Realiza una operación OR-Exclusiva con los elementos de la matriz de estado de la anterior transformación y los elementos de la matriz de la subclave de ronda, como se ve en la Figura 17-2:

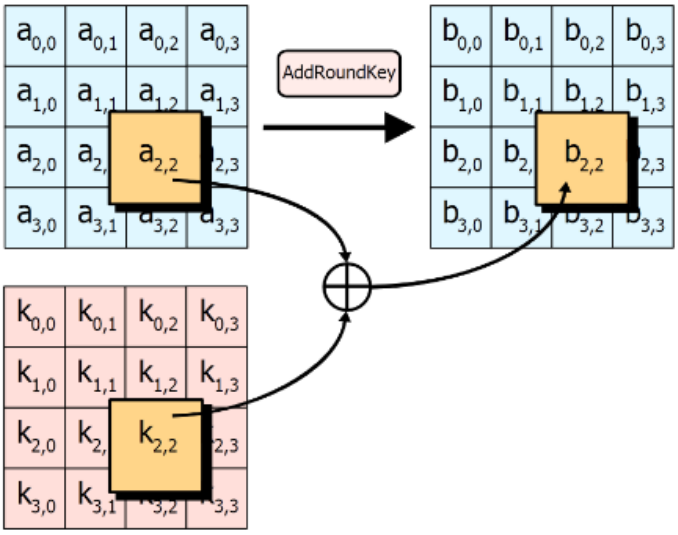


Figura 17-2: AddRoundkey

Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

Función SubByte

Realiza una sustitución no lineal a nivel de byte, que se aplica independientemente a todos los bytes que forman la matriz de estado y generan una nueva matriz de bytes. Tal como se muestra en la Figura 18-2.

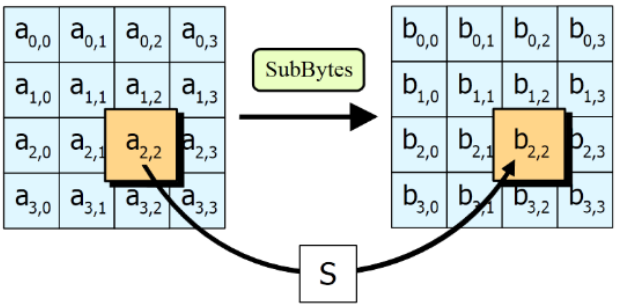


Figura 18-2: SubByte
Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

En la transformación se realiza la sustitución de cada byte por el resultado de aplicar la tabla de sustitución S-Box.

La tabla S-Box no puede ser invertida y se crea por medio de las siguientes dos transformaciones:

- Sustituir los elementos de la matriz de estado por sus inversos para multiplicar GF(2^8). Cuando el valor es {00} no tiene inverso, entonces éste se sustituye por sí mismo.
- Luego se aplica la próxima transformación afín en GF(2^8) al resultado de la transformación anterior.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figura 19-2: Transformación
Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

Por medio de las dos transformaciones que se aplicaron a todos los valores posibles de entrada, se deduce una tabla de sustitución que se denomina S-Box que agilita el proceso de cifrado.

Se utiliza la tabla para aplicar la función SubByte donde se divide la matriz de estado en dos partes de cuatro bits. Los más significativos se representan con X, y los menos significativos se representan con Y. El valor de la fila por la columna en la tabla resulta de aplicar S-box a un byte, como se muestra en la Figura 20-2

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figura 20-2: Sustitución S-box
Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

Función ShiftRows

Se realiza el desplazamiento de manera cíclica hacia la izquierda de los bytes de cada una de las filas de la matriz de estado. Es decir que la primera fila permanece igual, la segunda fila se rota hacia la izquierda una posición, la tercera se rota hacia la izquierda dos posiciones y, por último, la cuarta fila se rota hacia la izquierda tres posiciones, como se muestra en la Figura 21-2

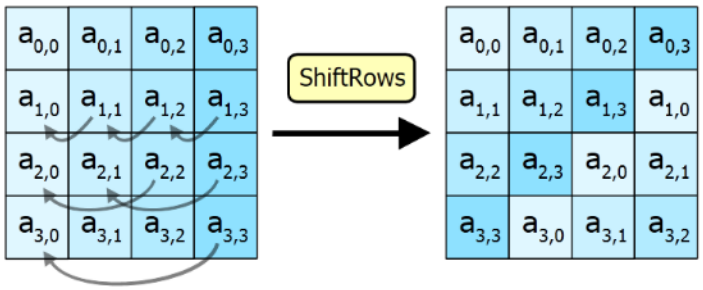


Figura 21-2: ShiftRows
Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

Función MixColumns

Esta transformación se realiza sobre los bytes de una misma columna de la matriz de estado. Permitiendo mezclar los bytes de las columnas, como se muestra en la Figura 22-2

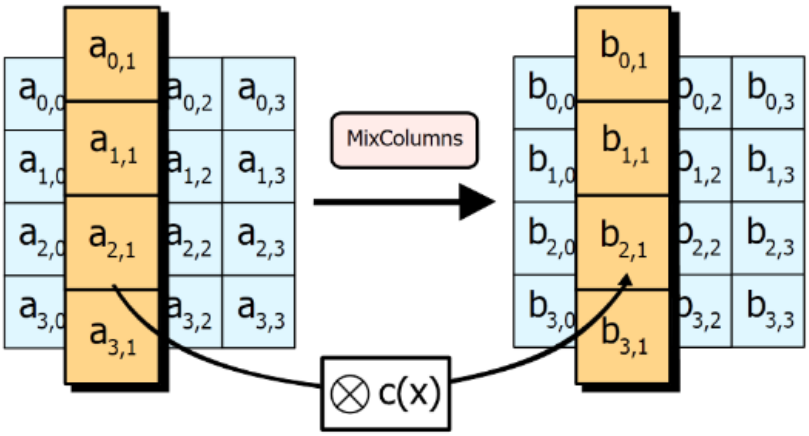


Figura 22-2: MixColumns
Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

Las columnas de la matriz de estado se consideran como polinomios, con coeficientes del campo GF (2^8). Se realiza la multiplicación del módulo $M(x)=x4 + 1$ con un polinomio fijo $a(x)= 03x^3 + 01x^2 + 01x + 02$

De forma matricial, se representa con los coeficientes b_i, los valores de las columnas i de la matriz de estado de salida y los coeficientes a_i los valores de la matriz de estado de salida.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Figura 23-2: Matriz de etapa
Fuente:
https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2

Proceso de descifrado

El proceso de descifrado consiste en aplicar en orden inverso al de cifrado. Se tiene las siguientes operaciones:

- InvSubBytes
- InvShiftRows
- InvMixColumns
- AddRoundkey

En la Figura 24-2 se muestra como se distribuye las operaciones del proceso de descifrado, si se tiene la longitud de la clave de 128 bits con N*r* = 10 rondas:

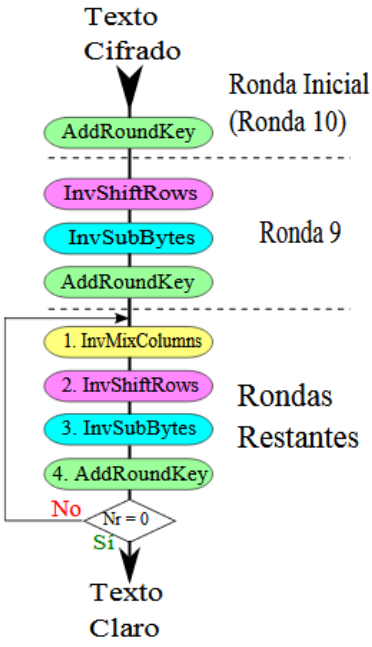


Figura 24-2: Proceso de descifrado AES
Fuente: *https://core.ac.uk/download/pdf/30046976.pdf*

El proceso empieza en la última ronda, es decir que la operación AddRoundKey, utilizará la subclave número 10. Posteriormente se aplican al estado las operaciones InvShiftRows, InvSubBytes y AddRoundKey

InvSubBytes

Para calcular la función inversa de SubBytes, se aplica una tabla inversa de la Figura 25-2 a la que se utilizó en el proceso de cifrado. Por último, hasta la ronda 0 se realizan las diversas operaciones de descifrado en el orden: InvMixClolumns, InvShiftRows, InvSubBytes y AddRoundKey.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figura 25-2: S-Box inversa
Fuente: https://core.ac.uk/download/pdf/30046976.pdf

InvShiftRows

En la función InvShiftRows se desplaza los bytes de las filas 1, 2 y 3 en un total de 1, 2 y 3 posiciones hacia la derecha.

InvMixColumns

En esta función se trabaja sobre los bytes de la misma columna, donde se considera a las columnas como polinomios con coeficientes en GF(2^8), se multiplican por el polinomio $d(x) = 0Bx^3 + 0Dx^2 + 09x + 0E$ siendo éste el inverso de c(x).

Matemáticamente sería:

$S(x) = d(x)\ \ S'(x)$

Donde:

S(x) = la matriz de estado que resulta de esta etapa

S'(x) = la matriz de estados de entrada.

La fórmula se representa con la matriz de la Figura 26-2.

$$\begin{pmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{pmatrix} = \begin{pmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{pmatrix} \cdot \begin{pmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{pmatrix}.$$

Figura 26-2: Matriz S-Box inversa
Fuente: https://www.iit.comillas.edu/pfc/resumenes/46ea7511774d8.pdf

2.2.3. Determinación del algoritmo criptográfico base

Luego de revisar la información de varios estudios principales sobre algoritmos criptográficos simétricos y considerando sus características se realiza una comparación entre ellos para determinar el algoritmo criptográfico base. Los algoritmos seleccionados son:

- 3DES (Triple Data Encryption Standard)
- RC6
- BLOWFISH
- AES (Advanced Encryption Standard)

Para la selección del algoritmo base se ha considerado los siguientes parámetros:

- Tipo de clave
- Longitud de clave
- Tamaño del bloque
- Nº. de rondas
- Resistencia a criptoanálisis
- Seguridad
- Tiempo requerido para determinar todas las posibles claves

A continuación, se muestra la Tabla 1-2 de comparación:

Tabla 1-2: Comparación de algoritmos criptográficos

Algoritmo	**Tipo de clave**	**Longitud de la clave**	**Tamaño del bloque utilizado**	**No. de rondas utilizadas**	**Resistencia a Criptoanálisis**	**Seguridad**	**Tiempo que se requiere para determinar las posibles claves**
3DES	Simple (dividida en tres partes)	(k1, k2, k3) 168 bits, (k1 y k2 son las mismas) 112 bits	128, 192, 256 bits	48	Vulnerable a: criptoanálisis diferencial	Debilidad en la salida en DES	Para una clave de 112 bits: 800 días
AES	Simple	128, 192, 256 bits	128, 192, 256 bits	10, 12, 14	Fuerte contra: criptoanálisis diferencial, lineal y truncado diferencial	Seguro	Para una clave de 128 bits: $5 * 10^{21}$ años
RC6	Simple	128,192,256 bits	128 bits	20	Vulnerable a: criptoanálisis diferencial, fuerza bruta	Vulnerable	Para una clave de 192 bits: 10^{40} años
BLOWFISH	Simple	32 – 448 bits	64 bits	16	Vulnerable a: Diferencial, Fuerza bruta	Vulnerable	Para una clave de 448 bits: 10^{116} años

Fuente: (MATHUR & KESARWANI, 2013)
Realizado por: Cushpa Ana, 2018

Una ventaja del algoritmo AES comparado con los demás algoritmos radica en que es el único que trabaja con claves y también bloques de cifrado de 128, 192, 256 bits imparcialmente, se puede usar 9 configuraciones diferentes, resultado de combinar cualquier longitud de clave con cualquier longitud de bloque. Además, sus operaciones son fáciles de defender contra distintos de ataque.

De acuerdo a sus características superiores frente a otros algoritmos se ***tomará como base el algoritmo AES*** para el correspondiente diseño e implementación del nuevo algoritmo con mayor seguridad para demostrar la hipótesis planteada.

2.3. Arquitectura de un entorno web

Según ML Castro Pérez (2008) una plataforma tecnológica es un sitio web cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios, entre los que suelen encontrarse buscadores, foros, documentos, aplicaciones, compra electrónica, etc.

Una plataforma web es el entorno de desarrollo del software empleado para diseñar y ejecutar un sitio web, provisto de interacción a través del uso de lenguajes interpretados. Una aplicación web es proporcionada por un servidor web y utilizadas por usuarios que se conectan desde cualquier punto vía clientes web (browsers o navegadores) (VIGNAGA & PEROVICH, 2010).

La arquitectura de un sitio web tiene tres componentes principales:

- Un servidor web
- Una conexión de red
- Uno o más clientes

El servidor web distribuye páginas de información formateada a los clientes que las solicitan. Los requerimientos son hechos a través de una conexión de red, y para ello se usa el protocolo HTTP. Una vez que se solicita esta petición mediante el protocolo HTTP y la recibe el servidor Web, éste localiza la página web en su sistema de archivos y la envía de vuelta al navegador que la solicitó, como se muestra en la Figura 27-2.

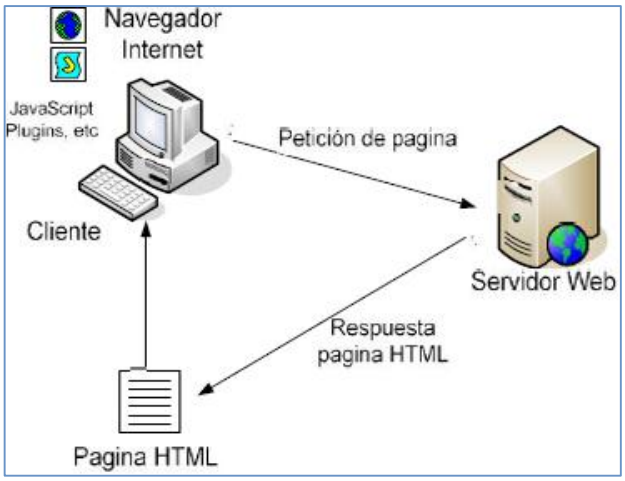


Figura 27-2: Arquitectura de una aplicación web
Fuente: *http://www.mailxmail.com/curso-php-mysql-sql-8/arquitectura-base-datos-web*

Un entorno web está basado en el modelo Cliente/Servidor que gestionan servidores web, y que utilizan como interfaz páginas web.

Las páginas web son el componente principal de una aplicación o sitio web. Los browsers piden páginas (almacenadas o creadas dinámicamente) con información a los servidores web. En algunos ambientes de desarrollo de aplicaciones web, las páginas contienen código HTML y scripts dinámicos, que son ejecutados por el servidor antes de entregar la página.

Las colecciones de páginas son en una buena parte dinámicas (ASP, PHP, etc.), y están agrupadas lógicamente para dar un servicio al usuario. El acceso a las páginas está agrupado también en el tiempo (sesión) (VIGNAGA & PEROVICH, 2010).

2.4. Mensajería instantánea

IM son las siglas en inglés de *instant messaging* y es un servicio de comunicación de tiempo real entre dispositivos como computadoras, tabletas, celulares, etc. La mensajería instantánea ha evolucionado desde los 90's y hoy en día se ha sofisticado y adoptado como parte del uso cotidiano. La mensajería instantánea se basa en el uso de programas conocidos como clientes de IM (IM clients, en inglés) que se instalan en una computadora o dispositivo móvil. Para que dos personas se puedan comunicar usando IM, cada uno debe tener instalado uno de estos programas, que se conectan entre sí para enviar mutuamente mensajes de texto e imágenes pequeñas (FERNÁNDEZ, 2009).

2.5. Análisis y diseño de algoritmos

El análisis de algoritmos pretende descubrir si estos son o no eficaces, estableciendo una comparación entre los mismos con el fin de saber cuál es más eficiente, aunque cada uno de los algoritmos sirva para resolver el mismo problema. Los aspectos a tomar en cuenta para estudiar la eficiencia de un algoritmo son el tiempo que se emplea en resolver el problema y la cantidad de recursos de memoria que ocupa. El tiempo de ejecución depende de los datos de entrada, de la implementación del programa, del procesador y de la complejidad del algoritmo (GÓMEZ & CERVANTES, 2014).

2.6. Complejidad

La complejidad considerando el tiempo de un algoritmo es similar para todas las instancias con un tamaño n del problema. En distintos casos, la complejidad de un algoritmo con tamaño n es diferente considerando las instancias de tamaño n que el problema resuelve. Esto conlleva a realizar un estudio de la complejidad en el peor caso, caso promedio y en el mejor caso (MÉNDEZ, 2015).

Dado T(n) = tiempo de ejecución en función del tamaño n del problema se tiene:

- **Caso peor:** es el valor máximo de tiempo en el cual se ejecuta el algoritmo.
- **Caso mejor:** es el menor tiempo en el cual las instrucciones son ejecutados por el algoritmo.
- **Caso medio:** es el equivalente a la esperanza matemática de los tiempos ejecutados por el algoritmo.

2.6.1. Ordenes de complejidad

En la complejidad se define el orden como O(f(n)). Las funciones de complejidad más comunes en las que el único factor del cual dependen es el tamaño de la muestra que tiene entrada n son: (AGUIRRE, 2006)

- O(1) = Orden constante
- O(log n) = Orden logarítmico
- O(n) = Orden lineal
- O(n log n) = Orden cuasi-lineal
- O(n2) = Orden cuadrático
- O(n3) = Orden cúbico
- O(na) = Orden polinómico
- O(2n) = Orden exponencial
- O(n!) = Orden factorial.

CAPITULO III

DISEÑO DE INVESTIGACIÓN

En el presente Capítulo, se especifica el tipo de investigación, diseño, métodos, técnicas e instrumentos utilizados, además se crea e implementa un nuevo algoritmo considerando el algoritmo criptográfico base, los prototipos creados definirán los escenarios de pruebas.

MARCO METODOLÓGICO

3.1. Tipo y diseño de la investigación

El tipo de la investigación será cuasi-experimental debido a que, en base a las características definidas en el estudio, se escogerá un algoritmo criptográfico simétrico que servirá como base para crear el nuevo algoritmo criptográfico simétrico, el cual se incorporará en una aplicación de mensajería instantánea con la finalidad de mejorar la seguridad de la misma. El diseño será transversal debido a que los resultados obtenidos en las pruebas realizadas en base a la muestra determinada serán comparados en un único momento.

3.2. Métodos de investigación

Para el desarrollo de esta investigación se aplicará los siguientes métodos:

- **Método analítico:** porque que se realizará un análisis de los algoritmos criptográficos simétricos existentes, su funcionalidad y características para determinar un algoritmo criptográfico simétrico base.
- **Método inductivo:** a partir del algoritmo criptográfico base seleccionado, se diseñará un nuevo algoritmo que mejore el nivel de seguridad de la información.

3.3. Enfoque de la investigación

El estudio se considerará un enfoque cuantitativo debido a que se verificará el nivel de mejora de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web.

3.4. Alcance de la investigación

El alcance de la investigación es correlacional debido a que determina el grado de relación entre los algoritmos criptográficos simétricos definidos, en los que se observa los elementos más importantes para obtener valores de los fenómenos en estudio.

3.5. Población de estudio

Debido a la naturaleza de la investigación, se considera que la población es desconocida, porque las pruebas realizadas con los prototipos se pueden ir generando indefinidamente en el tiempo.

Las pruebas se realizarán a los mensajes cifrados por los algoritmos criptográficos simétricos, lo que permitirá determinar la validación del instrumento propuesto.

3.6. Unidad de análisis

La unidad de análisis serán los mensajes cifrados por los algoritmos criptográficos simétricos implementados.

3.7. Selección de la muestra

Para validar la implementación del nuevo algoritmo criptográfico simétrico se realizarán pruebas de los mensajes cifrados, en las cuales se determinará si existe mejora o no.

3.8. Tamaño de la muestra

Para determinar el cálculo del tamaño de la muestra cuando se desconoce el tamaño de la población, se utiliza la siguiente fórmula:

$$n = \frac{Z_a^2 \cdot p \cdot q}{d^2}$$

Dónde:

z = nivel de confianza

p = probabilidad de éxitos o porción esperada

q = probabilidad de fracaso

d = decisión (error máximo admisible en términos de proporción)

Para la investigación se utilizará los siguientes valores:

z = 1,96 (seguridad del 95%)

p = q = 0,5 (maximiza el tamaño de la muestra)

d = error del 5%

$$n = \frac{1{,}96^2 \cdot 0{,}05 \cdot 0{,}95}{(0{,}05)^2} = 384{,}16$$

Por lo que el tamaño de la muestra será de 384 pruebas.

Los indicadores que serán evaluados serán:

- Entropía
- Histograma
- Autocorrelación

- Resistencia contra fuerza bruta

Para cada uno de los indicadores se tomará como parámetro de la población la media, para realizar el análisis correlacional se utilizará el software libre R stadistical.

3.9. Técnica de recolección de datos primarios y secundarios

Las siguientes técnicas se utilizarán en la presente investigación:

- **Búsqueda de información:** permite adquirir la información necesaria de los algoritmos criptográficos simétricos existentes, utilizando las fuentes primarias y secundarias disponibles.
- **Pruebas:** permite realizar experimentos en escenarios de laboratorio, en el primer escenario utilizando el algoritmo criptográfico simétrico base y en el segundo escenario utilizando el nuevo algoritmo criptográfico simétrico.
- **Observación:** ayuda a determinar resultados de las pruebas que se realizan en los escenarios.
- **Análisis:** ayuda a establecer los resultados de la investigación, para medir el nivel de mejora del nuevo algoritmo criptográfico simétrico.

3.10. Instrumentos de recolección de datos primarios y secundarios

Los instrumentos de recolección de datos para la presente investigación son:

Se utilizará el siguiente software:

- **Netbeans:** (IDE) Es un Entorno de Desarrollo Integrado de código abierto. Tolera el desarrollo de varios tipos de aplicación Java como: J2SE, web, EJB y también aplicaciones móviles. (NETBEANS, 2015)
- **PostgreSQL**: es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia BSD y con su código fuente disponible libremente. Es el sistema de gestión de bases de datos de código abierto más potente del mercado. Utiliza un modelo cliente/servidor y usa multiprocesos en vez de multihilos para garantizar la estabilidad del sistema. Un fallo en uno de los procesos no afectará el resto y el sistema continuará funcionando (POSTGRESQL, 2010).
- **Cryptool:** Es una aplicación que ayuda a entender el proceso de cifrado de archivos y datos de forma gráfica a los usuarios y trasladar lo aprendido a la práctica de forma que el proceso sea fácil de comprender para cualquier usuario. (VELASCO, 2014).
- **R Stadistical:** R es un lenguaje y un entorno para la informática estadística y los gráficos. Es un proyecto GNU que es similar al lenguaje S y el entorno que fue desarrollado en Bell Laboratories (anteriormente AT & T, ahora Lucent Technologies) por John Chambers y colegas. R proporciona una amplia variedad de modelos estadísticos (modelos lineales y no

lineales, pruebas estadísticas clásicas, análisis de series de tiempo, clasificación, agrupación, ...) y técnicas gráficas, y es muy extensible. R está disponible como Software Libre bajo los términos de la GNU General Public License de la Fundación de Software Libre en forma de código fuente (R-PROJECT, 2016).

3.11. Instrumentos para procesar datos recopilados

Se utilizará R Stadistical que es un software que proporciona una amplia variedad de modelos lineales y no lineales, pruebas estadísticas clásicas, análisis de series de tiempo, etc. para procesar los datos obtenidos de las pruebas realizadas a los mensajes cifrados por los algoritmos criptográficos simétricos implementados, en base a la muestra determinada para medir el nivel de seguridad de la información y demostrar la hipótesis.

3.12. Validación de los Instrumentos Software

Los instrumentos que se utilizan en el trabajo de investigación se han seleccionado de acuerdo a las características más importantes.

Netbeans

Se ha elegido debido a las siguientes características: (MENDOZA, 2014)

- Apoyo de la comunidad con el soporte
- Código abierto y gratuito.
- Multiplataforma.
- Multilenguaje.
- Disponibilidad de recursos como documentación, video tutoriales, traductores de herramientas.
- Fácil de usar y adaptable.

PostgreSQL

Aporta con las siguientes características: (ECURED, 2014)

- Es gratuito y libre
- Modelo Orientado a Objetos
- Alta concurrencia
- Amplia variedad de tipos de datos
- Acceso encriptado vía SSL.
- Copias de seguridad en caliente
- Bases de datos relacionales open-source.

Necesarias para realizar la conexión y desarrollo de la base de datos.

CrypTool

Se destaca las características más importantes: (ESSLINGE, 2014)

- Es un software libre que contiene conceptos criptográficos.
- Es un programa de aprendizaje electrónico de uso extenso en el mundo en el área de la criptología.
- Un gran número de algoritmos y de herramientas para el análisis están implementados, de forma eficiente.

Con el cual se realizan las pruebas necesarias para validar el nuevo algoritmo.

R Stadistical

Las características que presenta son las siguientes (VALLEJOS, 2012):

- Es un entorno integrado, no una colección de herramientas, especialmente desarrollado para el análisis de datos, los cálculos estadísticos y las representaciones gráficas.
- Es un lenguaje de programación muy sencillo
- Es software LIBRE
- Disponible para diferentes plataformas
- (Unix, MacOS, Windows)
- Muy usado en la investigación científica

Se utiliza para el análisis de los datos recolectados en las pruebas realizadas en los prototipos.

3.13. Implementación del algoritmo criptográfico base

3.13.1. Desarrollo de la aplicación

En el capítulo II se considera como base el algoritmo AES, se desarrolla la aplicación donde se implementa dicho algoritmo, utilizando el IDE de desarrollo Netbeans con el lenguaje java que se denomina Prototipo I de escritorio.

Paquetes utilizados

Los paquetes utilizados en la aplicación se muestran en la Figura 1-3

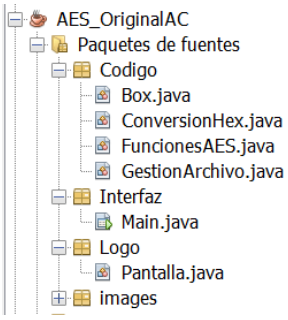


Figura 1-3: Paquetes utilizados Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

Los paquetes Interfaz, código, images y logo son los necesarios para el desarrollo de la aplicación. Se describen las clases más importantes en la Tabla 1-3

Tabla 1-3: Paquetes del Prototipo I de escritorio

Interfaz	Contiene la clase principal de la interfaz de usuario	Main.java
Images	Contiene las imágenes utilizadas en la aplicación.	Clear Close Open
Código	Contiene las clases necesarias para el funcionamiento del algoritmo AES.	Box ConversionHex GestionArchivo FuncionesAES
Logo	Contiene la clase donde se muestra la imagen de presentación.	pantalla

Realizado por: Cushpa Ana, 2018

Interfaz

Para el funcionamiento de la aplicación se ha desarrollado la siguiente interfaz que se muestra en la Figura 2-3

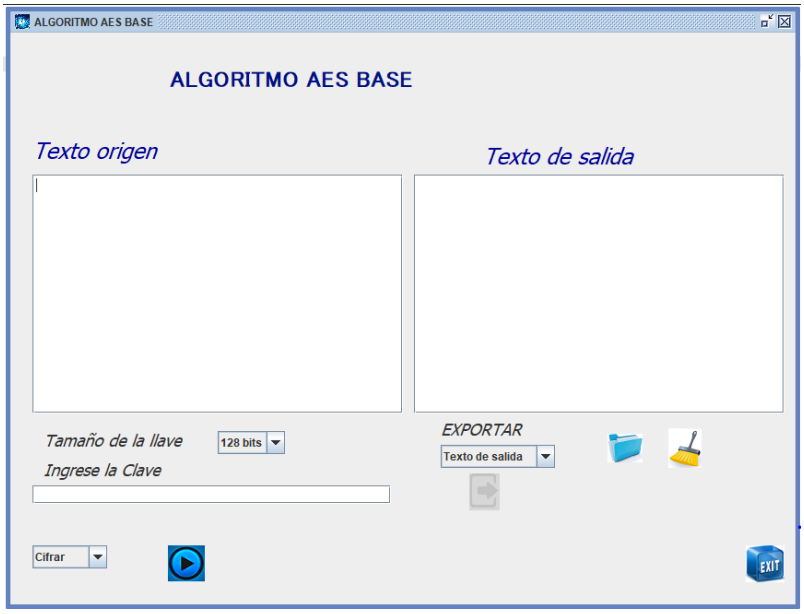


Figura 2-3: Interfaz Prototipo I de escritorio

Realizado por: Cushpa Ana, 2018

Descripción de la interfaz

Texto origen. - Área donde se ingresa el texto origen (texto plano o texto cifrado).

Texto destino. - Área donde se muestra el resultado luego de ejecutar la acción seleccionada.

Tamaño de la llave. – El usuario debe elegir el tamaño de la llave (128, 192, 256 bits)

Ingrese la clave. –Se debe ingresar la clave de acuerdo al tamaño definido.

Opción: cifrar/descifrar. – Se elige la opción a ejecutar sobre el texto origen (cifrar, descifrar).

Opción: Texto salida/texto entrada. – Se elige la opción a exportar (texto entrada, texto salida).

Botones

 **. -** Se utiliza para abrir archivos.

 **. -** Se utiliza para limpiar los datos de la pantalla

 . – Ejecuta la acción de cifrado/descifrado seleccionado.

 . – Ejecuta la acción de exportar el texto de entrada/texto de salida seleccionado.

. – Sale de la aplicación.

El Anexo B especifica el principal código fuente utilizado en la implementación del algoritmo criptográfico AES base.

3.13.2. Proceso de Cifrado Algoritmo base

A continuación, la Figura 3-3 muestra el proceso de cifrado que se implementa en la aplicación con el algoritmo base.

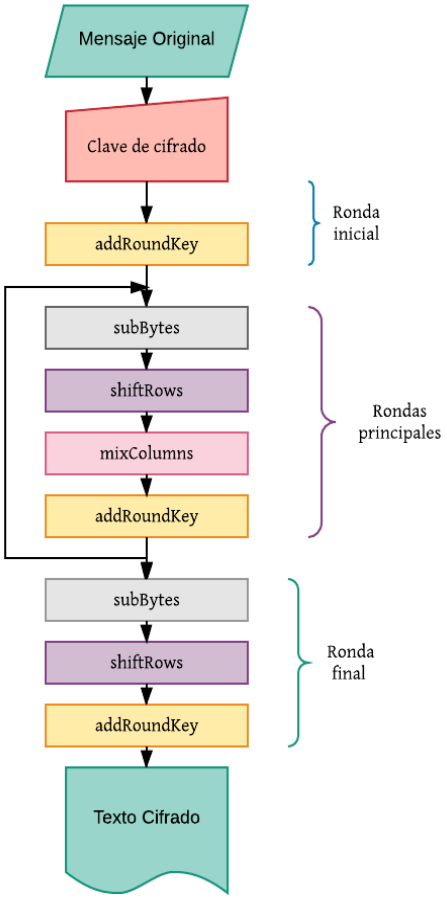


Figura 3-3: Proceso de cifrado Algoritmo base
Realizado por: Cushpa Ana, 2018

Ejecución del cifrado con el algoritmo AES base

Generación de claves

El algoritmo AES base trabaja con claves definidas en formato hexadecimal de:

- 128 bits
- 192 bits
- 256 bits

Para generación de claves se ha utilizado una aplicación de internet denominado **Traductor binario Hexadecimal base 64** que permite codificar texto en formato binario y hexadecimal, facilitando de esta forma la obtención de claves con tamaños de 128bits, 192bits y 256bits, como se muestra en la Figura: 4-3

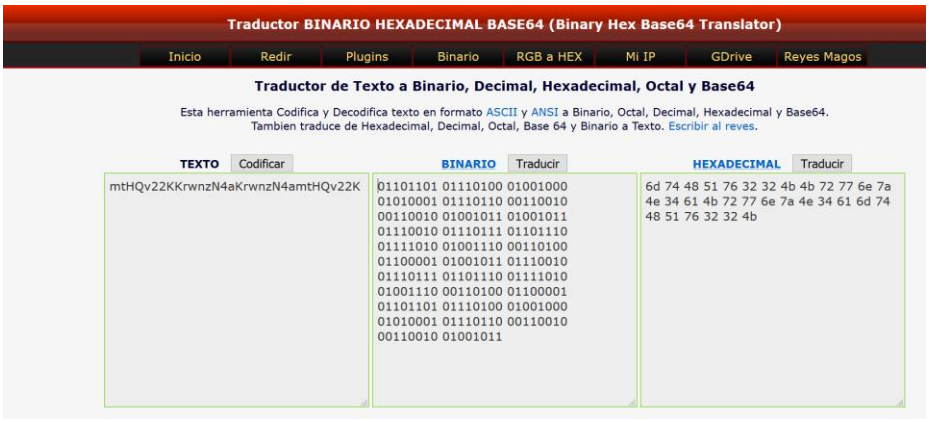


Figura 4-3: Generación de claves en formato Hexadecimal
Fuente: http://redir.dasumo.com/hex/

Donde se ingresa valores en hexadecimal y la aplicación traduce al formato binario y a su vez a formato texto. Para comprobar el funcionamiento de la aplicación se utiliza un texto plano y una clave de 128 bits que se muestra en la Tabla 2-3.

Tabla 2-3: Datos utilizados en la ejecución de la aplicación Prototipo I de escritorio

Documento Origen	Clave de cifrado (128 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4a	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultado

Se obtiene los siguientes resultados que se muestran en la Figura 5-3

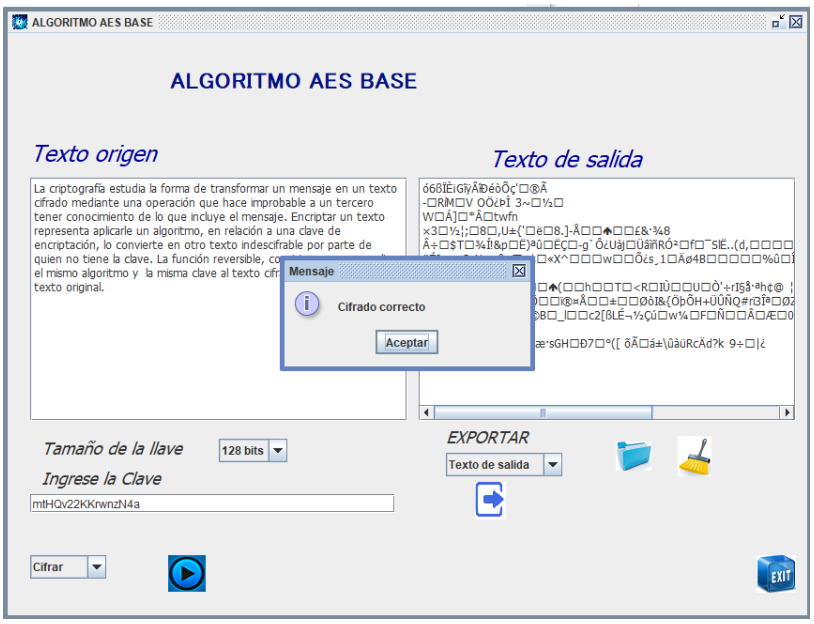


Figura 5-3: Ejecución de cifrado Algoritmo base
Realizado por: Cushpa Ana, 2018

Este documento puede ser exportado a un archivo.txt tal como se muestra en la Figura 6-3.

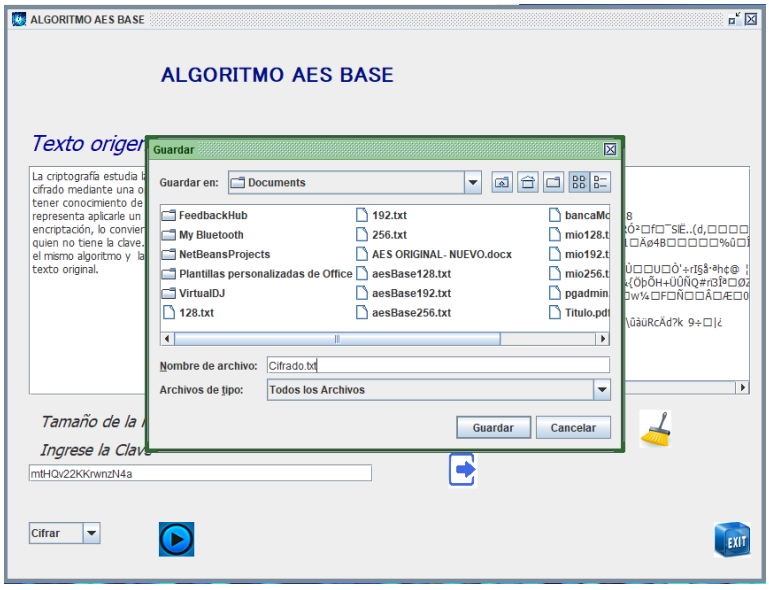


Figura 6-3: Exportar archivo, Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

3.13.3. Proceso de descifrado

En el algoritmo AES base el proceso de descifrado se muestra en la Figura 7-3

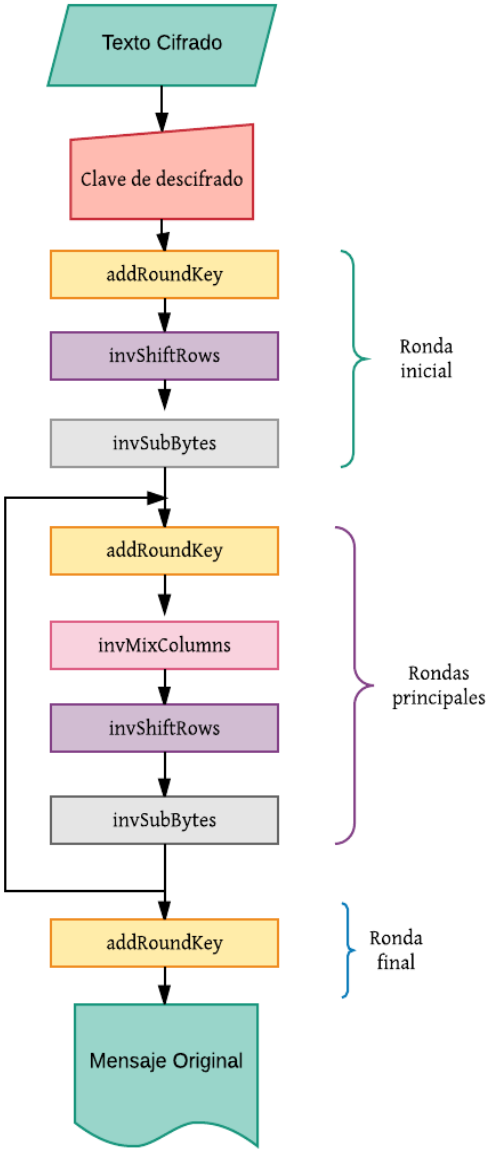


Figura 7-3: Proceso de descifrado: algoritmo base AES
Realizado por: Cushpa Ana, 2018

Ejecución del descifrado con el algoritmo AES base

En la ejecución de la aplicación se utiliza el texto encriptado anteriormente con una clave de 128 bits, que se muestra en la Tabla 3-3

Tabla 3-3: Datos utilizados en la ejecución de la aplicación con el algoritmo base

Document o Origen	Clave de cifrado (128 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4a	ó6ßÎÈiGïÿÂîÐéòÕç'□®Ã -□RÌM□V OÖ¿ÞÌ 3~□½□ W□Á]□*Â□twfn ×3□½¦;□8□,U±{'□ë□8.]-Å□□♠□□£&·¾8 Â÷□$T□¾Í!&p□Ë)ªû□ËÇ□-g`Ô¿Uàj□Üâiñ RÓ²□f□¯SlË..(d,□□□□ ¨É°×<rÇ¸Hµ¬ê+□_$□«X^□□□w□□Õ¿s¸1□Äø4B□□□□□%û□ □ĭáI□¬\² åd³èÃVtå{□¹□□×□□♠(□□h□□T□<R□IÙ□□U□Ò'÷rI§å·ªh¢@ ¦ èn Æ□á]-ß¸□tU¹□|Ô□□ï®¤Å□□±□□Øòl&{ÖþÕH+ÜÛÑQ#rï3Î ª□Ø: _qmù« □Á□DAéÚ´©B□_|□□c2[ßLÉ¬½Çú□w¼□F□Ñ□□Â□Æ□(ñ□F|□jG¤;□îè: ,å□Û_Û□nÖÉ♠©□0æ·sGH□Ð7□°([õÃ□á±\ûàüRcÄd?k 9÷□|¿

Realizado por: Cushpa Ana, 2018

Resultado de la ejecución

La aplicación muestra el resultado de ejecutar el descifrado con los datos anteriores en la Figura 8-3

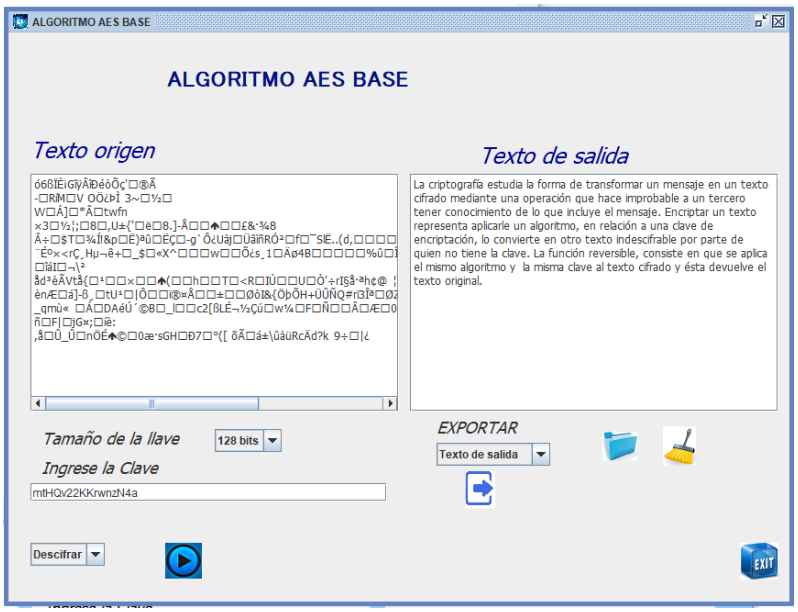


Figura 8-3: Ejecución descifrado Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

Se puede observar que el algoritmo cifra/descifra el texto original.

3.14. Diseño e Implementación del nuevo algoritmo criptográfico

3.14.1. Propuesta de mejora

Tomando como base el algoritmo AES se desarrolla un nuevo algoritmo. Para incrementar el nivel de seguridad se propone los siguientes avances:

- Aplicar una *nueva función* llamada *MIXDIAGONAL* que se ejecutará dentro de la ronda inicial, y en la ronda final, en la misma que se realiza un recorrido cíclico de forma diagonal en la matriz de estado actual.
- Almacenar los datos recorridos en una nueva matriz de forma consecutiva en filas y columnas.

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 9-3 se muestra el comportamiento de la función MixDiagonal.

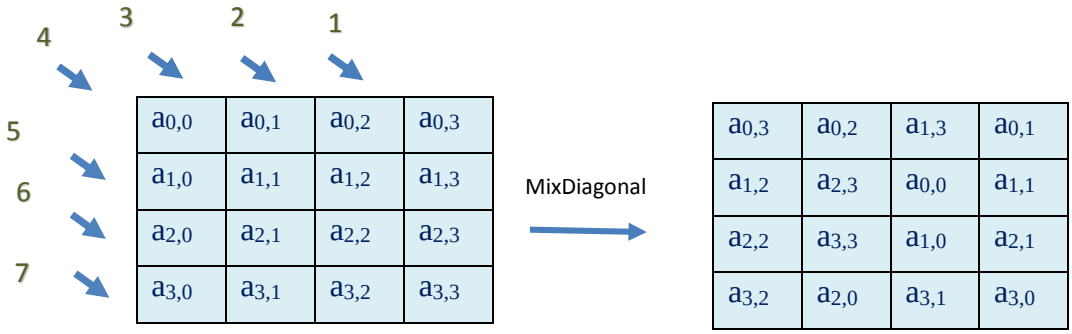


Figura 9-3: Función MixDiagonal
Realizado por: Cushpa Ana, 2018

A continuación, se muestra un ejemplo de la función MixDiagonal que se propone:

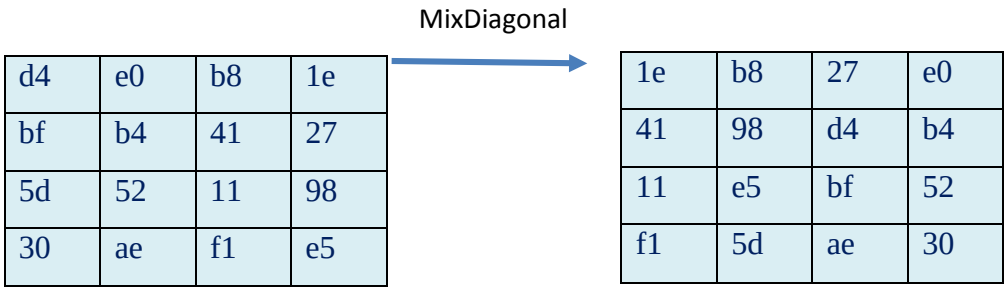


Figura 10-3: Ejemplo Función MixDiagonal
Realizado por: Cushpa Ana, 2018

- 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.

3.14.2. Desarrollo de la aplicación

Con la ilustración de las innovaciones que se proponen para el desarrollo del nuevo algoritmo, el proceso siguiente es realizar la implementación de la aplicación donde se utiliza el IDE de desarrollo Netbeans con el lenguaje Java, denominado Prototipo II de escritorio

Paquetes

Los paquetes utilizados en la aplicación se muestran en la Figura 11-4

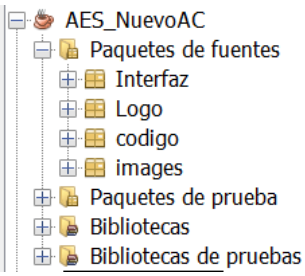


Figura 11-3: Paquetes utilizados nuevo algoritmo
Realizado por: Cushpa Ana, 2018

Interfaz

Dentro de este paquete se encuentra la clase main.java de la interfaz de usuario.

Logo

Contiene las funciones para la presentación de la pantalla principal y el logo de la aplicación.

Images

Se encuentran las imágenes utilizadas en la aplicación

Codigo

Es el paquete que contiene las clases desarrolladas para cifrado y descifrado de información, necesarias para la aplicación y funcionamiento del nuevo algoritmo. Se muestra en la Figura 12.3.

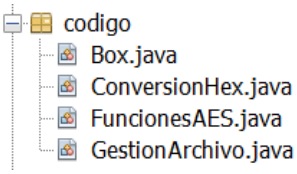


Figura 12-3: Paquete código, Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

Las clases que forman el paquete código contiene las siguientes funciones que muestra la Tabla 4-3:

Tabla 4-3: Funciones del paquete código, nuevo algoritmo

Clase	Funciones
FuncionesAES.java	Subword Rotword Cypher AddRoundKey SubByte ShiftRow MixColum **MixDiagonal** InversoCypher InvShiftRow InvSubByte **InvMixDiagonal** InvMixColumn InvSubWord
Box.java	S-Box InvS-Box
ConversionHexa.java	Hexadecimal a byte Hexadecimal a ASCII Byte a hexadecimal ASCII a hexadecimal
GestionArchivo.java	ReadFile OpenFile WriteFile SaveFilebytes

Realizado por: Cushpa Ana, 2018

El Anexo B muestra el código principal para la implementación del nuevo algoritmo.

3.14.3. Nuevo proceso de cifrado

En el nuevo algoritmo se incorpora la función **MixDiagonal** que es implementado en la ronda inicial y en la ronda final, se suma un ciclo secundario de Nr/2 rondas para de esta forma incrementar la seguridad.

A continuación, se muestra el proceso de funcionamiento del algoritmo criptográfico propuesto para el proceso de cifrado de la información en la Figura 13-3

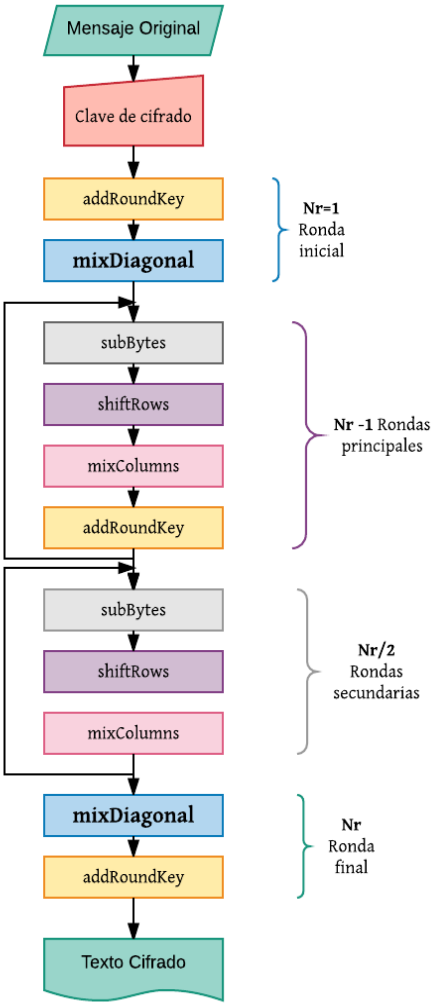


Figura 13-3: Proceso de cifrado: nuevo algoritmo
Realizado por: Cushpa Ana, 2018

Prueba de cifrado con la aplicación del nuevo algoritmo

Se han implementado las funciones en el nuevo algoritmo y para probar la aplicación se utilizan los datos que se muestran en la Tabla 5-3.

Tabla 5-3: Datos utilizados en el proceso de cifrado con el nuevo algoritmo

Documento Origen	Clave de cifrado (128 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4a	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultado

Después de ejecutar el proceso de cifrado se obtiene la información que muestra la Figura 14-3

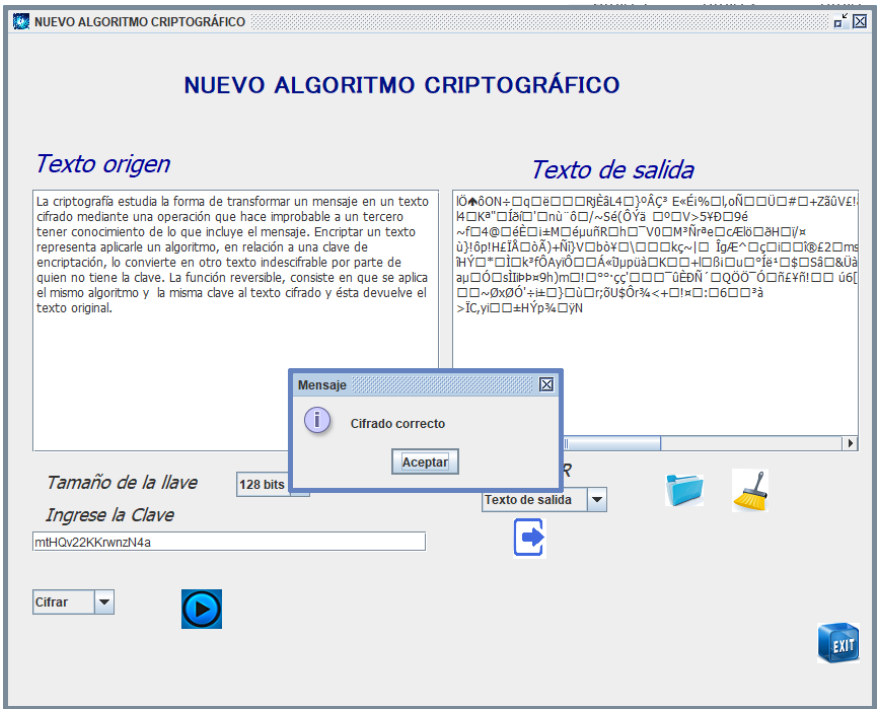


Figura 14-3: Ejecución de cifrado, Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

3.14.4. Nuevo proceso de descifrado

El proceso de descifrado del nuevo algoritmo incorpora la función inversa **InvMixDiagonal** en la ronda inicial y en la ronda final del cifrado, con la incorporación de un ciclo secundario de *Nr/2* rondas. Se muestra en la Figura 15-3

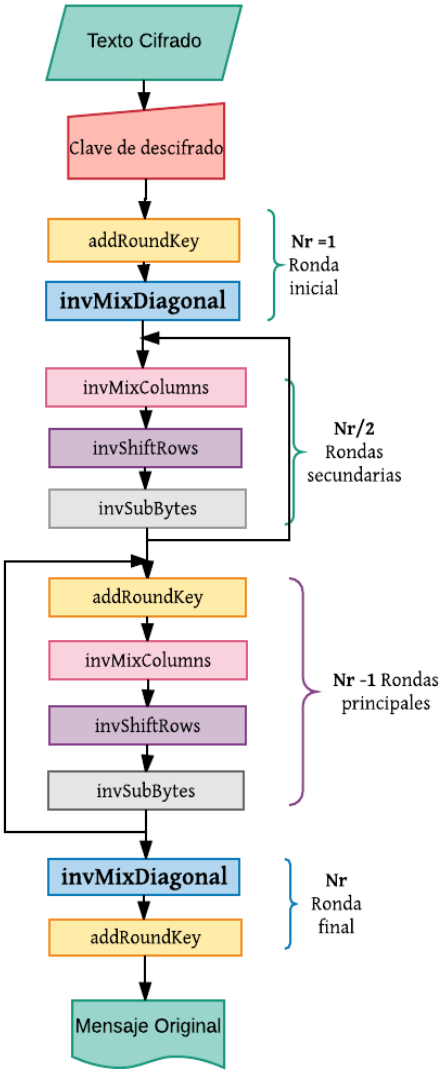


Figura 15-3: Proceso de descifrado: nuevo algoritmo
Realizado por: Cushpa Ana, 2018

Prueba de descifrado con la aplicación del nuevo algoritmo

Para ejecutar la aplicación se utilizan los datos que se muestran en la Tabla 6-3

Tabla 6-3: Datos utilizados en el proceso de descifrado con el nuevo algoritmo

Documento Origen	Clave de cifrado (128 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4a	lÖ♠ôON÷□q□ë□□□RjÈâL4□}ºÂÇ³ E«Éi%□l,oÑ□□Ü□#□+ZãûV£! ł4□Kª"□Íãí□'□nù¨ô□/~Sé{ÔÝã □º□V>5¥Ð□9é ~f□4@□éÈ□i±M□éµuñR□h□¯V0□M³Ñrªe□cÆlö□ðH□ï/¤ ù}!ôp!H£ÏÅ□òÃ)+Ñî}V□bò¥□\□□□kç~\□ ÎgÆ^□ç□i□□ï®£2□m‹ ĩHÝ□*□Ì□k³fÔAyïÔ□□Á«Üµpüà□K□□+l□ßi□u□°Íê¹□$□Sâ□&Üà aµ□Ó□sÌÏÞÞ¤9h)m□!□°°·çç'□□□¯ûÈÐÑ´□QÖÖ¯Ó□ñ£¥ñ!□□ ú6[□□~ØxØÓ'÷i±□}□ù□r;õU$Ôr¾<+□!¤□:□6□□³à >ÏC,yï□□±HÝp¾□ÿN

Realizado por: Cushpa Ana, 2018

Resultado

Luego de ejecutar el proceso de descifrado se obtiene los resultados que muestra la Figura 16-3

Figura 16-3: Ejecución descifrado del Prototipo II web
Realizado por: Cushpa Ana, 2018

3.15. Análisis y diseño de algoritmos

El análisis de complejidad de los algoritmos AES y AES nuevo se realiza a continuación:

3.15.1. Análisis de complejidad del algoritmo AES base

En la Figura 17-3 se muestra la complejidad del algoritmo base AES.

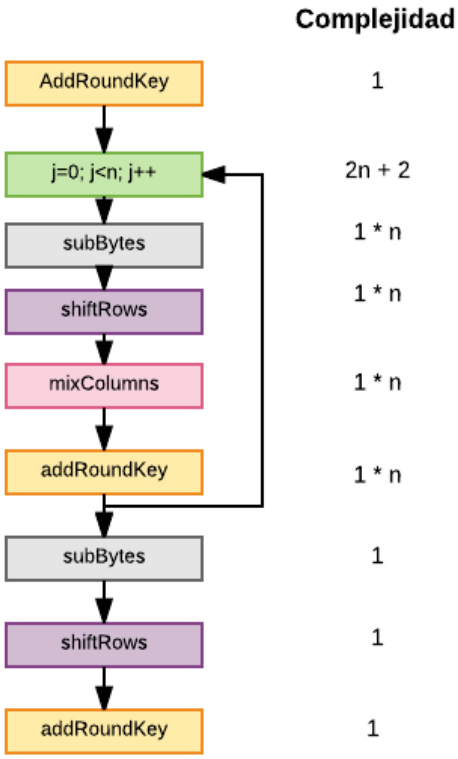


Figura 17-3: Análisis de complejidad del algoritmo AES base
Realizado por: Cushpa Ana, 2018

Cálculo de complejidad del algoritmo AES base

De acuerdo al tema de complejidad descrito en el capítulo II el cálculo se realiza de la siguiente forma:

1 + (2n + 2) + (1 * n) + (1 * n) + (1 * n) + (1 * n) + 1 + 1+ 1

= 1 + 2n + 2 + n + n + n + n + 1 + 1+ 1

= 6n + 6

Como resultado se obtiene:

Complejidad algoritmo AES base = **6n + 6**

3.15.2. Análisis de complejidad del nuevo algoritmo

En la Figura 18-3 se muestra la complejidad del nuevo algoritmo

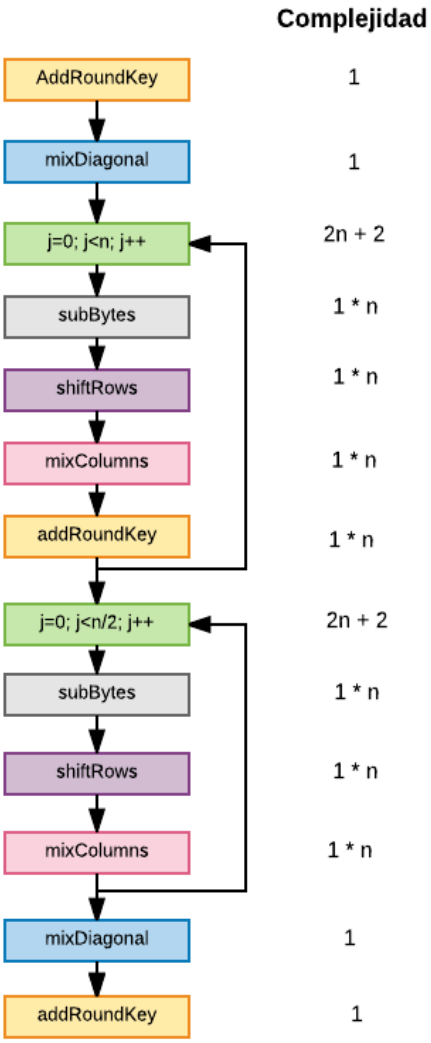


Figura 18-3: Análisis de complejidad: nuevo algoritmo
Realizado por: Cushpa Ana, 2018

Cálculo de complejidad del nuevo algoritmo

De acuerdo al tema de complejidad descrito en el capítulo II el cálculo se realiza de la siguiente forma:

1 + 1 + (2n + 2) + (1 * n) + (1 * n) + (1 * n) + (1 * n) + (2n + 2) + (1 * n) + (1 * n) +

(1 * n) + 1+ 1

= 2 + 2n + 2 + n + n + n + n + 2n + 2 + n + n + n + 2

= 11n + 8

Como resultado se obtiene:

Complejidad del nuevo algoritmo = **11n + 8**

La complejidad del nuevo algoritmo criptográfico obtenido tiene orden de complejidad lineal O(n) que es igual al orden del algoritmo AES base.

3.16. Pruebas de validación del nuevo Algoritmo

Para validar el algoritmo propuesto se realizan un conjunto de 384 pruebas definidas en la Muestra, que se describe en el capítulo II. Las claves que se utiliza son de longitud variable de 128bits, 192 bits y 256 bits generadas desde el *traductor binario hexadecimal* que se muestra en la Tabla 7-3, también se usan textos de un promedio de 65 palabras que se muestran en la Tabla 8-3

Tabla 7-3: Claves generadas para las pruebas con la muestra tomada

Código	Tamaño de la clave (bits)	Clave
C1	128	mtHQv22KKrwnzN4a
C2	192	mtHQv22KKrwnzN4amtHQv22K
C3	256	mtHQv22KKrwnzN4aKrwnzN4amtHQv22K
C4	128	N4aKrwnzmtHQv22K
C5	192	N4aKrwnzmtHQv22KKrwnzN4a
C6	256	N4aKrwnzmtHQv22KKrwnzN4amtHQv22K
C7	128	@TDA&10RcrsSdBcD
C8	192	@TDA&10RcrsSdBcDcrsSdBcD
C9	256	@TDA&10RcrsSdBcDcrsSdBcDcrsSdBcD
C10	128	kW]Ld5$\|E@Q^$iq"
C11	192	kW]Ld5$\|E@Q^$iq"kW]Ld5$|
C12	256	kW]Ld5$\|E@Q^$iq"kW]Ld5$\|E@Q^$iq"
C13	128	}yl%OckF x){gI~o
C14	192	<E?<E?<E?<E?<E?<E?<E?<E?
C15	256	<E?<E?<E?<E?<E?<E?<E?<E?<E?<E
C16	128	PIaWRZRrIxwO6CDp
C17	192	PIaWRZRrIxwO6CDpZRrIxwO6
C18	256	PIaWRZRrIxwO6CDpZRrIxwO6aWRZRrIx
C19	128	Y**GJ.FA6Pljg,Vp
C20	192	Y**GJ.FA6Pljg,Vp.FA6Pljg
C21	256	Y**GJ.FA6Pljg,Vp.FA6Pljg*GJ.FA6P
C22	128	oqaW33gizDProYFb
C23	192	oqaW33gizDProYFbaW33gizD
C24	256	GSPYol4nuW3kLE5M4nuW3kLEGSPYol4n
C25	128	LlSCUWeWRIaXEywZ
C26	192	LlSCUWeWRIaXEywZSCUWeWRI
C27	256	LlSCUWeWRIaXEywZSCUWeWRIaXEywZSC
C28	128	9hHt0L4dVhAjgveS
C29	192	9hHt0L4dVhAjgveSVhAjgveS
C30	256	9hHt0L4dVhAjgveSVhAjgveS9hHt0L4d
C31	128	r8Bjx4VGHdUrOiIi
C32	192	r8Bjx4VGHdUrOiIijx4VGHdU

C33	256	r8Bjx4VGHdUrOiIijx4VGHdUBjx4VGHd
C34	128	bFp&I5SvYsCsHR?a
C35	192	bFp&I5SvYsCsHR?aI5SvYsCs
C36	256	bFp&I5SvYsCsHR?aI5SvYsCsHR?aI5Sv
C37	128	GSPYol4nuW3kLE5M
C38	192	GSPYol4nuW3kLE5M4nuW3kLE
C39	128	lpNHPLb+8m%4UVl>

Realizado por: Cushpa Ana, 2018

Tabla 8-3: Mensajes utilizados para las pruebas con la muestra tomada

Código Mensaje	Texto
M1	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.
M2	La seguridad de la información contiene un conjunto de medidas defensoras y reactivas de los sistemas tecnológicos que permiten resguardar la información y mantener la confidencialidad, la disponibilidad e integridad de los datos. La encriptación protege la información que viaja a través de los canales inseguros por internet. Si los datos son interceptados, éstos serán ilegibles para los usuarios no autorizados porque no poseen la clave de encriptación.
M3	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.
M4	La mensajería instantánea es una vía de transmisión de información en tiempo real que puede darse entre dispositivos como celulares, computadoras, tabletas, etc. Para algunas compañías el uso del servicio representa productividad y comunicación, mientras que para otras constituye un entretenimiento para el personal. La comunicación entre dos personas es posible con la instalación de estos programas a cada uno para que se conecten y la información pueda ser enviada.
M5	La interconectividad de redes es una plataforma que es parte de las redes de datos, de las cuales dependen las relaciones sociales, así como también los negocios, está basado en un conjunto de servicios y tecnologías en el que se desarrollan redes modernas que en su mayor parte son heterogéneas. Hoy en día las redes transmiten información en una extensa gama de dispositivos que facilita el acceso a varios métodos de comunicación.
M6	La seguridad de los datos o seguridad informática es parte importante dentro de las Tecnologías de la Información en estructuras de cualquier tamaño. Es un aspecto que se refiere a la protección de la información de accesos que no están autorizados, de esta manera evitar el mal uso y descomposición de la misma durante su ciclo de vida.
M7	AES es un algoritmo que puede ser implementado tanto en sistemas hardware y en sistemas software trabaja con bloques de 128 bits y las claves con longitud variable que pueden ser de 128 bits, 192 bits y 256 bits. Aplica una matriz de bytes que consta de cuatro filas por cuatro columnas que es la que se utiliza en un conjunto de bucles donde se ejecutan operaciones matemáticas para conseguir el cifrado de la información.
M8	La encriptación de clave simétrica tiene su seguridad en su propia clave secreta, pero un problema que se presenta está en la distribución de dicha clave a todos los usuarios para el cifrado y descifrado de la información, de esta manera se mantiene en secreto el mensaje transmitido. Las llaves deben ser bien administradas de acuerdo a los canales seguros que se desea mantener.
M9	Las aplicaciones de chat constituyen programas clientes por medio de los cuales los usuarios acceden al servicio y se interconectan con oros usuarios para transmitir información, eligiendo con quiere compartirla. La estructura de este sistema es transparente para el usuario. Muchas aplicaciones se basan en html, o en el lenguaje java que debe estar disponible en el navegador a través del cual se realiza la comunicación.
M10	Cifrar es aplicar un determinado algoritmo y una clave determinada para de esta manera transmitir la información de forma confidencial. En el cifrado de clave simétrica dos o más usuarios tienen la misma clave secreta por medio de la cual se cifra y descifra la información que se transmite por el canal. Solo la persona que tenga la clave podrá descifrar el mensaje.

Realizado por: Cushpa Ana, 2018

Con estos datos se realiza las pruebas de cifrado con el prototipo I y prototipo II que se muestran en el Anexo A.

Los resultados de las pruebas realizadas se muestran en la Tabla 9-3

Tabla 9-3: Promedio de las pruebas con la muestra tomada

Indicador	**Prototipo I**	**Prototipo II**
Entropía	6.06	6.11

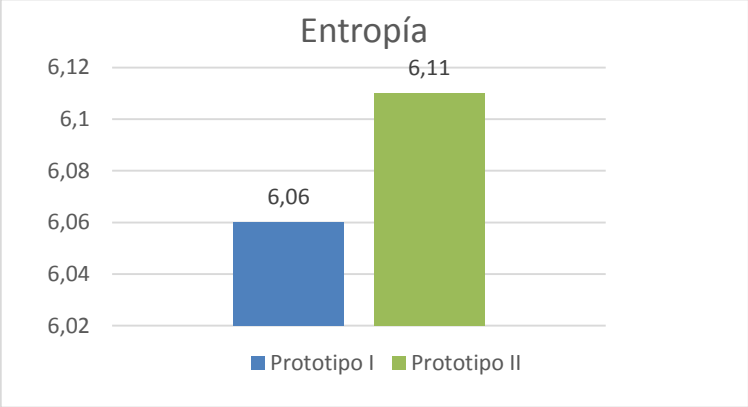


Figura 19-3: Valor promedio de las pruebas con la muestra, Prototipo I y II de escritorio.
Realizado por: Cushpa Ana, 2018

El prototipo II presenta un valor de entropía de 6.11 que es mayor al valor que presenta el prototipo I de 6.06, por lo tanto, muestra mayor difusión en los mensajes cifrados.

Diagrama de barra

Con la herramienta R Stadistical se puede verificar los valores del Prototipo I como se muestra en la Figura 20-3 y 21-3.

Prototipo I de escritorio

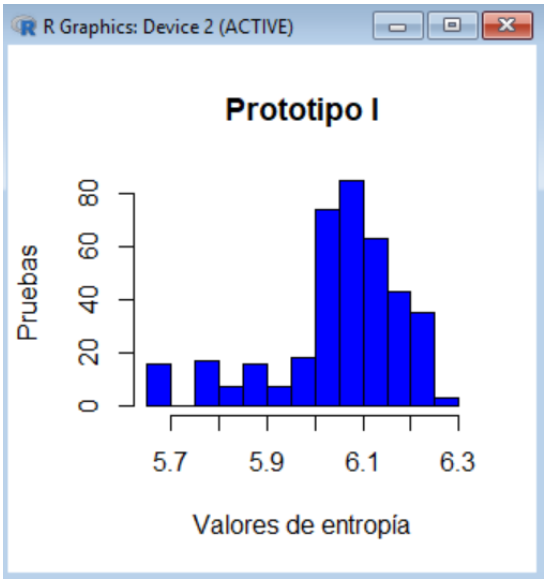


Figura 20-3: Valores obtenidos con la muestra, Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

Prototipo II de escritorio

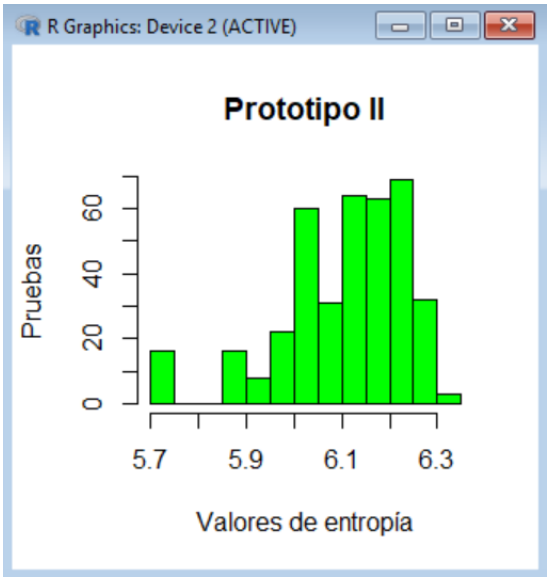


Figura 21-3: Valores obtenidos con la muestra, Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

En los valores obtenidos de las pruebas realizadas se obtiene mayor entropía con el Prototipo II de escritorio en comparación con el prototipo I de escritorio.

Medidas de localización

De cada uno de los prototipos se realiza un análisis estadístico de los datos. La Figura 22-3 muestra las medidas de posición o localización del prototipo I de escritorio

Prototipo I de escritorio

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

Figura 22-3: Medidas de posición, Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

Se puede observar los valores obtenidos en cuanto a la distribución, los cuartiles representan cómo los datos están posicionados en el conjunto ordenado, en este case se encuentran entre el primer cuartil igual a 6.010 y el tercer cuartil igual a 6.150, con una media de 6.056.

En el diagrama de caja y bigote de la Figura 23-4 podemos complementar los datos obtenidos anteriormente.

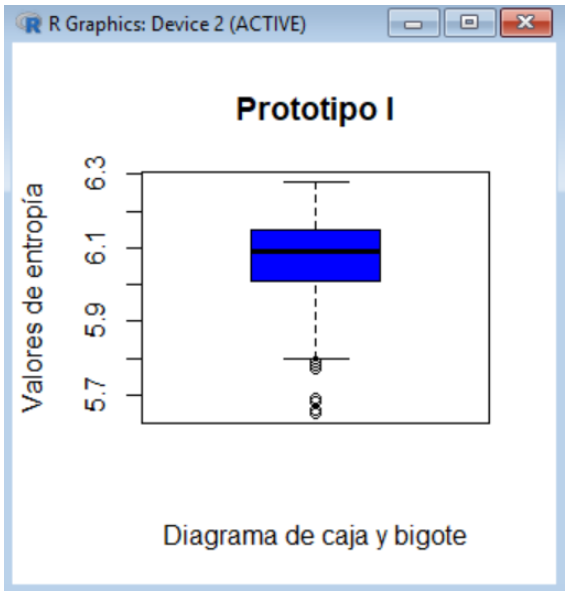


Figura 23-3: Diagrama de caja y bigote, Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

La distribución de la información está concentrada en mayor parte entre 6.056(Q2) y 6.150(Q3) mientras que los datos están más dispersos entre 6.010(Q1) y 6.056(Q2).

Prototipo II de escritorio

La Figura 24-3 muestra la distribución de los datos en el Prototipo II de escritorio

```
> summary(PrototipoII)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
  5.700   6.040   6.140   6.111   6.210   6.310
>
```

Figura 24-3: Medidas de posición, Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

Se puede determinar que los datos están distribuidos entre los cuartiles:6.040 y 6.210, con una media de 6.111. Por lo tanto, se puede determinar que los valores del Prototipo I de escritorio I están distribuidos en un intervalo mayor al del prototipo I de escritorio.

En la Figura 25 -3 se muestra la distribución de los datos con relación a los cuartiles

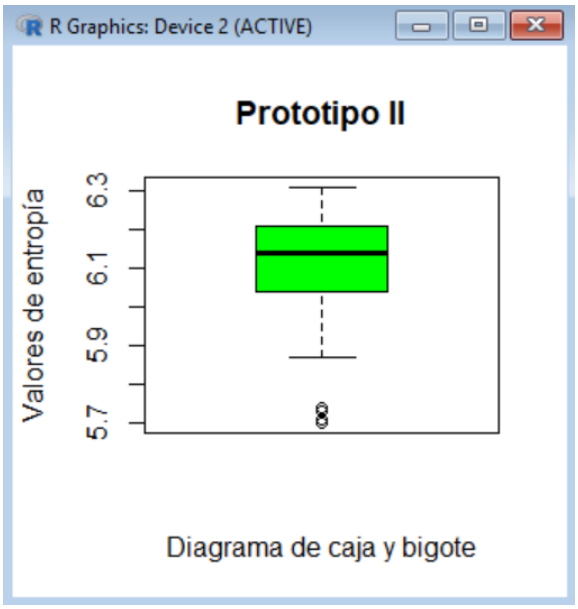


Figura 25-3: Diagrama de caja y bigote, Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

El diagrama muestra que en el intervalo de 6.111(Q2) y 6.210(Q3) se encuentran la mayor concentración de valores mientras que en el intervalo 6.040(Q1) y 6.111(Q2) los valores están más dispersos.

Medidas de dispersión

En cada uno de los prototipos se aplica la desviación estándar (sd) y la varianza (var), para determinar cuánto se pueden alejarse los valores respecto a la media.

Prototipo I de escritorio

La Figura 26-3 muestra los valores calculados del Prototipo I de escritorio

```
> sd(PrototipoI)
[1] 0.1373627
> var(PrototipoI)
[1] 0.01886851
```

Figura 26-3: Desviación estándar y varianza del Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

La desviación estándar igual a 0.1373627 indica que los valores de entropía no se encuentran muy alejados con respecto a la media, y la varianza igual a 0.01886851 indica que los datos no se encuentran muy dispersos, lo que indica que existe una adecuada distribución de los datos obtenidos.

A continuación, la Figura 27-3 muestra la ubicación de cada uno de los valores de las pruebas de entropía realizadas con los mensajes cifrados por el prototipo I de escritorio.

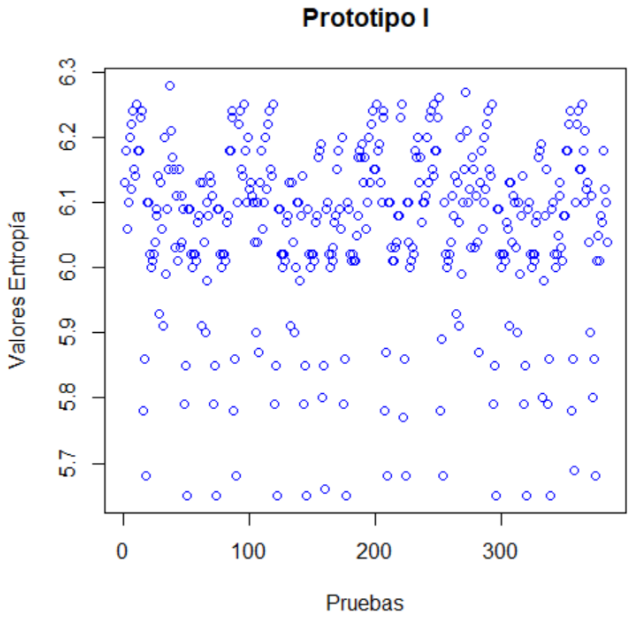


Figura 27-3: Diagrama plot, Prototipo I de escritorio
Realizado por: Cushpa Ana, 2018

El gráfico anterior muestra que existe simetría en los datos obtenidos de las pruebas realizadas con el prototipo I.

Prototipo II de escritorio

La Figura 28-3 muestra los valores calculados del Prototipo II de escritorio

```
> sd(PrototipoII)
[1] 0.1331594
> var(PrototipoII)
[1] 0.01773143
```

Figura 28-3: Desviación estándar y varianza del Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

La desviación estándar igual a 0.1331594 indica que los valores de entropía no se encuentran muy alejados con respecto a la media, y la varianza igual a 0.01773143 indica que los datos no se encuentran muy dispersos, lo que indica que existe una adecuada distribución de los datos obtenidos.

A continuación, la Figura 29-3 muestra la ubicación de cada uno de los valores de las pruebas de entropía realizadas con los mensajes cifrados por el prototipo II.

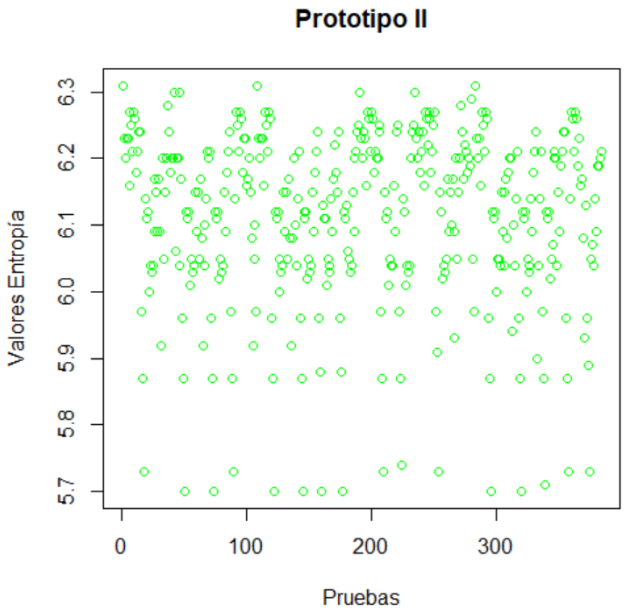


Figura 29-3: Diagrama plot, Prototipo II de escritorio
Realizado por: Cushpa Ana, 2018

El gráfico de plot muestra que existe simetría en la obtención de los valores de entropía, realizados con el prototipo II de escritorio.

Se concluye que con las pruebas de entropía realizadas al Prototipo I de escritorio y Prototipo II de escritorio, y con la aplicación del análisis estadístico se puede determinar que el nuevo algoritmo implementado mejora la seguridad de la información y se valida su implementación en un chat web.

3.17. Integración del algoritmo criptográfico en una aplicación web para mensajería instantánea

Para integrar el algoritmo criptográfico en una aplicación web se desarrollan 2 prototipos.

Prototipo I Web

El prototipo I Web integra en la aplicación el algoritmo base que consta de 4 funciones principales que se distribuyen en el proceso de cifrado que son:

- AddRoundKey
- SubByte
- ShiftRow
- MixColumn

Prototipo II Web

En el desarrollo del prototipo II web se suma la función propuesta al algoritmo criptográfico AES base que consta de las siguientes funciones:

- AddRoundKey
- SubByte
- ShiftRow
- MixColumn
- **MixDiagonal (función propuesta)**

Además, contiene el ciclo secundario de las funciones shiftRows y subBytes.

3.17.1. Prototipo I Web

3.17.1.1. Desarrollo de la aplicación

En el capítulo II se describe la arquitectura de una aplicación web, misma que se utiliza para el desarrollo de la aplicación con Netbeans, un IDE de desarrollo que utiliza el lenguaje Java.

Base de Datos

Se ha creado una base de datos con las siguientes tablas:

- Usuario
- Mensaje
- Clave

Usuario. – Se almacena información de los usuarios registrados en el chat.

Mensaje. – Se registra el mensaje enviado de forma encriptada.

Clave. – Se almacena los datos de la llave utilizada para el cifrado.

A continuación, se muestra el esquema de la base de datos en la Figura 30-3:

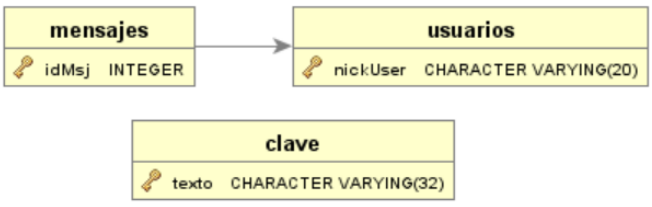


Figura 30-3: Tablas de Base de datos Prototipo I web
Realizado por: Cushpa Ana, 2018

Se tiene tres tablas donde se almacenan los datos de los usuarios y de los mensajes enviados, así como también se registra la clave de cifrado.

Paquetes

Los paquetes que se utilizan en la aplicación muestra la Figura 31-3

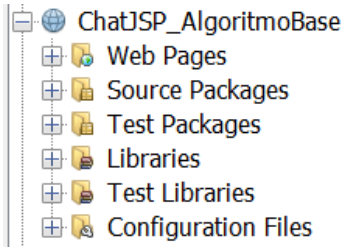


Figura 31-3: Paquetes Prototipo I web
Realizado por: Cushpa Ana, 2018

Web Pages

Contiene los jsp necesarios para la interacción con el usuario, entre los más importantes 32-3

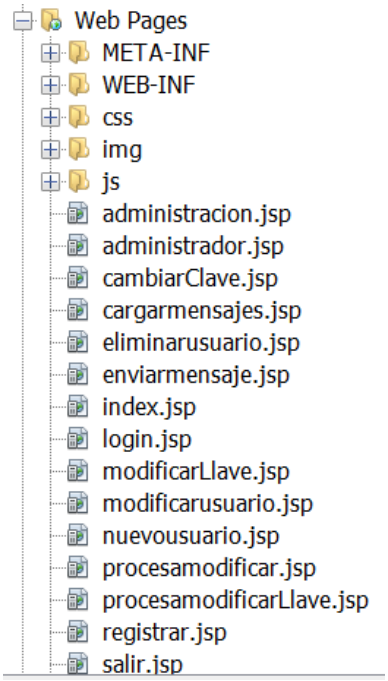


Figura 32-3: Jsp de Web Pages, Prototipo I web
Realizado por: Cushpa Ana, 2018

Los jsp administrador, cargarmensajes, login, enviarmensajes, cambiarClave, eliminarusuario, etc son jsp relacionados con el funcionamiento del chat.

Source Pages

Contiene las clases necesarias para el acceso y administración de la Base de Datos. Se incluye el paquete **codigo,** como se muestra en la Figura 33-3

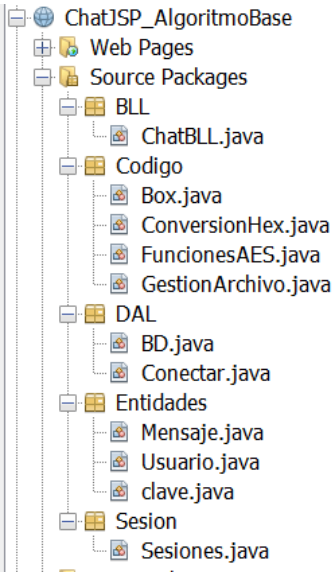


Figura 33-3: Clases Web Packages, Prototipo I web
Realizado por: Cushpa Ana, 2018

Interfaz

La aplicación web con la implementación del algoritmo AES base muestra la Figura 34-3

Figura 34-3: Interfaz Aplicación, Prototipo I web
Realizado por: Cushpa Ana, 2018

BOTONES

Registrarse. - Permite registrar los datos a un usuario para que pueda ingresar al chat como muestra la Figura 35-3

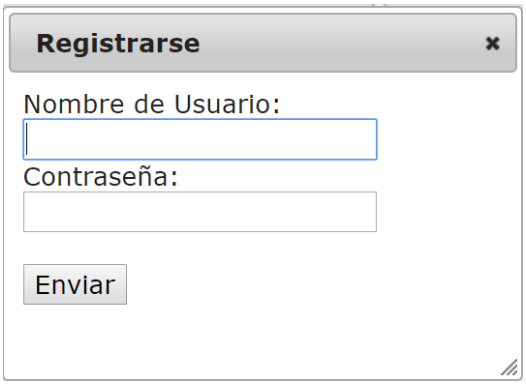


Figura 35-3: Interfaz Registrarse Prototipo I web
Realizado por: Cushpa Ana, 2018

Ingresar al chat. – Solicita el usuario, contraseña y la clave de cifrado, necesarios para el desarrollo del chat, como muestra la Figura 36-3

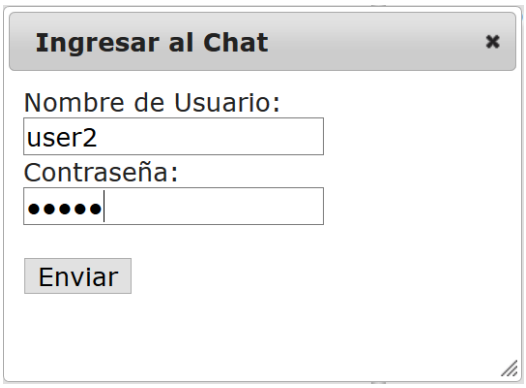


Figura 36-3: Interfaz Ingresar, Prototipo I web
Realizado por: Cushpa Ana, 2018

Una vez ingresado al web chat se muestra los mensajes enviados desde y hacia el usuario ingresado como se muestra en la Figura 37-3

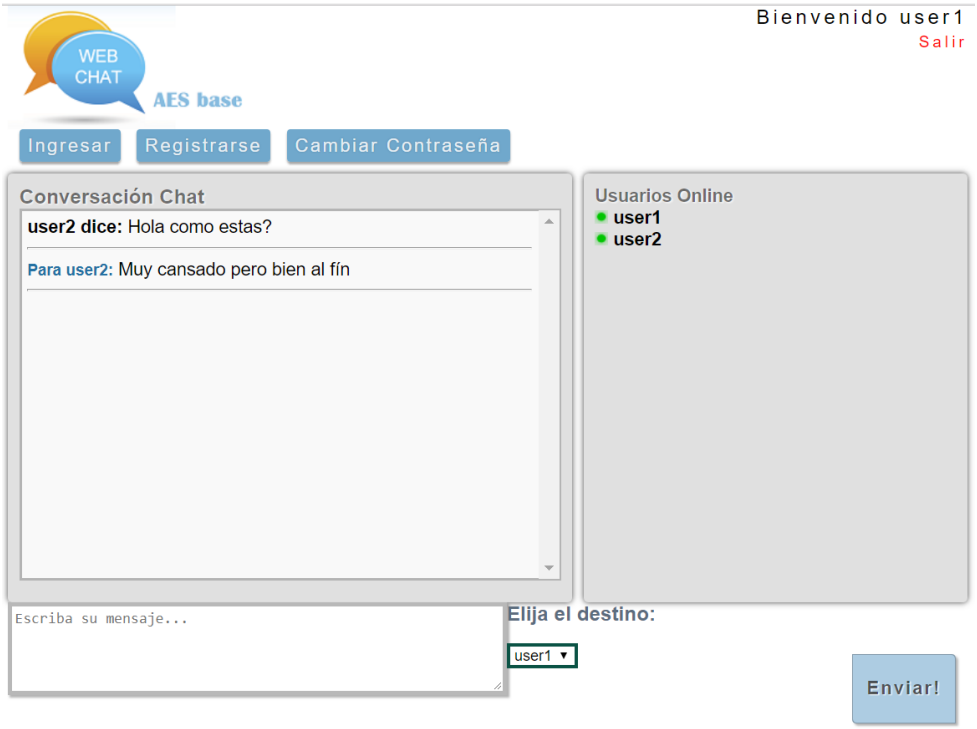


Figura 37-3: Interfaz del chat, Prototipo I web
Realizado por: Cushpa Ana, 2018

Los mensajes enviados por el usuario se almacenan en la base de datos con el texto cifrado, utilizando el algoritmo AES base con una clave que es gestionada por el administrador de la aplicación, para luego ser descifrado por el mismo algoritmo al momento de mostrarse, siendo este proceso totalmente transparente para el usuario.

La Figura 38-3 muestra cómo se almacena la información en la base de datos

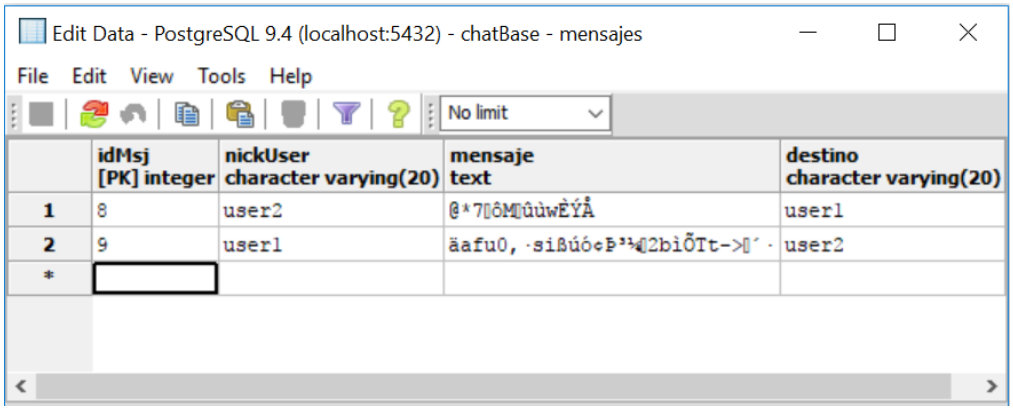


Figura 38-3: Almacenamiento de mensajes en la Base de datos, Prototipo I web
Realizado por: Cushpa Ana, 2018

Administrador. – Permite el ingreso al usuario administrador, se muestra en la Figura 39-3

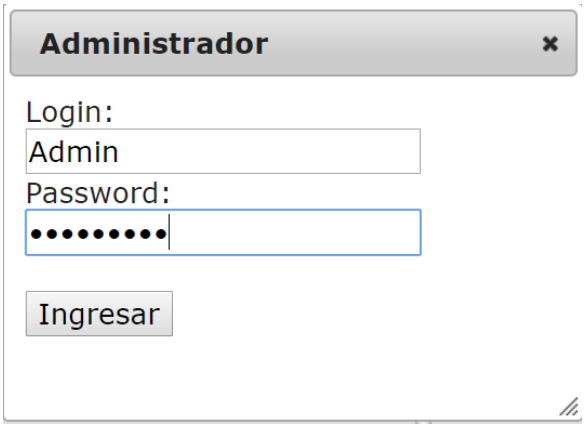


Figura 39-3: Interfaz Ingreso Administrador, Prototipo I web
Realizado por: Cushpa Ana, 2018

Las tareas del administrador son: gestión de usuarios y cambio de la clave de cifrado., como se muestra en la Figura 40-3

Figura 40-3: Interfaz Administración de usuarios, Prototipo I web
Realizado por: Cushpa Ana, 2018

Si la clave es cambiada por el Administrador los mensajes enviados anteriormente se muestran de forma cifrada y los mensajes que se envíen con la nueva clave serán descifrados y mostrados en texto plano como se muestra en la Figura 41-3

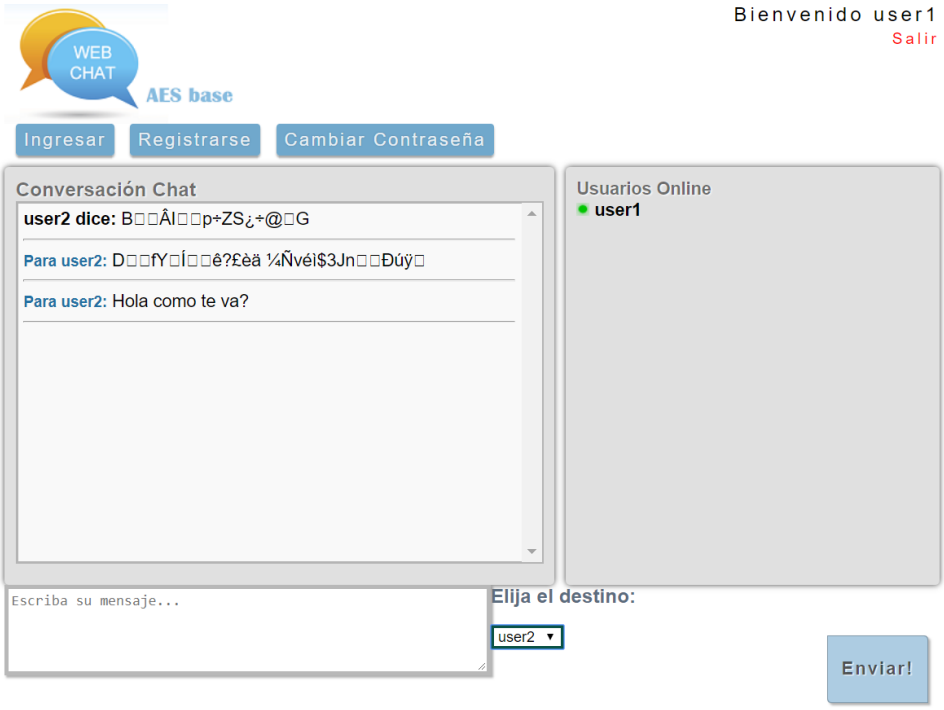


Figura 41-3: Mensajes después de cambiar la clave de cifrado, Prototipo I web
Realizado por: Cushpa Ana, 2018

Proceso general de Chat Web

El proceso general del funcionamiento del chat se muestra en la Figura 42-3

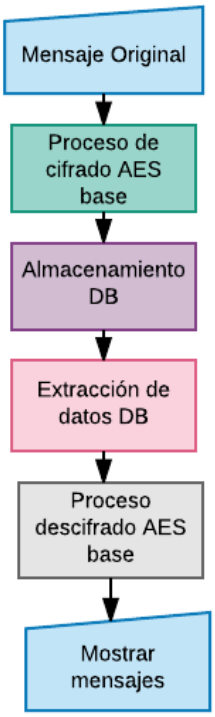


Figura 42-3: Proceso general, Prototipo I web
Realizado por: Cushpa Ana, 2018

El Anexo B muestra las funciones principales de envío y visualización de mensajes.

3.17.2. Prototipo II Web

3.17.2.1. Desarrollo de la aplicación

En el prototipo II web se incorpora el nuevo algoritmo con las funciones propuestas y el ciclo secundario.

Base de Datos

La base de datos consta de las siguientes tablas:

- Usuario
- Mensaje
- Clave

Paquetes

Los paquetes que se utilizan en la aplicación muestra la Figura 43-3

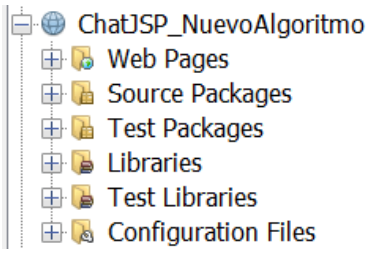


Figura 43-3: Paquetes aplicación Prototipo II web
Realizado por: Cushpa Ana, 2018

Web Pages

Contiene los jsp necesarios para la interacción con el usuario, entre los más importantes index, administrador e imágenes utilizados en la aplicación, como muestra la Figura 44-3

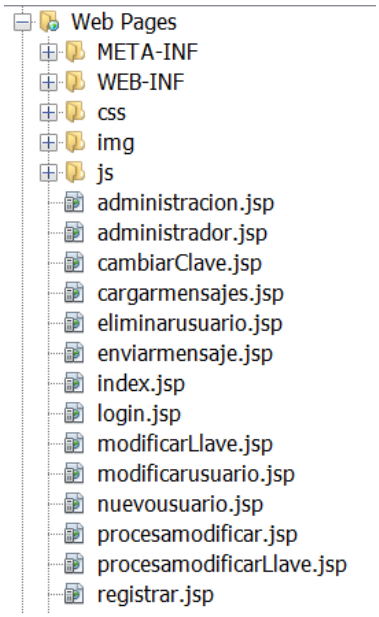


Figura 44-3: Jsp de Pages Prototipo II Web
Realizado por: Cushpa Ana, 2018

Los jsp administrador, cargarmensajes, login, enviarmensajes, cambiarClave, eliminarusuario, etc son jsp relacionados con el funcionamiento del chat.

Source Pages

Contiene las clases necesarias para el acceso y administración de la Base de Datos. Se incluye el paquete **code,** como se muestra en la Figura 45-3

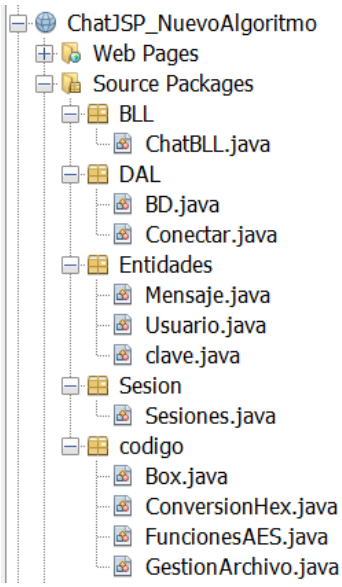


Figura 45-3: Clases Web Packages, Prototipo II web
Realizado por: Cushpa Ana, 2018

Interfaz

La aplicación web con la implementación del nuevo algoritmo muestra la Figura 46-3

Figura 46-3: Interfaz Prototipo II web
Realizado por: Cushpa Ana, 2018

Interfaz de chat

La aplicación recepta los mensajes del usuario, los envía y recarga la ventana de conversación chat como se muestra en la Figura 47-3

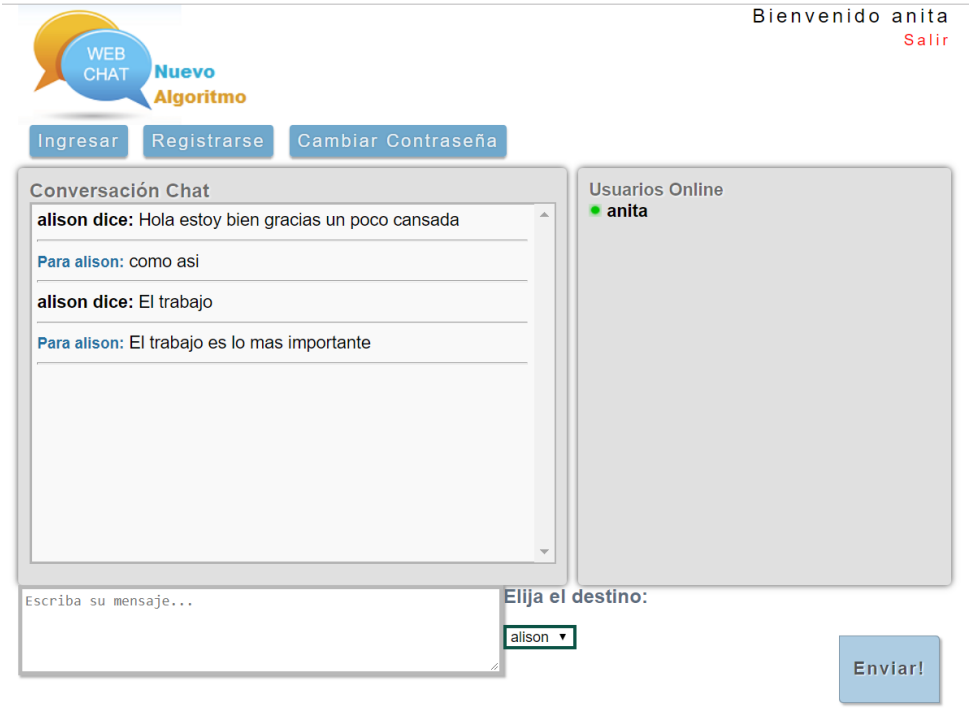
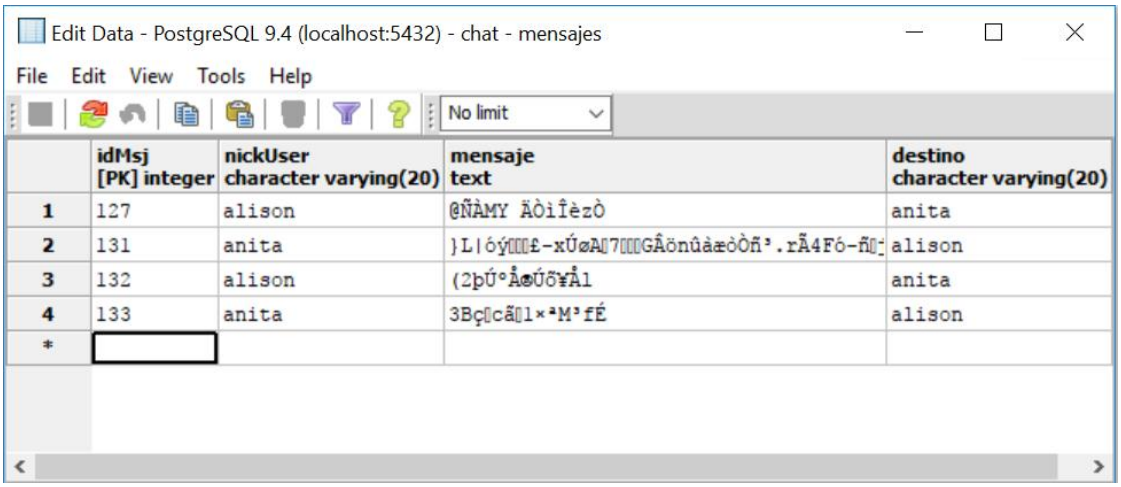


Figura 47-3: Interfaz Chat Prototipo II web
Realizado por: Cushpa Ana, 2018

Los mensajes enviados por el usuario se guardan en la base de datos luego de ser cifrados con el *nuevo algoritmo* como se muestra en la Figura 46-3, utilizando una clave que maneja el administrador, para luego ser descifrado por el mismo algoritmo y mostrarse al usuario; siendo todo este proceso transparente.



	idMsj [PK] integer	nickUser character varying(20)	mensaje text	destino character varying(20)
1	127	alison	@ÑÀMY ÃÒìÎèzÒ	anita
2	131	anita	}L|óý□□£-xÚøA□7□□GÂönûàæòÒñ³.rÃ4Fó-ñ□	alison
3	132	alison	(2þÚ°Åø¤Ú5¥Å1	anita
4	133	anita	3Bç□cã□1×³M³fÉ	alison
*				

Figura 48-3: Almacenamiento de mensajes, Prototipo II web
Realizado por: Cushpa Ana, 2018

Proceso general del Chat

El proceso general del funcionamiento del chat web se muestra en la Figura 49-3

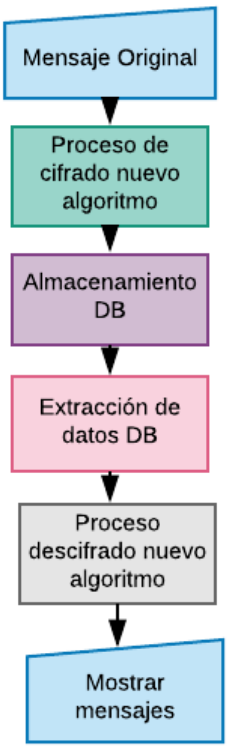


Figura 49-3: Proceso general Prototipo II web
Realizado por: Cushpa Ana, 2018

El Anexo B muestra las funciones principales de envío y visualización de mensajes.

3.18. Definición de los escenarios de pruebas

Ambiente de pruebas

Los 2 escenarios para el cifrado/descifrado de información se definen en un ambiente uniforme en el que se utiliza la aplicación de escritorio que se los denominará prototipo I-E y prototipo II-E por la facilidad que brinda para la toma de datos. Se establecen las siguientes condiciones;

- Aplicación de tamaños de clave de cifrado de: 128, 192, 256 bits.
- Tamaño de bloque de 128 bits.

Escenarios

Se establecen dos escenarios.

Escenario 1

El primer escenario utiliza la aplicación de escritorio Prototipo I-E definida con el algoritmo considerado como base AES.

Escenario 2

El segundo escenario utiliza la aplicación de escritorio Prototipo II-E definida con el nuevo algoritmo que incorpora nuevas funciones en el algoritmo de cifrado.

Resultados

Las pruebas que se realizan posteriormente en los escenarios propuestos tienen la finalidad de demostrar el mejoramiento de la seguridad con la implementación del algoritmo propuesto, comparando los resultados que se obtienen de: Prototipo I-E de escritorio que implementa el algoritmo AES seleccionado como base y el Prototipo II-E de escritorio que implementa el nuevo algoritmo desarrollado con la incorporación de las nuevas funciones realizadas.

3.19. Hipótesis

3.19.1. Determinación de variables

Según la hipótesis planteada se identifican las variables siguientes:

Hipótesis general: La implementación de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web mejorará el nivel de seguridad de la información.

Variable independiente:

Algoritmo criptográfico para mensajería instantánea en un entorno web

Variable dependiente:

El nivel de seguridad de la información.

Hipótesis específica 1: Las características de los algoritmos criptográficos simétricos más conocidos permitirán seleccionar uno de ellos como base.

Variable independiente:

Características de los algoritmos criptográficos simétricos más conocidos.

Variable dependiente:

Algoritmo criptográfico simétrico base

Hipótesis específica 2: El algoritmo criptográfico simétrico seleccionado permitirá diseñar el nuevo algoritmo criptográfico simétrico.

Variable independiente:

Algoritmo criptográfico simétrico seleccionado.

Variable dependiente:

Nuevo algoritmo criptográfico simétrico.

Hipótesis específica 3: La prueba de los prototipos implementados para mensajería instantánea en un entorno web permitirá verificar el nivel de seguridad en los escenarios.

Variable independiente:

Prototipos implementados para mensajería instantánea en un entorno web.

Variable dependiente:

Nivel de seguridad.

3.19.2. Operacionalización conceptual

La operacionalización de las variables definidas se muestra en la Tabla 10-3

Tabla 10-3: Operacionalización de variables

VARIABLE	TIPO	DEFINICIÓN
Algoritmo criptográfico simétrico para mensajería instantánea en un entorno web	Independiente	Algoritmo que modifica los datos de un documento con el objetivo de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.
Seguridad de la información.	Dependiente	Nivel de protección de la información.

Realizado por: Cushpa Ana, 2018

3.19.3. Operacionalización metodológica

La operacionalización metodológica se muestra en la Tabla 11-3

Tabla 11-3: Operacionalización metodológica

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO/ FUENTE
Independiente Algoritmo criptográfico para mensajería instantánea en un entorno web.	▪ Complejidad ▪ Líneas de código ▪ Recursos utilizados	▪ Búsqueda de información ▪ Pruebas ▪ Observación	▪ Netbeans ▪ Postgres
Dependiente La seguridad de la información.	▪ Entropía ▪ Histograma ▪ Autocorrelación ▪ Resistencia contra fuerza bruta	▪ Pruebas ▪ Observación ▪ Análisis	▪ Cryptool ▪ R Stadistical

Realizado por: Cushpa Ana, 2018

CAPITULO IV

RESULTADOS Y DISCUSIÓN

Se realizan las pruebas, considerando los escenarios definidos en el capítulo anterior con los prototipos I-E y II-E de escritorio, se comparan los resultados que se obtuvieron para comprobar la hipótesis planteada.

4.1. Desarrollo de las pruebas

4.1.1. Prototipo I-E de escritorio

En el prototipo I-E se considera la aplicación de escritorio donde se implementa al algoritmo criptográfico AES base.

4.1.1.1. Cifrado

4.1.1.1.1. Clave de 128 bits

En la comprobación del proceso de cifrado con el prototipo I-E se emplean los datos de la Tabla 1-4.

Tabla 1-4: Datos utilizados en la ejecución con el algoritmo base,128 bits

Documento Origen	Clave de cifrado (128 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4a	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultados

Luego de ejecutar el cifrado en la aplicación se obtiene los siguientes resultados que incluyen caracteres imprimibles y no imprimibles de acuerdo con la tabla ASCII.

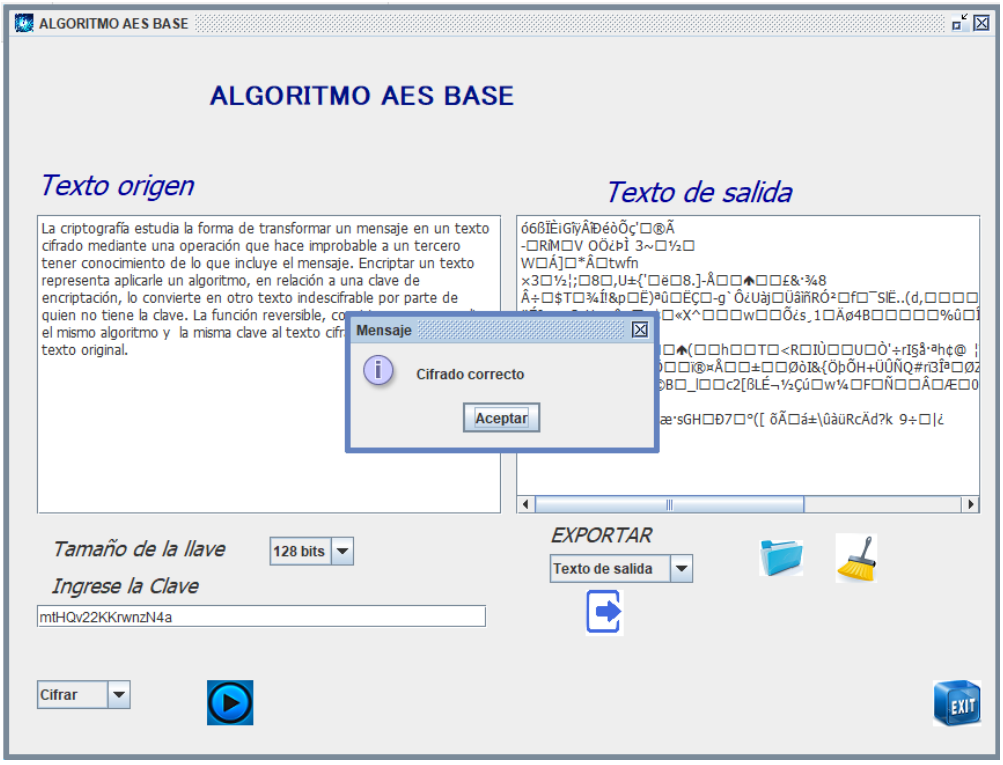


Figura 1-4: Ejecución de cifrado Algoritmo base, 128 bits
Realizado por: Cushpa Ana, 2018

4.1.1.1.2. Clave de 192 bits

Se utiliza la información que muestra la Tabla2-4 para la ejecución del algoritmo

Tabla 2-4: Datos utilizados en la ejecución con el algoritmo base, 192 bits

Documento Origen	Clave de cifrado (192 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4amtHQv22K	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados obtenidos del proceso de cifrado se muestran la Figura 2-4.

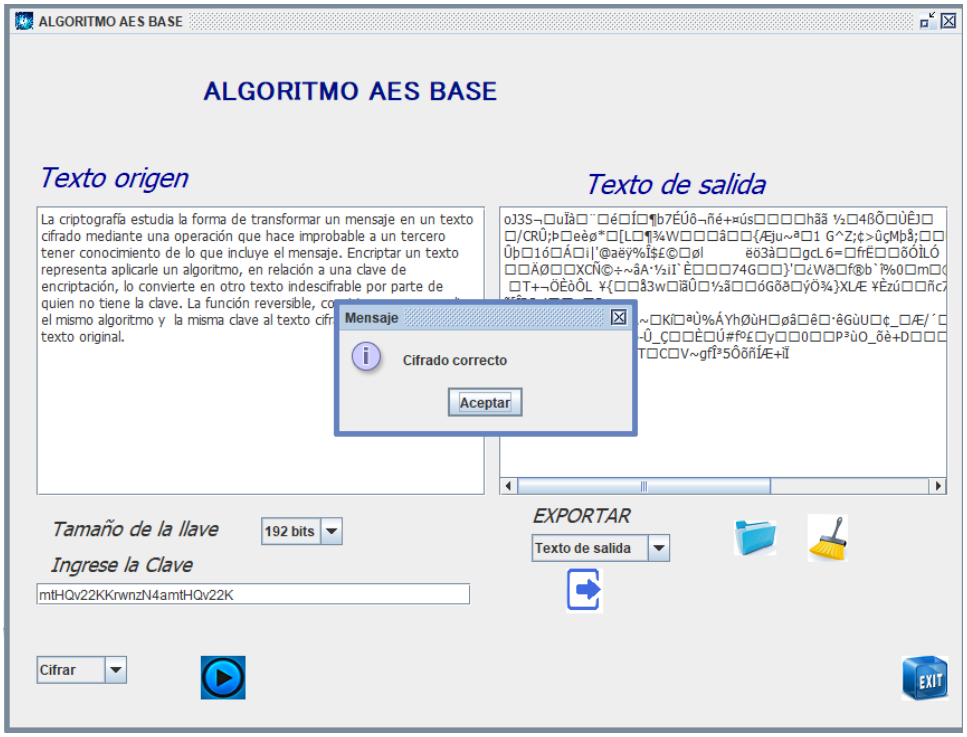


Figura 2-4: Ejecución de cifrado Algoritmo base, 192 bits
Realizado por: Cushpa Ana, 2018

4.1.1.1.3. Clave de 256 bits

Se utiliza la información que muestra la Tabla3-4 para la ejecución del algoritmo.

Tabla 3-4: Datos utilizados en la ejecución con el Prototipo I-E 256 bits

Documento Origen	Clave de cifrado (256 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4aKrwnzN4amtHQv22K	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados obtenidos se muestran en la Figura 3-4

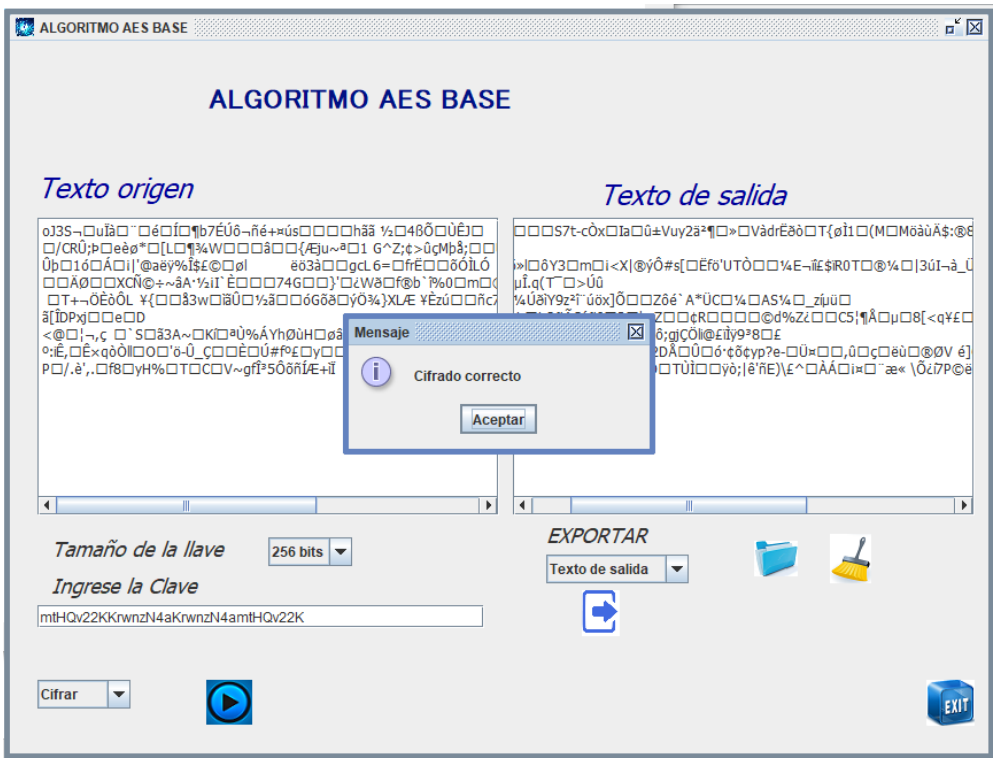


Figura 3-4: Ejecución de cifrado Prototipo I-E 256bits
Realizado por: Cushpa Ana, 2018

4.1.1.2. Descifrado

4.1.1.2.1. Clave de 128 bits

Para ejecutar el proceso de descifrado se emplean los datos de la tabla 4-4

Tabla 4-4: Datos utilizados en la ejecución con el algoritmo base 128 bits

Documento Origen	Clave de cifrado (128 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4a	ó6ßÎÈiGïÿÃÎÐéòÕç'□®Ã -□RÌM□V OÖ¿ÞÌ 3~□½□ W□Á]□*Â□twfn ×3□½¦;□8□,U±{'□ë□8.]-Å□□♠□□£&·¾8 Â÷□$T□¾Í!&p□Ë)ªû□ËÇ□-g`Ô¿Uàj□Üâ¡ñRÓ²□f□¯SlË..(d,□□□□ ¨É⁰×<rÇ¸Hµ¬ê+□_$□«X^□□□w□□Õ¿s¸1□Äø4B□□□□□%û□ □ĭáI□¬\² åd³èÃVtå{□¹□□×□□♠(□□h□□T□<R□IÙ□□U□Ò'÷rIg§å·ªh¢@ ¦ ènÆ□á]-ß¸□tU¹□|Ô□□ï®¤Å□□±□□Øòì&{ÖþÕH+ÜÛÑQ#rï3Îª□Ø _qmù« □Á□DAéÚ´©B□_l□□c2[ßLÉ¬½Çú□w¼□F□Ñ□□Â□Æ□0 ñ□F|□jG¤;□íè: ,å□Û_Û□nÖÉ♠©□0æ·sGH□Ð7□°([õÃ□á±\ûàüRcÄd?k 9÷□|¿

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados obtenidos se muestran en la Figura 4-4

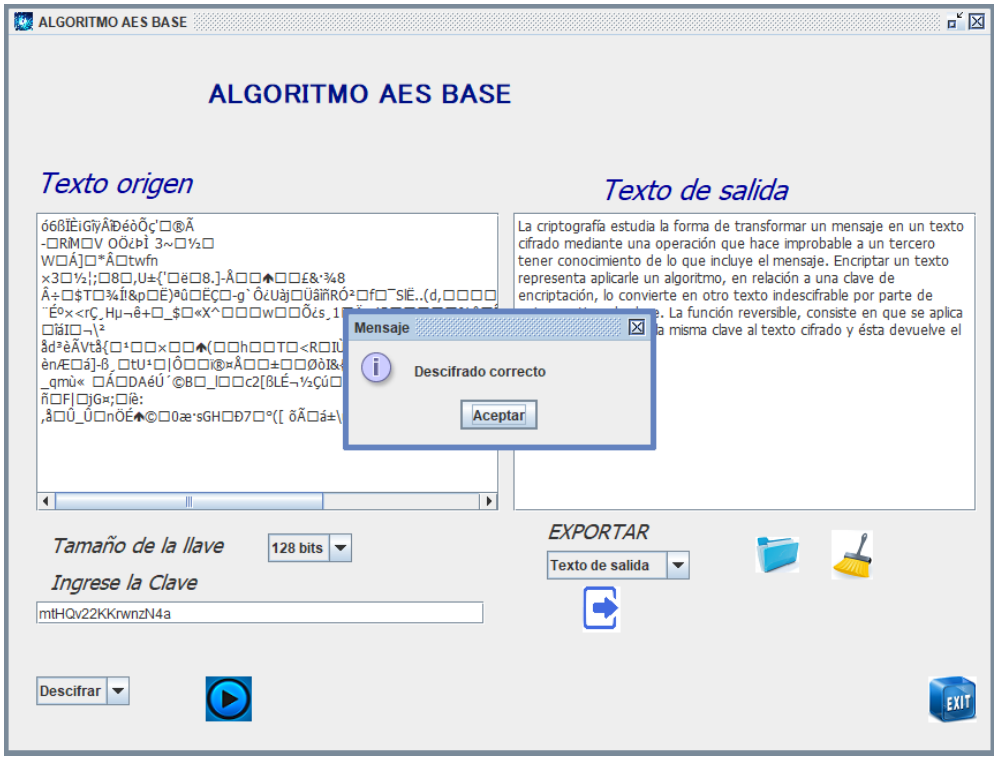


Figura 4-4: Ejecución de descifrado Algoritmo base, 128bits
Realizado por: Cushpa Ana, 2018

4.1.1.2.2. Clave de 192 bits

Para realizar la comprobación con el prototipo I-E se emplean los datos de la Tabla 5-4

Tabla 5-4: Datos utilizados en la ejecución con el algoritmo base 192 bits

Documento Origen	Clave de cifrado (192 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4amtHQv22K	oJ3S¬□uÌà□¨□é□Í□¶b7ÉUô¬ñé+¤ús□□□□hãã ½□4ßÖ□UËJ□ □/CRÛ;Þ□eèø*□[L□¶¾W□□□â□□{Æju~ª□1 G^Z;¢>ûçMþå;□□ Ûþ□1ó□Á□i|'@aëÿ%Î$£©□ø ë ö3à□□gcL6=□frÉ□□õÓÌLÓ □□ÄØ□□XCÑ©÷~åA·½iÌ`È□□□74G□□}'□¿Wð□f®b`Ì%0□m□ □T+¬ÖÈòÔL ¥{□□å3w□ïäÛ□½ã□□óGõð□ýÖ¾}XLÆ ¥Èzú□□ñc ã[ÎDPxj□□e□D <@□¦¬,ç □`S□ã3A~□KÍ□ªÙ%ÁYhØùH□øâ□ê□·êGùU□¢_□Æ/´[º:ìÊ,□Êxqòò|l□O□'ö-Û_Ç□□È□Ú#fº£□y□□0□□□P³ùO_õè+D□□□[P□/.è',.□f8□yH%□T□C□V~gfÎ³5Ôõ ñÍÆ+ìÏ

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados obtenidos se muestran en la Figura 5-4

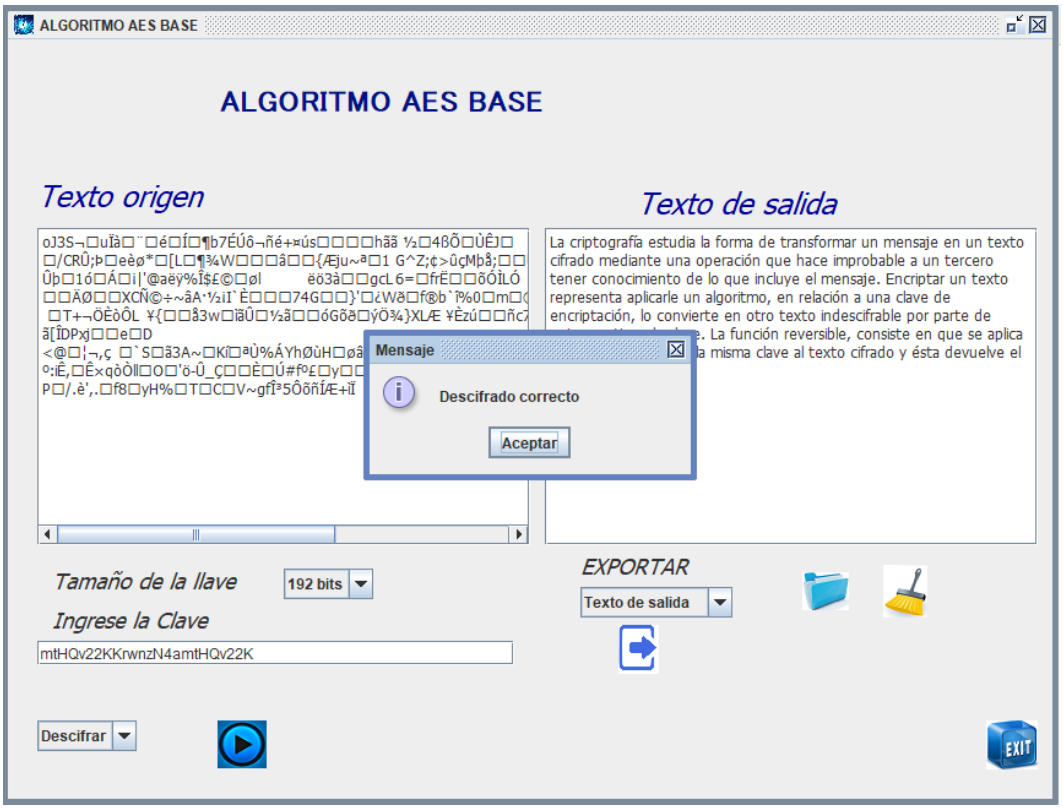


Figura 5-4: Ejecución de descifrado Algoritmo base, 192bits
Realizado por: Cushpa Ana, 2018

4.1.1.2.3. Clave de 256 bits

En la comprobación del prototipo I-E se utilizan los datos de la Tabla 6-4

Tabla 6-4: Datos utilizados en la ejecución con el algoritmo base 256 bits

Documento Origen	Clave de cifrado (256 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4aKrwnzN4amtHQv22K	Ɔ□□S7t-cÒx□Ia□û±Vuy2ã²¶□»□VàdrÉäö□T{øÌ1□(M□MöàùÄ$:® •\|□ôY3□m□i<X\|®ýÔ#s[□Ëfö'UTÒ□□¼E¬ïÉ$ïR0T□®¼□|3úI¬à_(ıÎ.q(T¯□>Úû ¼ÚðïY9z²ï¨úöx]Õ□□Zôé`A*ÜC□¼□AS¼□_zíµü□ ›□LQãÃÇ´ð°□2□I-_Z□□¢R□□□□©d%Z¿□□C5¦¶Å□µ□8[<q¥£□ E-ã□ûg².ck=É□□±þô;gjÇÒl@£ïÝ9³8□£ Ɔn%Ó□.3↟ýx□{Hn2DÅ□Û□ó·¢õ¢yp?e-□Ù×□□,û□ç□ëù□®ØV é] ìÁ□â-□□M□□OßýO□TÙÌ□□ýò;|ê'ñE)\£^□ÀÁ□ı×□¨æ« \Õ¿ì7P©é

Realizado por: Cushpa Ana, 2018

Resultados

Se obtienen los resultados que se muestran en la Figura 6-4

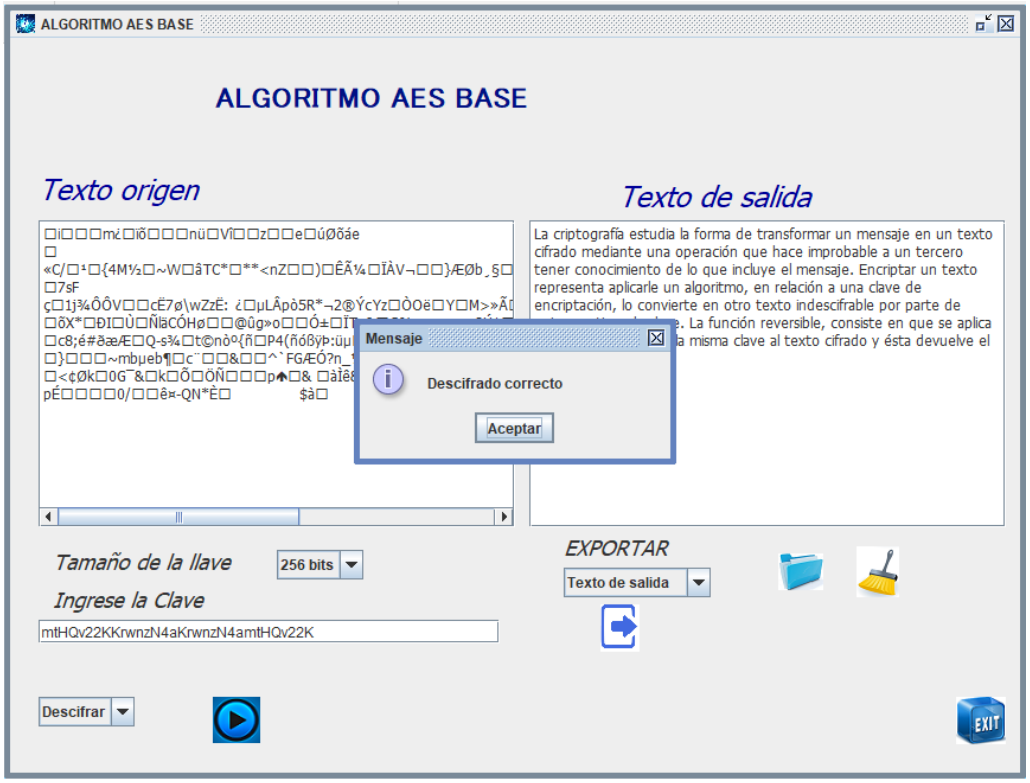


Figura 6-4: Ejecución de descifrado Algoritmo base, 256bits
Realizado por: Cushpa Ana, 2018

4.1.2. Prototipo II-E de escritorio

En el prototipo II-E se utiliza la aplicación de escritorio que integra el nuevo algoritmo con las funciones propuestas.

4.1.2.1. Cifrado

4.1.2.1.1. Clave de 128 bits

En la comprobación del proceso de cifrado se utiliza los datos de la Tabla 7-4.

Tabla 7-4: Datos utilizados en la ejecución con el nuevo algoritmo 128 bits

Documento Origen	Clave de cifrado (128 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4a	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados que se obtienen con la ejecución del prototipo se muestra en la Figura 7-4

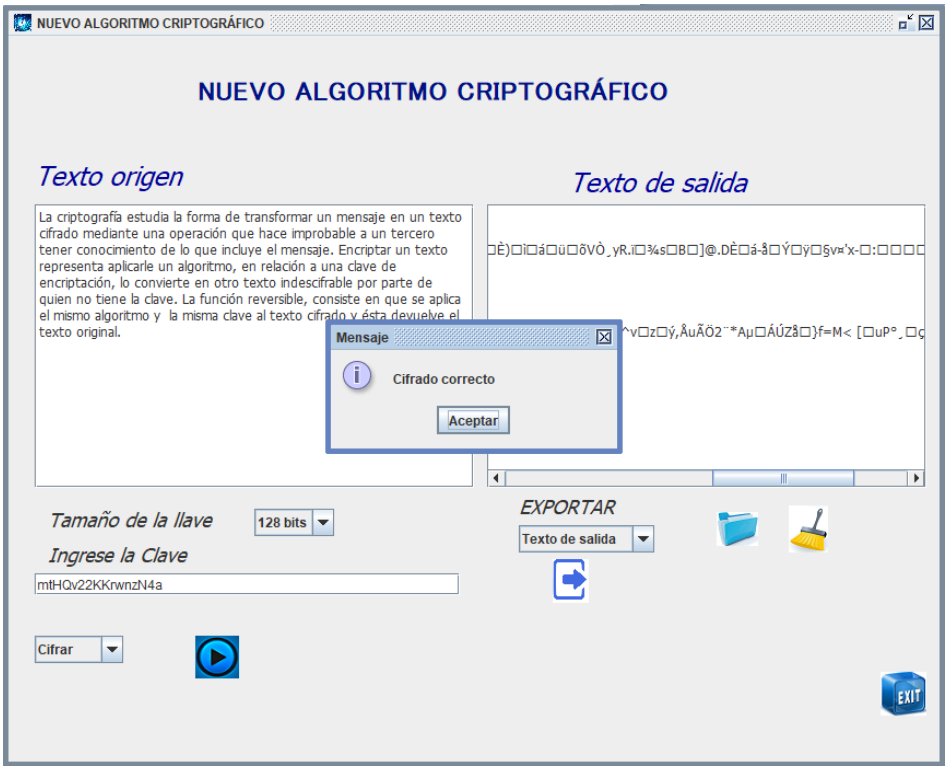


Figura 7-4: Ejecución del cifrado nuevo Algoritmo, 128bits
Realizado por: Cushpa Ana, 2018

4.1.2.1.2. Clave de 192 bits

En la comprobación del proceso de cifrado se utiliza los datos de la Tabla 8-4.

Tabla 8-4: Datos utilizados en la ejecución con el nuevo algoritmo 192 bits

Documento Origen	Clave de cifrado (192 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4 amtHQv22K	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados que se obtienen con la ejecución del prototipo II-E se muestra en la Figura 8-4

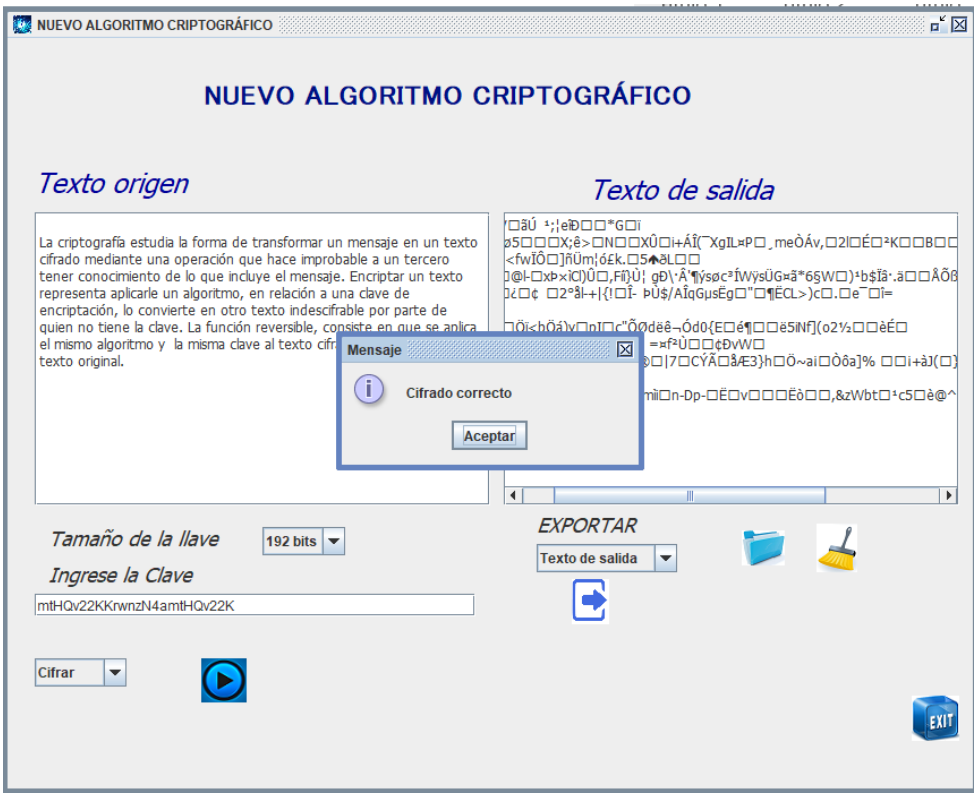


Figura 8-4: Ejecución del cifrado nuevo Algoritmo, 192 bits
Realizado por: Cushpa Ana, 2018

4.1.2.1.3. Clave de 256 bits

En la comprobación del proceso de cifrado se utiliza los datos de la Tabla 9-4.

Tabla 9-4: Datos utilizados en la ejecución con el nuevo algoritmo 256 bits

Documento Origen	Clave de cifrado (256 bits)	Mensaje
Archivo.txt	mtHQv22KKrwnzN4aKrwnzN4amtHQv22K	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados que se obtienen con la ejecución del prototipo II-E se muestra en la Figura 9-4

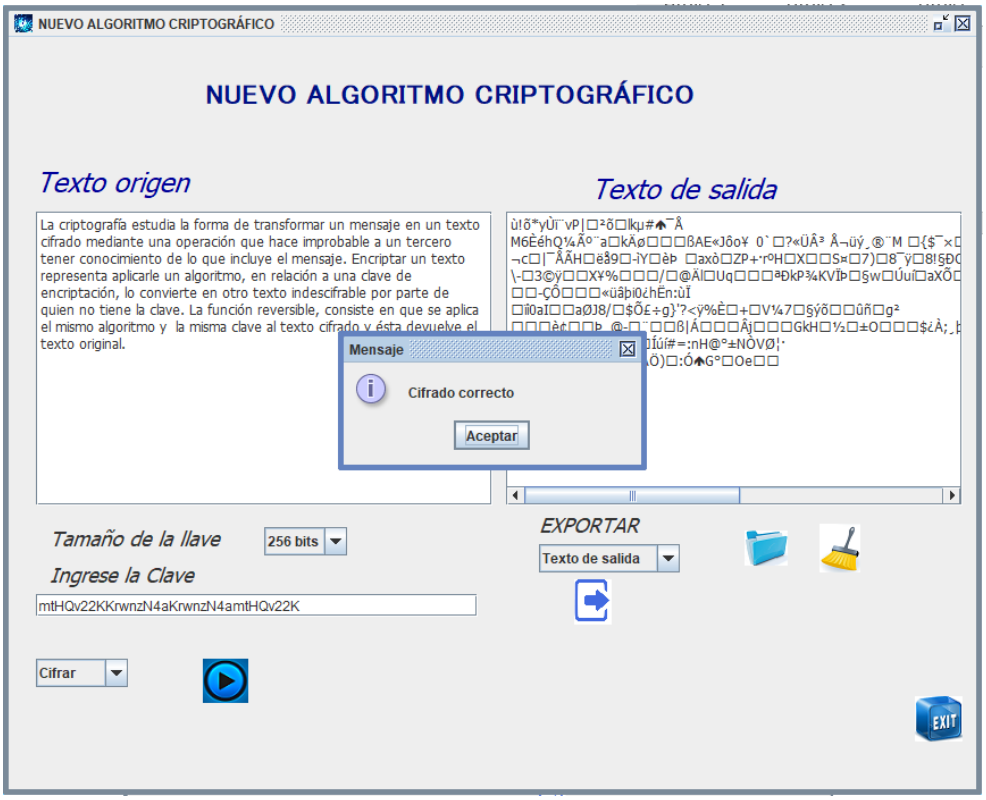


Figura 9-4: Ejecución del cifrado nuevo Algoritmo, 256 bits
Realizado por: Cushpa Ana, 2018

4.1.2.1. Descifrado

4.1.2.2.1. Clave de 128 bits

En la comprobación del proceso de cifrado se utiliza los datos de la Tabla 10-4.

Tabla 10-4: Datos utilizados en la ejecución con el nuevo algoritmo 128 bits

Documento Origen	Clave de cifrado (128 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4a	ú□□□s4>e□¿□I□3Ô□□Û□v□W¸iBÈ□¸(Pz¾□×d0¢A»¦□QX½□ □1 +z×X□äP□ÝGìHpÞÚY□ï-iCÌK□Ém□uìZø4ýÐµ□ÿ{□®¿BlÇr□å¢·sgèHn(□bÔ□ç9□¹□lÜoÍÃ§□8srD f□@÷p°¬-à□□S□H$¥, þu lÓ^b□MU□*G/¥Ïñ□E=□>AË□{UléÃ6"o8□¢□q¾ÈâÄù¯À]ß4□N. □-ÍWl!Á□□Z&¤□Ý□□~ðT□□$TûXù□*Ùþl³,_É©²i,□□□□ ~□³¦□®Àim □Ü□9Þ□Ù□]ç3»□□ÉeÎAØ□ôÏC%+©□iõN□Â"□z$|□

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados que se obtienen con la ejecución del prototipo se muestra en la Figura 10-4

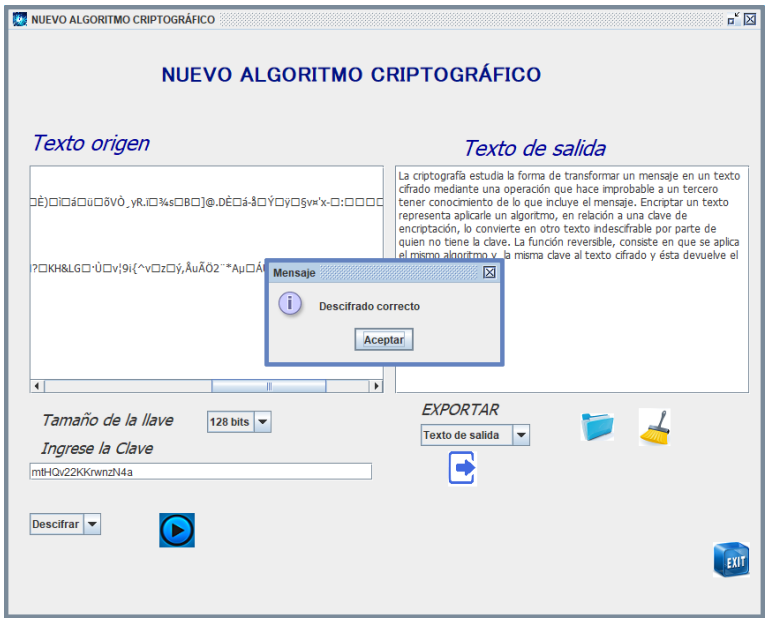


Figura 10-4: Ejecución descifrado nuevo Algoritmo, 128 bits
Realizado por: Cushpa Ana, 2018

4.1.2.2.2 Clave de 192 bits

En la comprobación del proceso de cifrado se utiliza los datos de la Tabla 11-4.

Tabla 11-4: Datos utilizados en la ejecución con el nuevo algoritmo 192 bits

Documento Origen	Clave de cifrado (192 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4 amtHQv22K	·Vh□ÎÌi□9óõÏ%é□¯Úß□p\%:□□Æ□Ræ□hsBGyÊ3-t□□□ý□µüD;yJ)jÌ□½^A?T□□□ 2□éý"ß=Â-ýfø %½Âá□□À&ªÊ□ãw□=tß□Øó$3□ CJIm□__□□Êý□¿ ¦□µw8□ºJyVS:□µñpAaA□ÊòÐ□□N2C»BpÁµ¶Üð²m□□~Wá(4ågf\+ç QÁ□{~´ÿ°À T□ □ÉäIè¼LÈ□□□ã□□Â□mwE□□□Ì□äÉ□æL¨□□Ú □ù□B]âÍ□k□□4_CÏ□S½□□¥□□□È[êQp□□¯Ò¯À↑þVl%□dn□|A

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados que se obtienen con la ejecución del prototipo se muestra en la Figura 10-4

Figura 11-4: Ejecución descifrado nuevo Algoritmo, 192 bits
Realizado por: Cushpa Ana, 2018

4.1.2.2.3 Clave de 256 bits

En la comprobación del proceso de cifrado se utiliza los datos de la Tabla 12-4.

Tabla 12-4: Datos utilizados en la ejecución con el nuevo algoritmo 256 bits

Documento Origen	Clave de cifrado (256 bits)	Mensaje
cifrado.txt	mtHQv22KKrwnzN4aKrwnz N4amtHQv22K	ù!õ*yÙï¨vP|□²õ□lkµ#↑¯Å M6ÈéhQ¼Ã°¨a□kÄø□□□ßAE«Jôo¥ 0`□?«ÜÂ³ Å¬üý¸®¨M □{$¯×□ ¬c□\|¯ÅÃH□ëå9□-ïY□èÞ □axò□ZP+·r°H□X□□S¤□7)□8¯ÿ□8!§Đ□ \-□3©ÿ□□X¥%□□□/□@Äl□Uq□□□ªĐkP¾KVÏÞ□§w□Úuí□aXÕ□ □□-ÇÔ□□□«üâþi0¿hËn:ùÏ □íl0aI□□aØJ8/□$Õ£÷g}'?<ÿ%È□+□V¼7□§ýõ□□ûñ□g² □□□è¢□□Þ_@-□¨□□ß|Á□□□Âj□□□GkH□½□±O□□□$¿À;¸þ □²teÊpR□1r8ã²ð□□Íúí#=:nH@°±NÒVØ¦· □□!□ËhÙRWA□Ñ]ÁÖ)□:Ó↑G°□Oe□□

Realizado por: Cushpa Ana, 2018

Resultados

Los resultados que se obtienen con la ejecución del prototipo II.E se muestra en la Figura 12-4

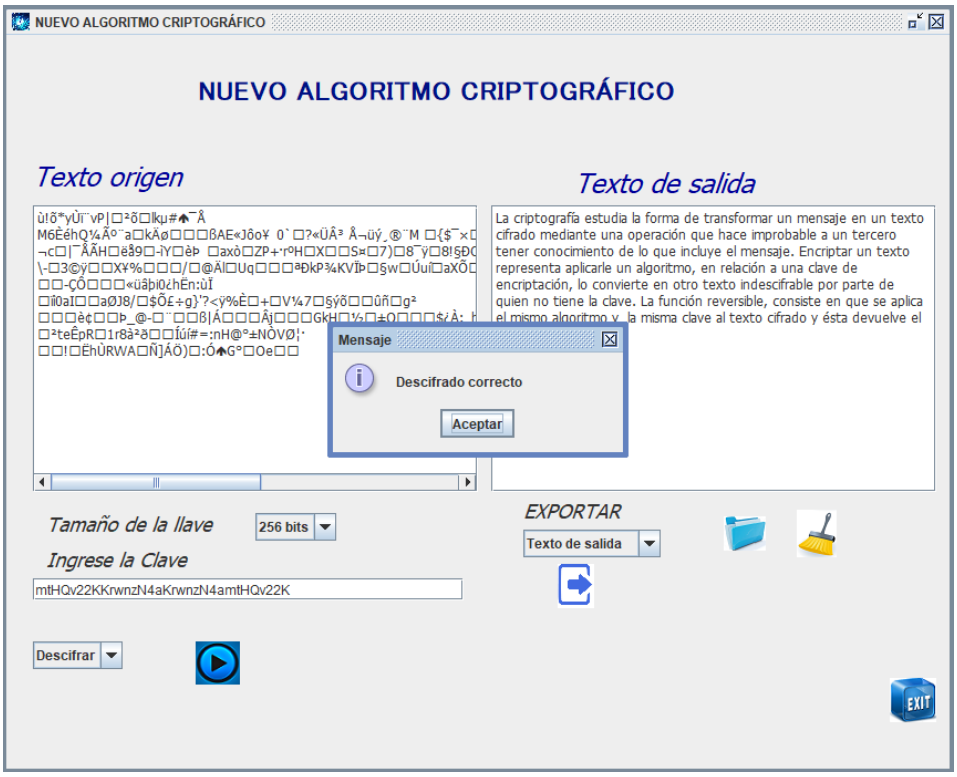


Figura 12-4: Ejecución descifrado nuevo Algoritmo, 256 bits
Realizado por: Cushpa Ana, 2018

4.2. Análisis y comparación de resultados

Después de ejecutar los procesos criptográficos en las pruebas realizadas de los escenarios establecidos, proviene realizar el análisis y comparación de los resultados obtenidos.

4.2.1. Comparación de resultados

4.2.1.1. Clave de 128 bits

La comparación de los resultados se realiza con los mensajes cifrados por los prototipos I-E y II-E con la clave de 128 bits, se exponen en la Tabla 13-4

Tabla 13-4: Comparación de los mensajes cifrados, clave 128 bits

Prototipo I-E	Prototipo II-E
ó6ßÎÈiGÿÂïÐéòÕç'□®Ã -□RÌM□V OÖ¿ÞÎ 3~□½□ W□Á]□*Â□twfn ×3□½¦;□8□,U±{'□ë□8.]-Â□□♠□□£&·¾8 Â÷□$T□¾Î!&p□Ë)ªû□ÉÇ□-g` Ô¿Uàj□Ûâïñ²RÓ²□f□¯SlË..(d,□□□□ ¨É⁰×<rÇ_Hµ¬ê+□_$□«X^□□□w□□Õ¿s¸1□Áø4B□□□□□%û□ □ïáI□¬\² åd³èÃVtå{□¹□□×□□♠(□□h□□T□<R□IÙ□□U□Ò'÷rI§å·ªh¢@ ¦ ènÆ□á]-ß¸□tU¹□|Ô□□ï®¤Å□□±□□ØòI&{ÖþÕH+ÙÛÑQ#rïãÎª□Ø; _qmù« □Á□DAéÚ´©B□_l□□c2[ßLÉ¬½Çú□w¼□F□Ñ□□Â□Æ□0 ñ□F|□jG¤;□ïë: ,å□Ú_Ú□nÖÉ♠©□0æ·sGH□Ð7□°([õÃ□á±\ûàüRcÃd?k 9÷□|¿	ú□□□s4>e□¿□I□3Ô□□Û□v□W¸ìBÈ□¸(Pz¾□×d0¢A»¦□QX½□ □1 +z×X□äP□ÝGïHpÞÚY□i-iCÏK□Ém□uïZø4ýÐµ□ÿ{□®¿BlÇr□å¢·sgèHn(□bÔ□ç9□¹□lÜoÍÃ§□8srD f□@÷p°¬-à□□S□H$¥, þu lÓ^b□MU□*G/¥Îñ□E=□>AË□{UléÃ6"o8□¢□q¾ÈâÄù¯À]ß4□N. □-ÍWl!Á□□Z&¤□Ý□□~ðT□□$TûXù□*Ùþl³,_É©²i,□□□□ ~□³¦□®Àim □Ü□9Þ□Ù□]ç3»□□ÉeÎA Ø□ôÎC%+©□ïõN□Â"□z$|□

Realizado por: Cushpa Ana, 2018

4.2.1.2. Clave de 192 bits

La comparación de los resultados se realiza con los mensajes cifrados por los prototipos I-E y II-E con la clave de 192 bits, muestra la Tabla 14-4

Tabla 14-4: Comparación de los mensajes cifrados, clave 192 bits

Prototipo I-E	Prototipo II-E
oJ3S¬□uÏà□¨□é□Í□¶b7ÉÚô¬ñé+¤ús□□□□hãã ½□4ßÕ□ÙÊ)□ □/CRÛ;Þ□eèø*□[L□¶¾W□□□â□□{Æju~ª□1 G^Z;¢>ûçMþå;□□ Ûþ□1ó□Á□i¦'@aëÿ%Î$£©□ø ëö3à□□gcL6=□frË□□ôÓÌLÓ □□ÄØ□□XCÑ©÷~âA·½iÌ`È□□□74G□□}'□¿Wã□f®b`Ì%0□m□ □T+¬ÖÈòÔL ¥{□□å3w□ïäÛ□½ã□□óGõð□ýÖ¾}XLÆ ¥Èzú□□ñc ã[ÍDPxj□□e□D <@□¦¬,ç □`S□ã3A~□Kí□ªÙ%ÁYhØùH□øâ□ê□·êGùU□¢_□Æ/´□ º:iÊ,□Ê×qòÒll□O□'ö-Û_Ç□□È□Ú#fº£□y□□0□□Pª³ùO_ôè+D□□□ P□/.è',.□f8□yH%□T□C□V~gfÎ³5Ôõñ͍Æ+ïÏ	·Vh□ïÌi□9óõÏ%é□¯Úß□p\%:□□Æ□Ræ□hsBGyÊ3-t□□□ý□µüD;yJ)jÌ□½^A?T□□□ 2□éý"ß=Â-ýfø %½Âã□□À&ªÊ□ãw□=tß□Øó$3□ CJIm□__□□Êý□¿ ¦□µw8□ºJyVS:□µñpAaA□Êòð□□N2C»BpÁµ¶Üã²m□□~Wá(4ågf\+ç QÁ□{~´ÿ°À T□ □ÉäIè¼LÈ□□□ã□□Â□mwE□□□Ì□ïäÉ□æL¨□□Ú ¬ù□B]âÍ□k□□4_CíÎ□S½□□¥□□□Ê[êQp□□¯Ò¯À♠þVï%□dn□|A

Realizado por: Cushpa Ana, 2018

4.2.1.3. Clave de 256 bits

Para comparar los resultados se realiza con los mensajes que han sido cifrados por los prototipos I-E y II–E con la clave de 256 bits, se presentan en la Tabla 15-4

Tabla 15-4: Comparación de los mensajes cifrados con una clave de 256 bits

Prototipo I-E	Prototipo II-E
□i□□□m¿□ïõ□□□nü□Ví□□z□□e□úØõáe □ «C/□¹□{4M½□~W□âTC*□**<nZ□□)□ÊÃ¼□ÏÀV¬□□}ÆØb_§□ □7sF ç□1j¾ÔÔV□□cË7ø\wZzÉ: ¿□µLÂpò5R*¬2®ÝcYz□ÒOë□Y□M>»Ã □õX*□ÐI□Ù□ÑïäCÓHø□□@ûg»o□□Ó±□ÎTp&□G%+ :8Ú1□ □c8;é#ãæÆ□Q-s¾□t©nºº{ñ□P4(ñóßÿÞ:üµ□□□f½ì=i□µådÚ4gè# □}□□□~mbµeb¶□c¨□□&□□^`FGÆÓ?n_½H*øn»□®e&oÚè\»□ □<¢Øk□0G¯&□k□Õ□ÖÑ□□□p♠□& □àÎê&□¾Ø|□Z□«Íã□□-åC pÉ□□□□0/□□ê¤-QN*È□ $à□ ©ó¥	ù!õ*yÙï¨vP|□²õ□lkµ#♠¯Å M6ÈéhQ¼Ã°¨a□kÁø□□□ßAE«Jôo¥ 0`□?«ÜÂ³ Å¬üý¸®¨M □{$¯×□ ¬c□\|¯ÅÃH□ëå9□-ìY□èÞ □axò□ZP+·rºH□X□□S¤□7)□8¯ÿ□8!§Ð□ \-□3©ÿ□□X¥%□□□/□@Ä\|□Uq□□□ªÐkP¾KVÏÞ□§w□Úuî□aXÕ□ □□-ÇÔ□□□«üâþi0¿hËn:ùÎ □ïî0aI□□aØJ8/□$Õ£÷g}'?<ÿ%È□+□V¼7□§ýõ□□ûñ□g² □□□è¢□□Þ_@-□¨□□ß|Á□□□Âj□□□GkH□½□±O□□□$¿À;¸þ □²teÊpR□1r8à²ð□□Íúí#=;nH@°±NÒVØ¦· □□!□ËhÙRWA□Ñ]ÁÖ)□:Ó♠G°□Oe□□

Realizado por: Cushpa Ana, 2018

4.3. Prueba de hipótesis

4.3.1. Pruebas

Para realizar la comprobación de la hipótesis se efectuarán las siguientes pruebas:

- Análisis de las principales características del algoritmo definido como AES base que se ha implementado en el Prototipo I y del Prototipo II donde se ha implementado las funciones propuestas, con el indicador: No. de funciones usadas por el algoritmo, que se realiza en la variable dependiente (seguridad).
- Criptoanálisis que se realiza en los mensajes cifrados con el Prototipo I-E y Prototipo II-E, para la variable dependiente (seguridad) con los indicadores: Entropía, Histograma, Autocorrelación, Resistencia contra fuerza bruta.

Para medir los indicadores se maneja los datos promedio de los resultados que se obtienen del Prototipo I-E y Prototipo II-E.

4.3.1.1. Análisis de características de los algoritmos

En la comparación se considera los siguientes indicadores:

- No. de funciones utilizadas
- No. de rondas

Se muestra en la Tabla 16-4.

Tabla 16-4: Definición de indicadores en la comparación de algoritmos

Indicador 1	Prototipo I-E	Prototipo II-E
No. de funciones utilizadas	addRoundKey subByte ShiftRow MixColumn	addRoundKey subByte ShiftRow MixColumn MixDiagonal
No. de rondas	Clave de 128 bits: 10 rondas Clave de 192 bits: 12 rondas Clave de 256 bits: 14 rondas	Clave de 128 bits: 15 rondas Clave de 192 bits: 18 rondas Clave de 256 bits: 21 rondas

Realizado por: Cushpa Ana, 2018

4.3.1.1.1. Resultado del análisis

Luego de realizar la comparación de características en los dos algoritmos implementados se muestran los resultados en la Tabla 17-4

Tabla 17-4: Comparación de indicadores

No.	Indicador	Prototipo I-E			Prototipo II-E		
		128 bits	192 bits	256 bits	128 bits	192 bits	256 bits
1	No. de funciones utilizadas	4	4	4	5	5	5
2	No. de rondas	10	12	14	15	18	21

Realizado por: Cushpa Ana, 2018

Para mostrar el promedio obtenido de los indicadores se presenta la Tabla 18-4

Tabla 18-4: Promedio de comparación Prototipo I y Prototipo II

No.	Indicador	Prototipo I-E	Prototipo II-E
1	No. de funciones utilizadas	4	5
2	No. de rondas	12	18

Realizado por: Cushpa Ana, 2018

Los resultados de la comparación realizada con los indicadores 1 y 2 se muestran en la Figura 13-4

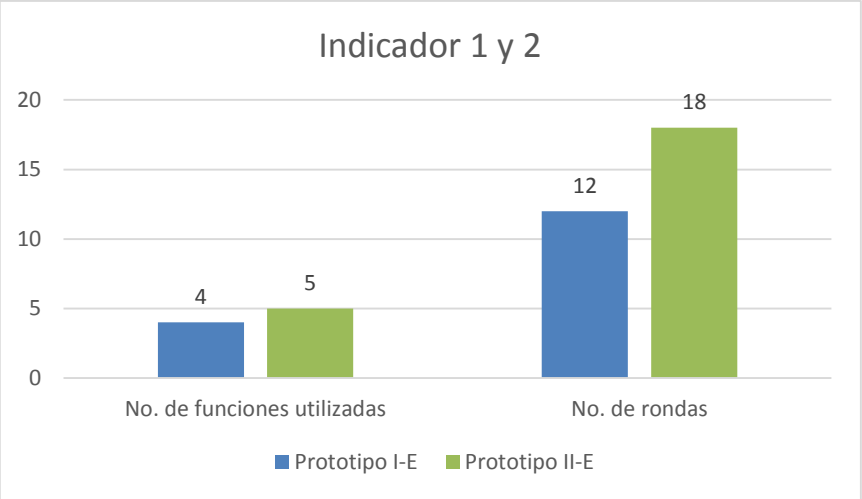


Figura 13-4: Valor promedio, indicador 1 y 2
Realizado por: Cushpa Ana, 2018

El prototipo II-E muestra mayor número de funciones utilizadas y mayor número de rondas, que ayudan a una mayor difusión del mensaje.

4.3.1.2. Criptoanálisis de los mensajes cifrados por los algoritmos

4.3.1.2.1. Ambiente de pruebas

Se realiza la comparación de los prototipos I y II donde se ha implementado el algoritmo AES base y el nuevo algoritmo propuesto respectivamente. Se han definido para la variable dependiente los siguientes indicadores:

- Entropía
- Histograma
- Autocorrelación
- Fuerza bruta

Para realizar el criptoanálisis se utiliza la herramienta Cryptool donde se comparan los mensajes cifrados de 128, 192 y 256 bits en los 2 prototipos donde se ha implementado el algoritmo AES base y el nuevo algoritmo.

Para ello se utilizan los datos que mostrados en la Tabla 19-4

Tabla 19-4: Datos utilizados para ejecutar las pruebas

Clave: 128 bits	mtHQv22KKrwnzN4a
Clave: 192 bits	mtHQv22KKrwnzN4amtHQv22K
Clave: 256 bits	mtHQv22KKrwnzN4aKrwnzN4amtHQv22K
Mensaje	La criptografía estudia la forma de transformar un mensaje en un texto cifrado mediante una operación que hace improbable a un tercero tener conocimiento de lo que incluye el mensaje. Encriptar un texto representa aplicarle un algoritmo, en relación a una clave de encriptación, lo convierte en otro texto indescifrable por parte de quien no tiene la clave. La función reversible, consiste en que se aplica el mismo algoritmo y la misma clave al texto cifrado y ésta devuelve el texto original.

Realizado por: Cushpa Ana, 2018

4.3.1.2.1.1. Mensajes cifrados

Los mensajes cifrados muestran caracteres imprimibles y no imprimibles de acuerdo con la tabla ASCII.

4.3.1.2.1.1.1. Clave de 128 bits

El mensaje cifrado por el Prototipo I-E con la clave de 128 bits se muestra en la Figura 14-4

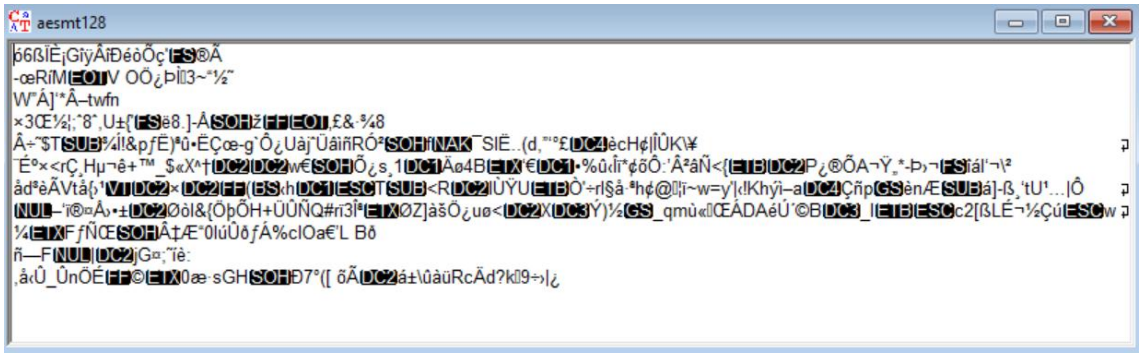


Figura 14-4: Texto cifrado con el prototipo I-E, 128 bits
Realizado por: Cushpa Ana, 2018

En la Figura 15-4 se muestra el mensaje cifrado por el Prototipo II-E y una clave de 192 bits.

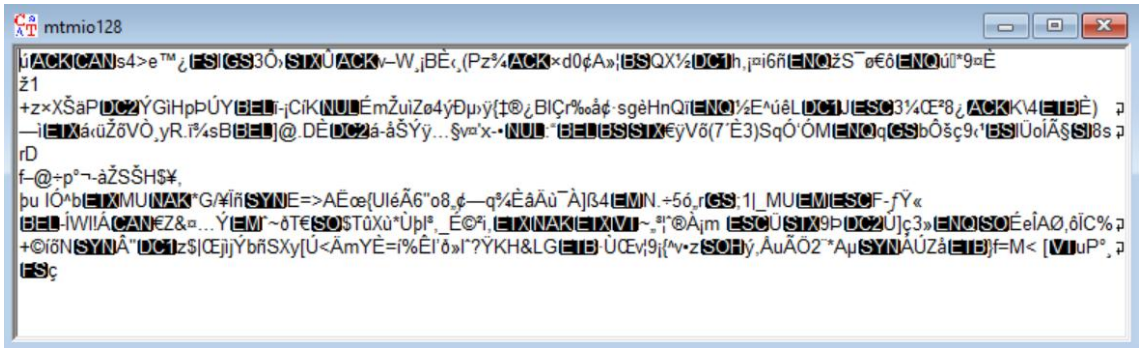


Figura 15-4: Mensaje cifrado por el prototipo II-E, 128 bits
Realizado por: Cushpa Ana, 2018

4.3.1.2.1.1.2. Clave de 192 bits

El mensaje cifrado por el Prototipo I-E con una clave de 192 bits muestra la Figura 16-4

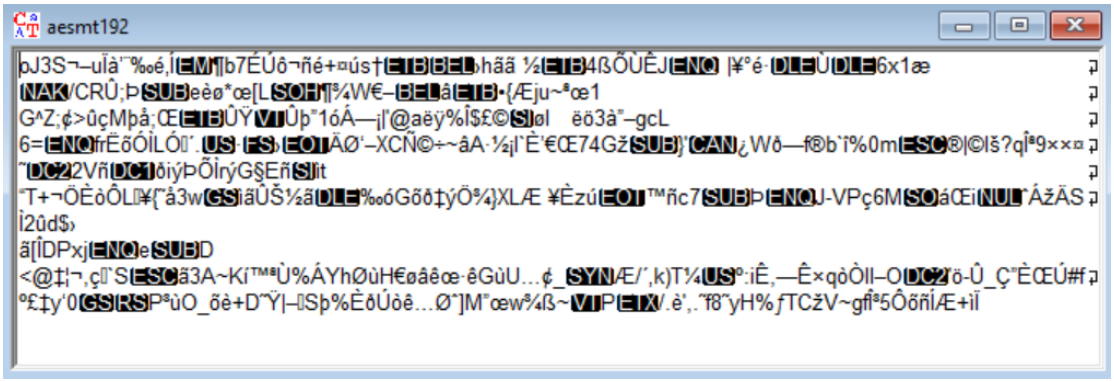


Figura 16-4: Mensaje cifrado por el prototipo I-E, 192 bits
Realizado por: Cushpa Ana, 2018

En la Figura 17-4 se muestra el mensaje cifrado con el Prototipo II-E

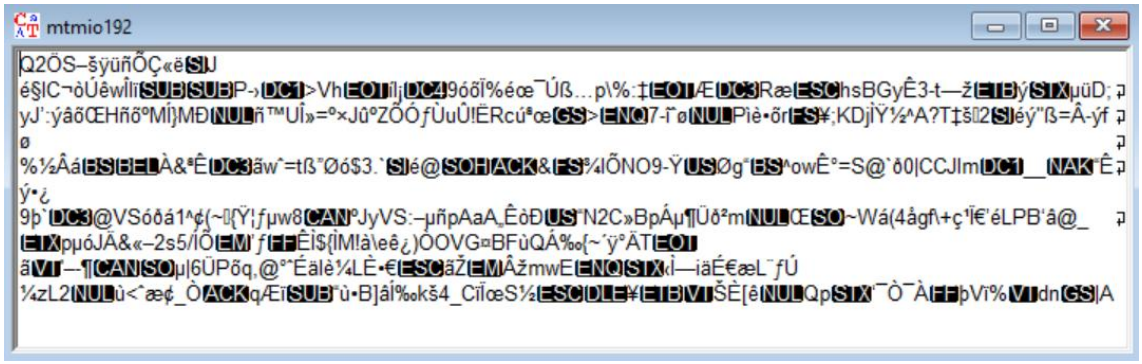


Figura 17-4: Mensaje cifrado con el prototipo II-E, clave de 192 bits
Realizado por: Cushpa Ana, 2018

4.3.1.2.1.1.3. Clave de 256 bits

El texto cifrado por el Prototipo I con una clave de 256 bits muestra la Figura 18-4

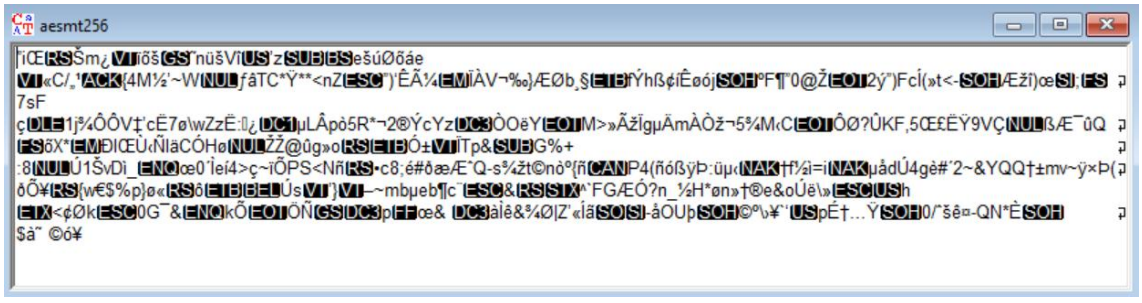


Figura 18-4: Mensaje cifrado con el prototipo I-E, 256 bits
Realizado por: Cushpa Ana, 2018

A continuación, la Figura 19-4 muestra el mensaje cifrado con el Prototipo II-E

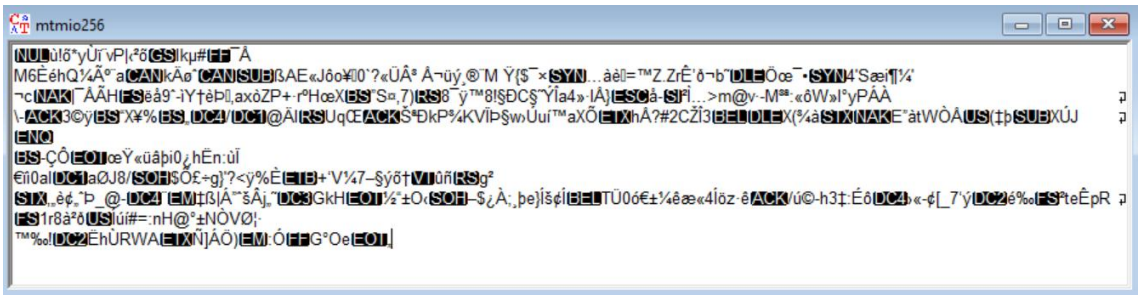


Figura 19-4: Mensaje cifrado con el prototipo II-E, 256 bits
Realizado por: Cushpa Ana, 2018

4.3.1.2.1.2. Definición del alfabeto

Para realizar las pruebas de criptoanálisis se maneja un alfabeto extenso de 98 caracteres donde se define las siguientes opciones que se muestran en la Figura 20-4

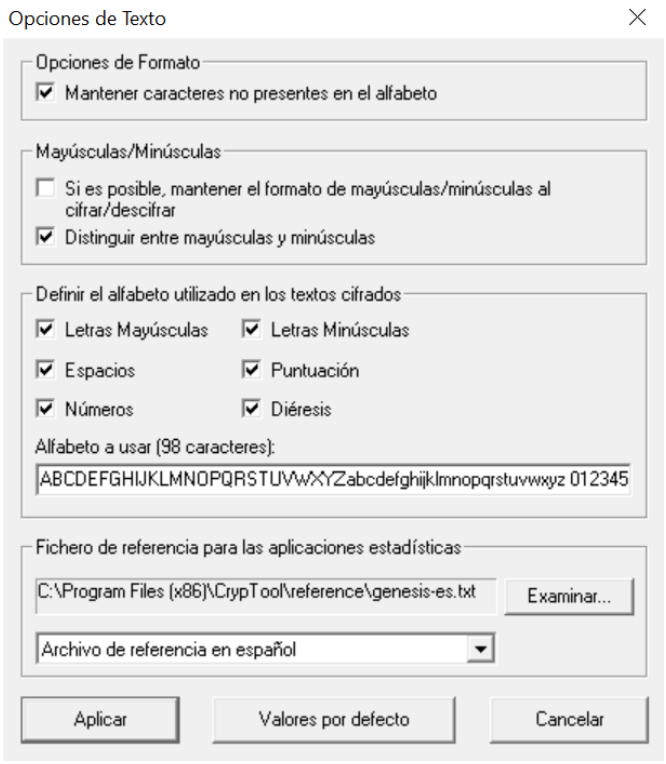


Figura 20-4: Definición del alfabeto
Realizado por: Cushpa Ana, 2018

4.3.1.2.2. Criptoanálisis

Los experimentos de criptoanálisis que se realizaron a los 5 indicadores anteriormente definidos, presentan los siguientes resultados:

4.3.1.2.2.1. Indicador 2: Entropía

Para definir el nivel de difusión que presentan los mensajes cifrados con el Prototipo I-E y II-E se realiza la prueba de entropía.

4.3.1.2.2.1.1. Clave de 128 bits

El análisis de los mensajes cifrados con la clave de 128 bits se muestra en las siguientes Figuras:

Prototipo I-E

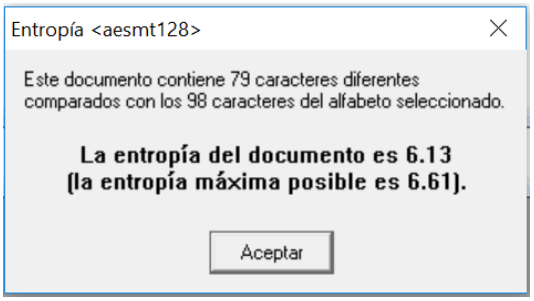


Figura 21-4: Entropía, prototipo I-E, 128 bits
Realizado por: Cushpa Ana, 2018

Prototipo II-E

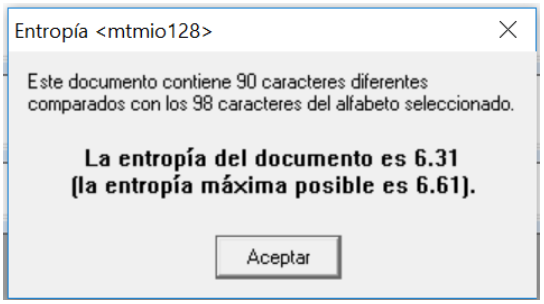


Figura 22-4: Entropía, prototipo II-E, 128 bits
Realizado por: Cushpa Ana, 2018

El texto cifrado con el prototipo II-E contiene mayor número de caracteres diferentes que el texto cifrado con el prototipo I-E, lo cual ayuda a que el mensaje sea más difuso.

4.3.1.2.2.1.2. Clave 192 bits

El análisis de los mensajes cifrados con la clave de 192 bits se muestra en las siguientes Figuras:

Prototipo I-E

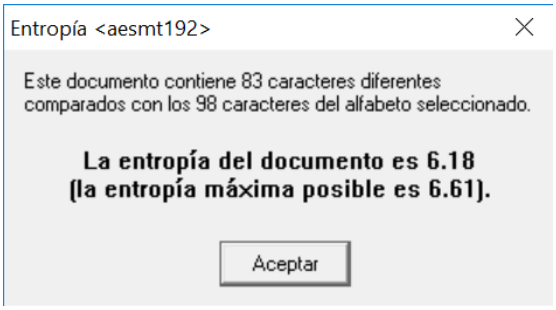


Figura 23-4: Entropía, prototipo I-E, 192 bits
Realizado por: Cushpa Ana, 2018

Prototipo II-E

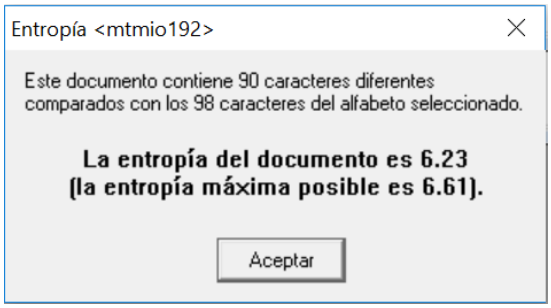


Figura 24-4: Entropía, prototipo II-E, 192 bits
Realizado por: Cushpa Ana, 2018

En el prototipo II-E se presenta mayor número de caracteres diferentes que en prototipo I-E, contribuyendo así a incrementar la difusión en la información.

4.3.1.2.2.1.3. Clave 256 bits

El análisis de los mensajes cifrados con la clave de 256 bits se muestra en las siguientes Figuras:

Prototipo I-E

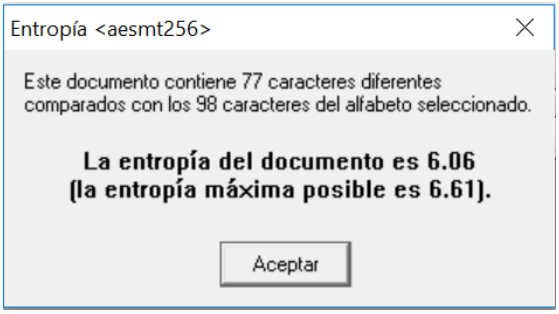


Figura 25-4: Entropía, prototipo I-E, 256 bits
Realizado por: Cushpa Ana, 2018

Prototipo II-E

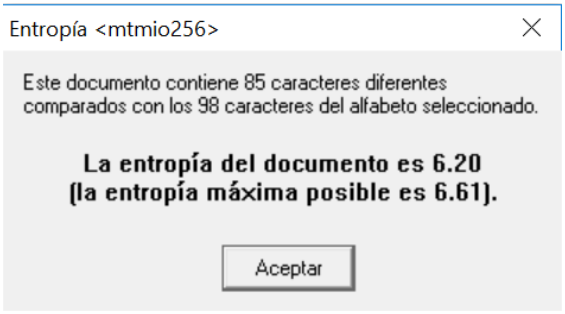


Figura 26-4: Entropía, prototipo II-E, 256 bits
Realizado por: Cushpa Ana, 2018

El documento cifrado con el prototipo II-E presenta mayor número de caracteres diferentes que el prototipo I-E, logrando de esta forma más difusión del mensaje.

El valor máximo posible de entropía es de 6.61. Los datos obtenidos con las pruebas realizadas con el indicador 3 Entropía se muestran en la Tabla 20-4.

Tabla 20-4: Datos obtenidos de la Entropía en los mensajes cifrados

Prototipo	Caracteres diferentes	Valor de Entropía	Tamaño de clave
Prototipo I-E	79	6,13	128 bits
Prototipo II-E	90	6,31	
Prototipo I-E	83	6,18	192 bits
Prototipo II-E	90	6.23	
Prototipo I-E	77	6,06	256 bits
Prototipo II-E	85	6,20	

Realizado por: Cushpa Ana, 2018

De los valores obtenidos del indicador Entropía aplicados a los textos cifrados en los prototipos I-E y II-E se calcula el promedio, los valores obtenidos se muestran en la Tabla 21-4

Tabla 21-4: Promedio del indicador:3 Entropía

No.	Indicador	Prototipo I-E	Prototipo II-E
3	Entropía	6,12	6,24

Realizado por: Cushpa Ana, 2018

Los valores obtenidos del indicador 3 Entropía se muestra en la Figura 27-4

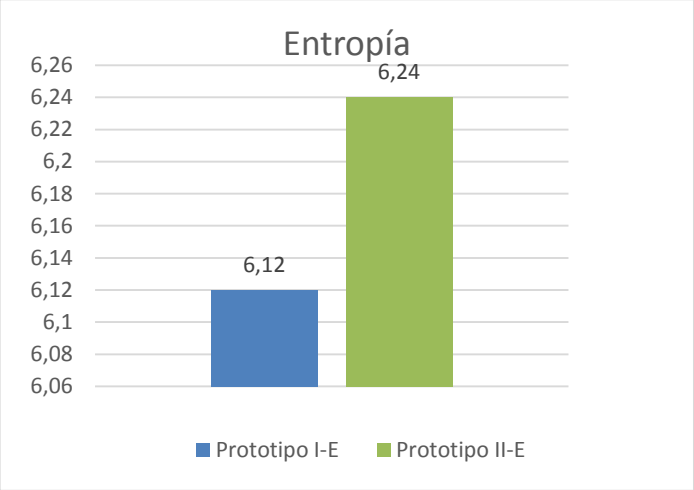


Figura 27-4: Valor promedio Indicador 3: Entropía
Realizado por: Cushpa Ana, 2018

El Prototipo II-E presenta una entropía de 6.24 que es mayor al prototipo I-E que presenta una entropía de 6.12.

4.3.1.2.2.2. Indicador 4: Histograma

En las pruebas de histograma se relaciona los valores que contienen los mensajes cifrados y el porcentaje de frecuencia entre los Prototipos I-E y II-E.

4.3.1.2.2.2.1. Clave de 128 bits.

Los valores obtenidos del análisis de los mensajes cifrados con claves de 128 bits se muestran en las Figuras

Prototipo I-E

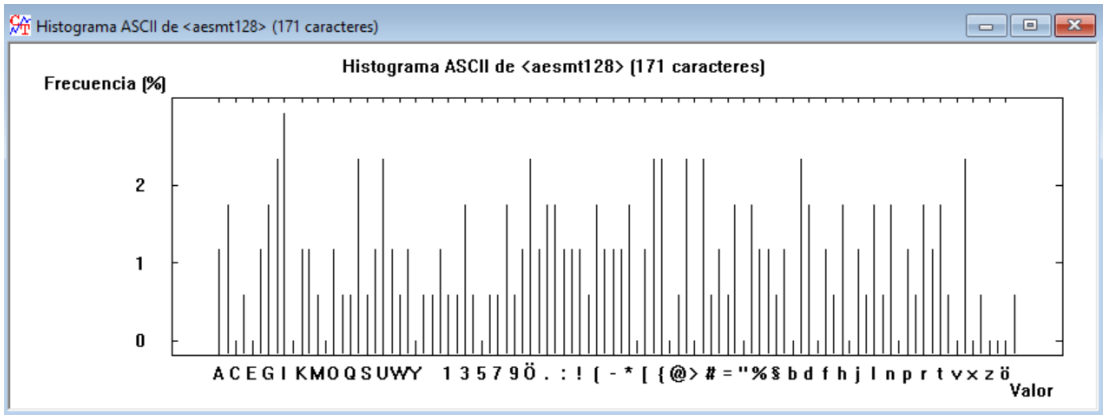


Figura 28-4: Histograma Prototipo I-E, 128 bits
Realizado por: Cushpa Ana, 2018

Con una clave de 128 bits el prototipo I-E utiliza 171 caracteres en el texto cifrado.

Prototipo II-E

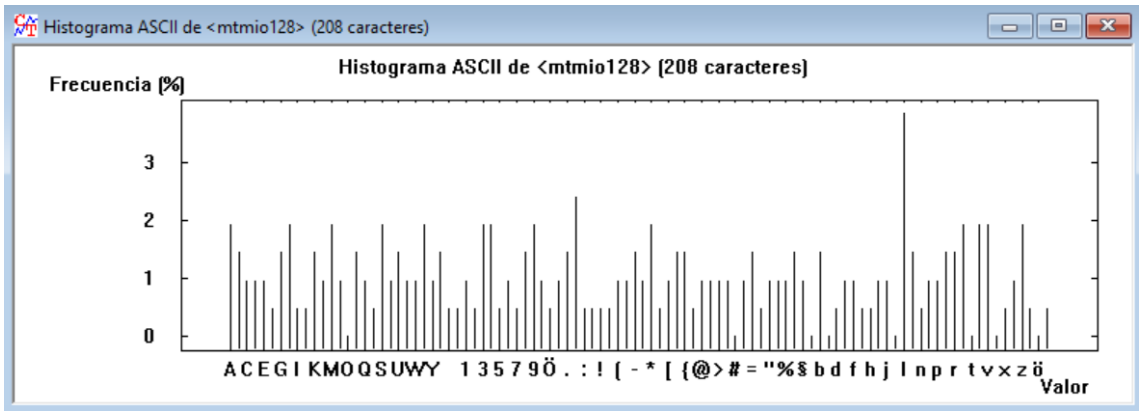


Figura 29-4: Histograma Prototipo II-E, 128 bits
Realizado por: Cushpa Ana, 2018

Con una clave de 128 bits el prototipo II-E utiliza 208 caracteres en el texto cifrado.

4.3.1.2.2.2.2. Clave 192 bits

Los valores obtenidos del análisis de los mensajes cifrados con claves de 192 bits se muestran en las Figuras

Prototipo I-E

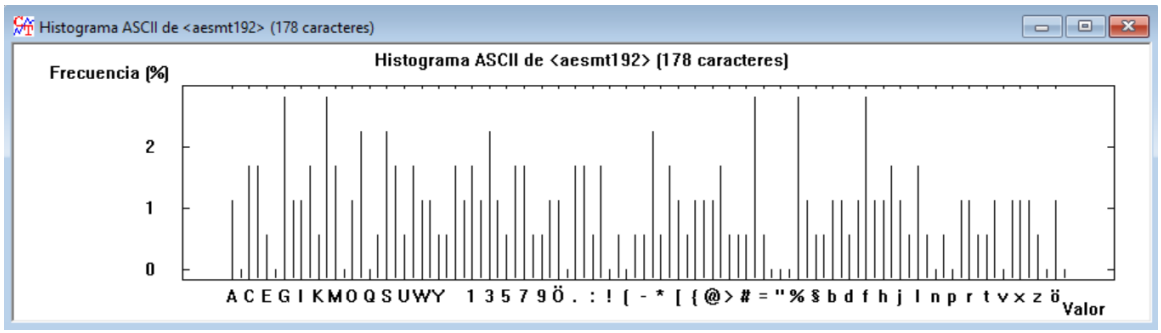


Figura 30-4: Histograma Prototipo I-E, 192 bits
Realizado por: Cushpa Ana, 2018

Con una clave de 192 bits el prototipo I-E utiliza 178 caracteres en el texto cifrado.

Prototipo II-E

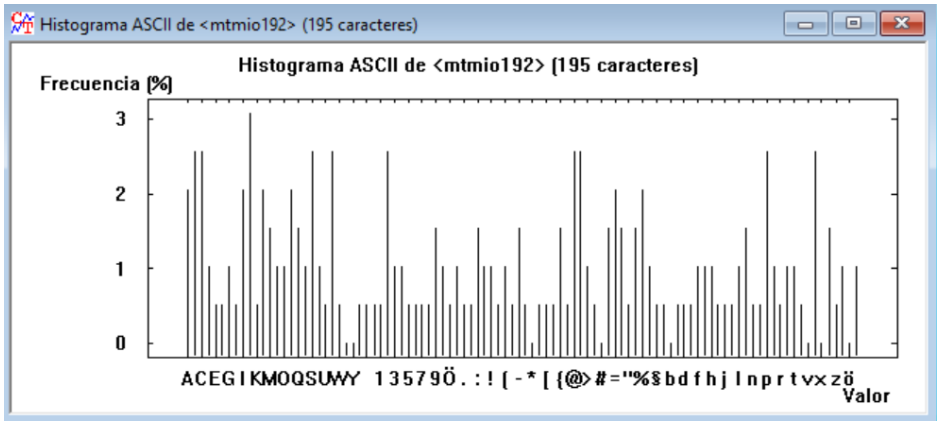


Figura 31-4: Histograma Prototipo II-E, 192 bits
Realizado por: Cushpa Ana, 2018

Con una clave de 192 bits el prototipo II-E utiliza 195 caracteres en el texto cifrado.

4.3.1.2.2.2.3. Clave 256 bits

Los valores obtenidos del análisis de los mensajes cifrados con claves de 256 bits se muestran en las Figuras.

Prototipo I-E

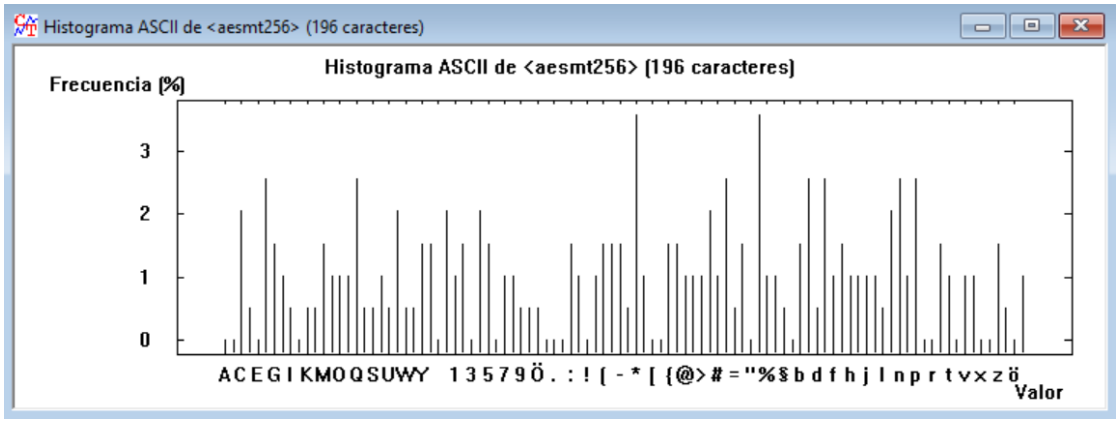


Figura 32-4: Histograma Prototipo I-E, 256 bits
Realizado por: Cushpa Ana, 2018

Con una clave de 256 bits el prototipo I-E utiliza 196 caracteres en el texto cifrado.

Prototipo II-E

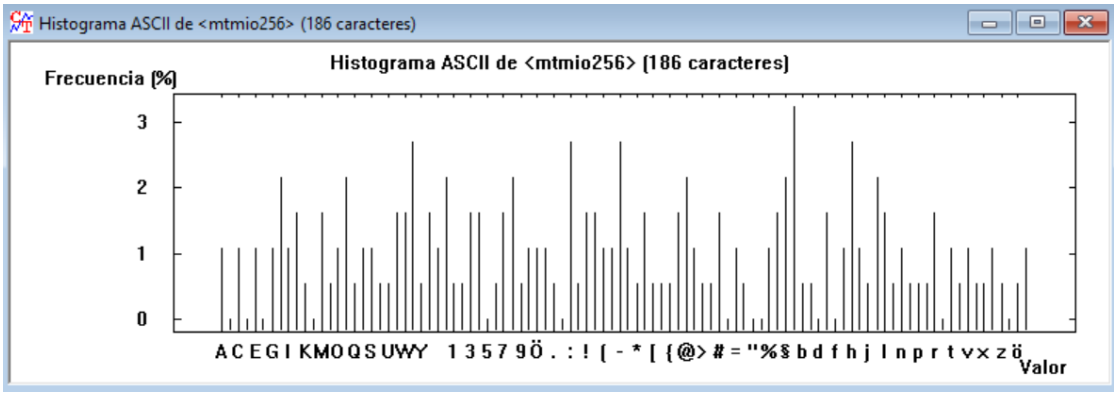


Figura 33-4: Histograma Prototipo II-E, 256 bits
Realizado por: Cushpa Ana, 2018

Con una clave de 256 bits el prototipo II-E utiliza 186 caracteres en el texto cifrado.
Los resultados obtenidos con el indicador 4 Histograma aplicados a los mensajes cifrados por los prototipos I y II se muestran en la Tabla 22-4

Tabla 22-4: Resultados Histograma Prototipo I-E y Prototipo II-E

Prototipo	Caracteres	Tamaño de clave
Prototipo I-E	171	128 bits
Prototipo II-E	208	
Prototipo I-E	178	192 bits
Prototipo II-E	195	
Prototipo I-E	196	256 bits
Prototipo II-E	186	

Realizado por: Cushpa Ana, 2018

Los valores promedios de los resultados obtenidos con la aplicación del indicador 4: Histograma muestran la Tabla 23-4

Tabla 23-4: Valores promedio del indicador 4: Histograma

No.	Indicador	Prototipo I-E	Prototipo II-E
4	Histograma	181,6	196,3

Realizado por: Cushpa Ana, 2018

Los valores obtenidos del indicador 4 Histograma se muestra en la Figura 34-4

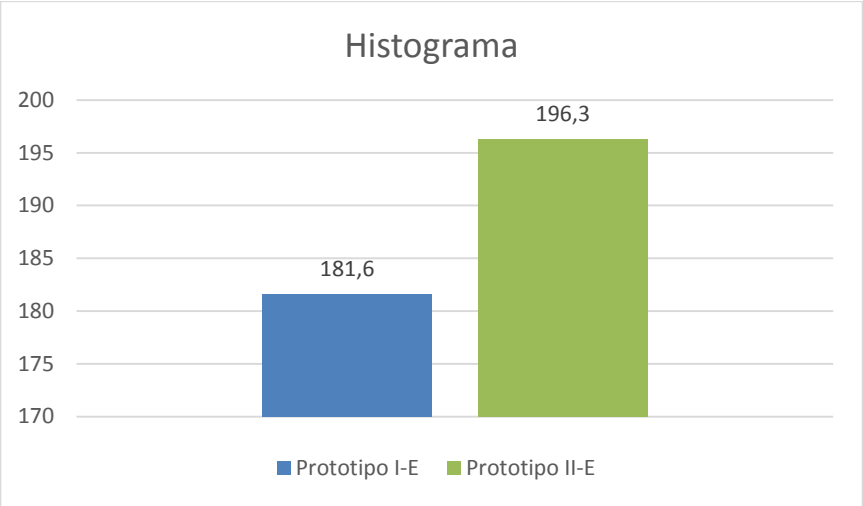


Figura 34-4: Valor promedio Indicador 4: Histograma Prototipo I-E y II-E
Realizado por: Cushpa Ana, 2018

El valor promedio en el indicador 4: Histograma el prototipo II-E presenta 181.6 caracteres empleados en el cifrado de la información que es mayor al prototipo I-E que presenta un valor promedio de 181.6 caracteres empleados en el cifrado de la información.

4.3.1.2.2.3. Indicador 5: Autocorrelación

En las pruebas de autocorrelación se realiza una analogía entre el número de los caracteres que concuerdan y el desplazamiento de mensajes que han sido cifrados por los Prototipos I-E y II-E.

4.3.1.2.2.3.1. Clave de 128 bits

Los mensajes que han sido cifrados con el Prototipo I-E y el Prototipo II-E aplicando una clave de 128 bits se analizan y muestran los resultados en las Figuras.

Prototipo I-E

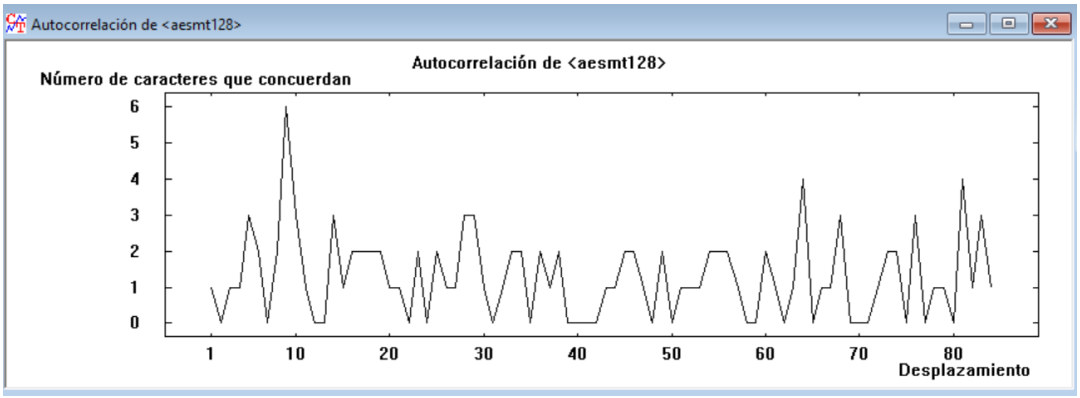


Figura 35-4: Autocorrelación con el Prototipo I-E, 128 bits
Realizado por: Cushpa Ana, 2018

Con la clave de 128 bits el mensaje cifrado por el prototipo I-E presenta un valor máximo de 6 caracteres, los mismos que concuerdan con el desplazamiento de los mensajes.

Prototipo II-E

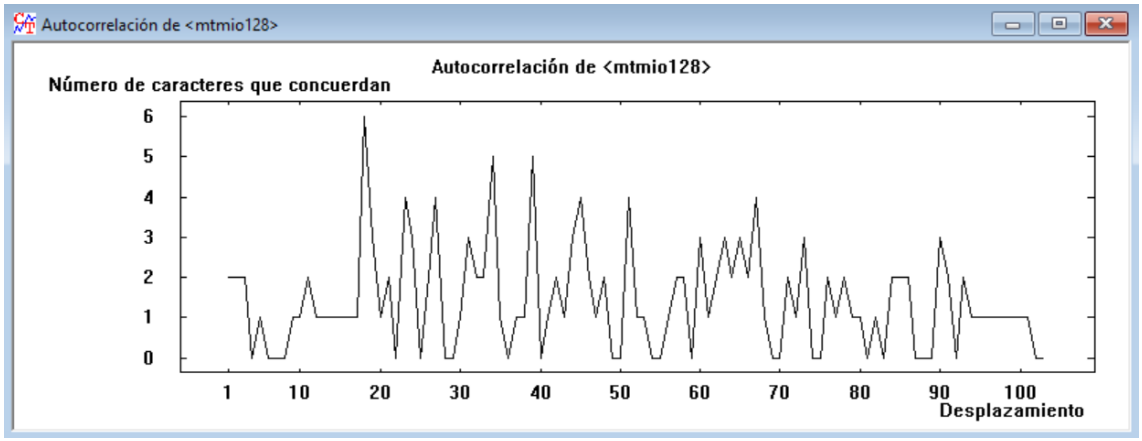


Figura 36-4: Autocorrelación con el Prototipo II-E, 128 bits
Realizado por: Cushpa Ana, 2018

Con la clave de 128 bits el mensaje cifrado por el prototipo II-E presenta un valor máximo de 6 caracteres, mismos que concuerdan con el desplazamiento de los mensajes.

4.3.1.2.2.3.2. Clave de 192 bits

Los mensajes que han sido cifrados con el Prototipo I-E y el Prototipo II-E con una clave de 192 bits se visualizan sus resultados en las Figuras siguientes:

Prototipo I-E

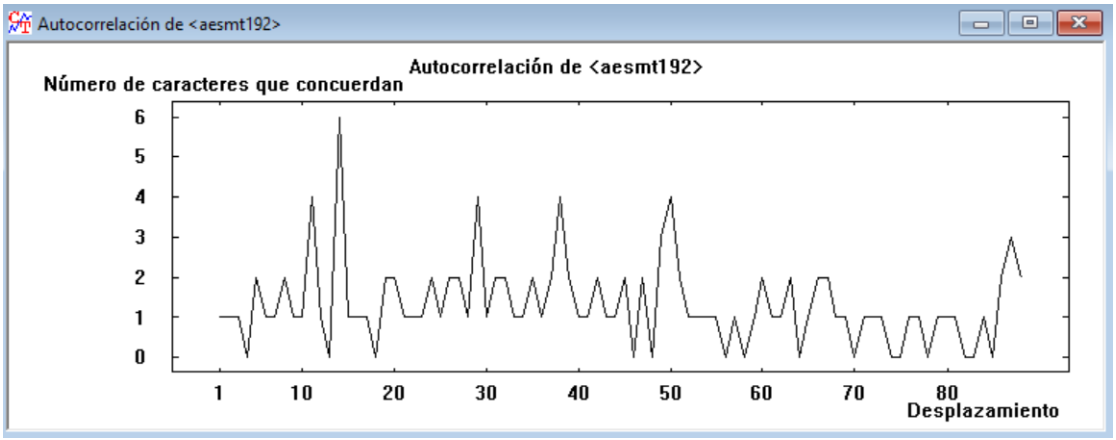


Figura 37-4: Autocorrelación con el Prototipo I-E, 192 bits
Realizado por: Cushpa Ana, 2018

Con la clave de 192 bits el mensaje cifrado por el prototipo I-E presenta un valor máximo de 6 caracteres que concuerdan con el desplazamiento de los mensajes.

Prototipo II-E

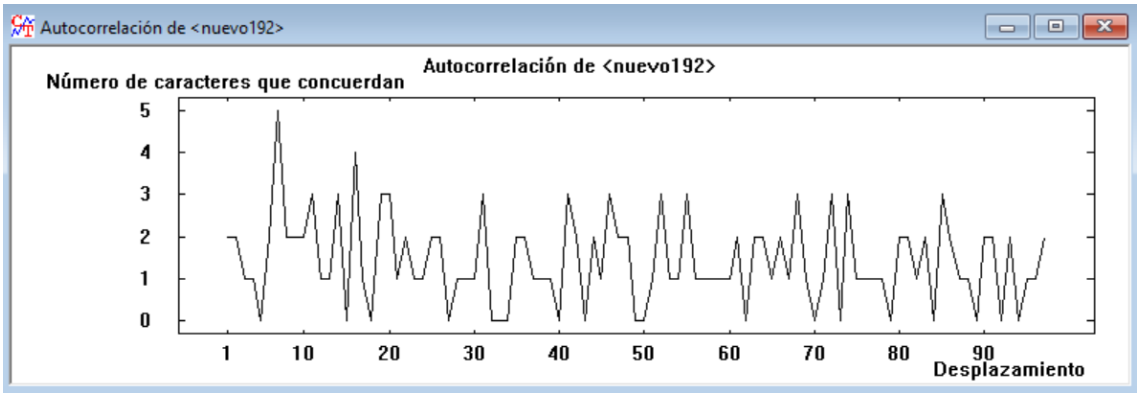


Figura 38-4: Autocorrelación con el Prototipo II-E, 192 bits
Realizado por: Cushpa Ana, 2018

Con la clave de 192 bits el mensaje cifrado por el prototipo I-E presenta un valor máximo de 5 caracteres que son los que concuerdan con el desplazamiento de los mensajes cifrados.

4.3.1.2.2.3.3. Clave de 256 bits

Los mensajes que han sido cifrados con el Prototipo I-E y el Prototipo II-E con una clave de 256 bits se visualizan sus resultados en las Figuras siguientes:

Prototipo I-E

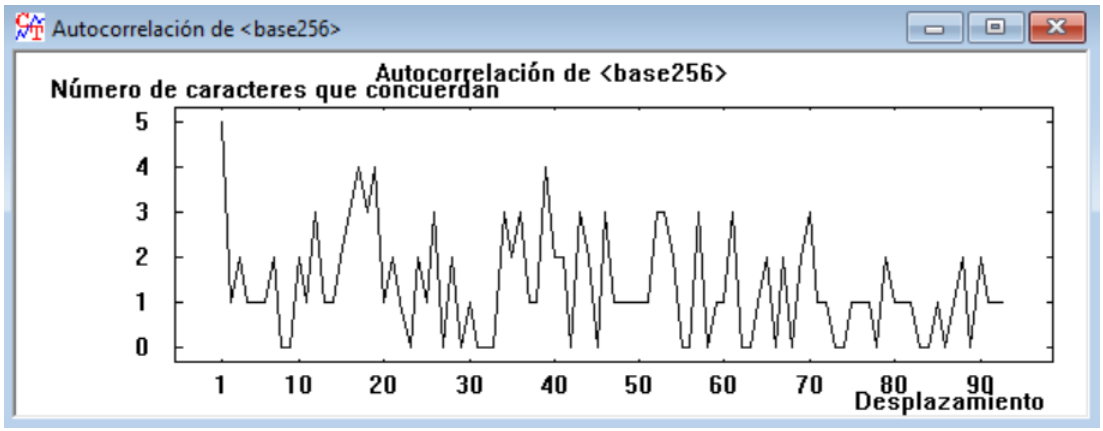


Figura 39-4: Autocorrelación con el Prototipo I-E, 256 bits
Realizado por: Cushpa Ana, 2018

Con la clave de 256 bits el mensaje cifrado por el prototipo I-E presenta un valor máximo de 5 caracteres que concuerdan con el desplazamiento de los mensajes.

Prototipo II-E

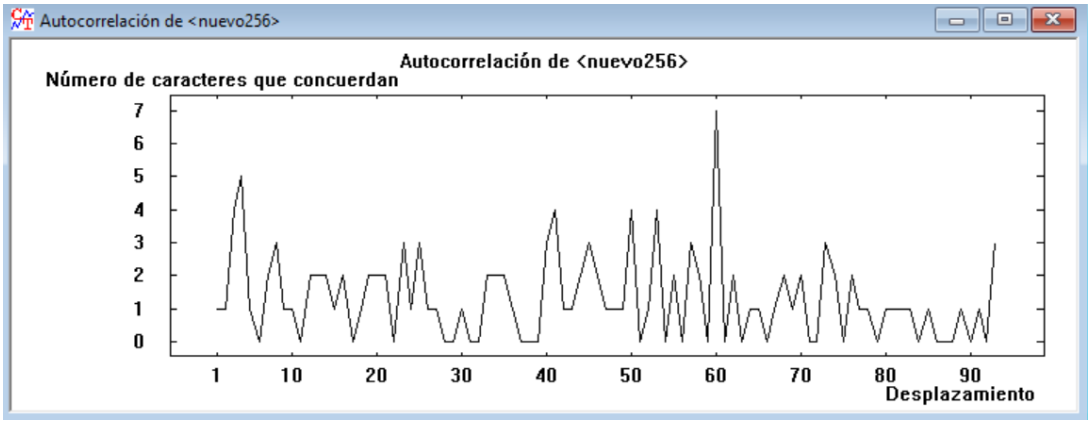


Figura 40-4: Autocorrelación con el Prototipo II-E, 256 bits
Realizado por: Cushpa Ana, 2018

Con la clave de 256 bits el mensaje cifrado por el prototipo II-E presenta un valor máximo de 6 caracteres que concuerdan con el desplazamiento de los mensajes.

El resumen de la aplicación del indicador 5 Autocorrelación en los mensajes cifrados por los Prototipos I-E y II-E se muestran en la Tabla 24-4

Tabla 24-4: Resumen del indicador 5 Autocorrelación a los Prototipos I-E y II-E

Prototipo	Caracteres que concuerdan	Tamaño clave
Prototipo I-E	6	128 bits
Prototipo II-E	6	
Prototipo I-E	6	192 bits
Prototipo II-E	5	
Prototipo I-E	5	256 bits
Prototipo II-E	7	

Realizado por: Cushpa Ana, 2018

Los valores promedios obtenidos de los resultados del indicador 5: Autocorrelación se muestran en la Tabla 25-4

Tabla 25-4: Valores promedio del indicador 5 Autocorrelación

No.	Indicador	Prototipo I-E	Prototipo II-E
5	Autocorrelación	5,66	6

Realizado por: Cushpa Ana, 2018

Los valores obtenidos del indicador 5: Autocorrelación se muestra en la Figura 41-4

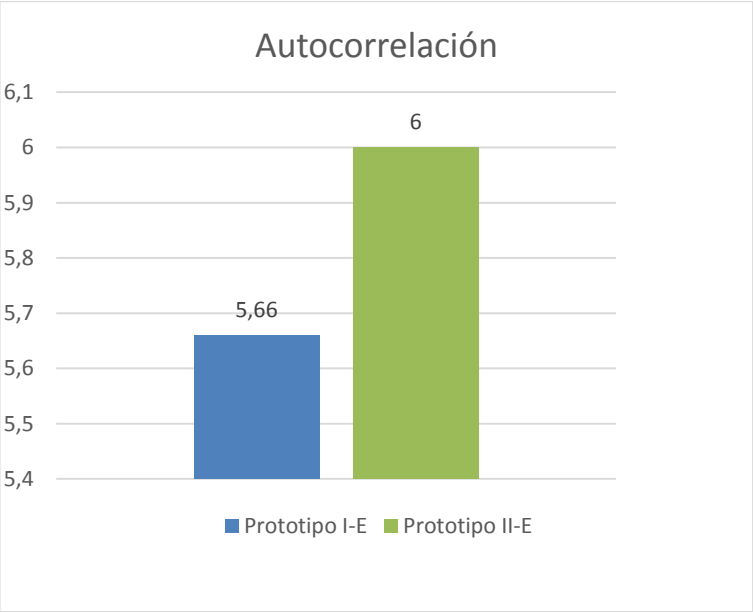


Figura 41-4: Valor promedio Indicador 5: Autocorrelación Prototipo I-E y II-E
Realizado por: Cushpa Ana, 2018

El valor promedio del indicador 5: Autocorrelación que presenta el prototipo II-E es de 6 caracteres que concuerdan con el deslazamiento de los mensajes, siendo mayor que el valor de 5.66 que presenta el prototipo I-E, aportando de esta forma el prototipo II-E a un texto cifrado con mayor difusión.

4.3.1.2.2.4. Indicador 6: Análisis de Fuerza Bruta

En las pruebas de fuerza bruta se realiza todas las posibles combinaciones con la clave para descifrar el mensaje que ha sido cifrados por los Prototipos I-E y II-E.

Para que la herramienta cryptool genere todas las combinaciones posibles, es preciso seleccionar el tamaño de la clave (128, 192, 256 bits) así como también el patrón o en su lugar usar comodines (*), como se muestra en la Figura 42-4.

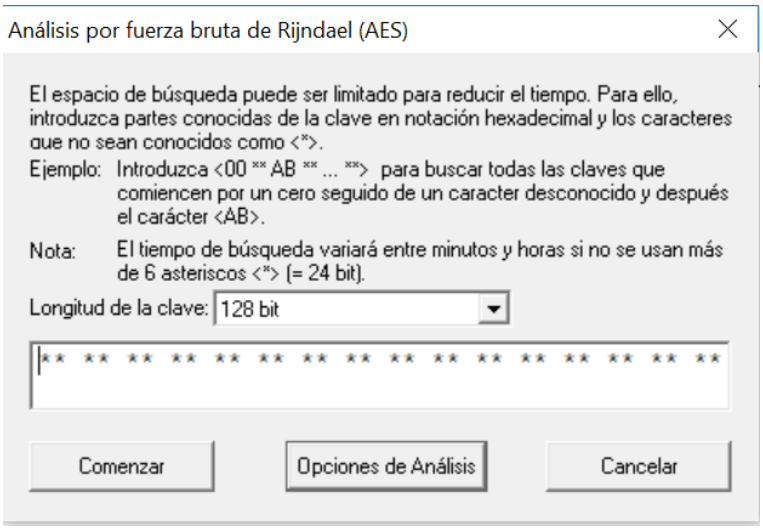


Figura 42-4: Valor promedio Indicador 6: Interfaz para determinar la clave por Fuerza bruta
Realizado por: Cushpa Ana, 2018

4.3.1.2.2.4.1. Clave de 128 bits

Las pruebas se realizan con los mensajes cifrados por los prototipos I-E y II-E, en este caso con las pruebas de 128 bits para determinar todas las combinaciones posibles. Los resultados se muestran en las Figuras 43-4 y 44-4.

Prototipo I-E

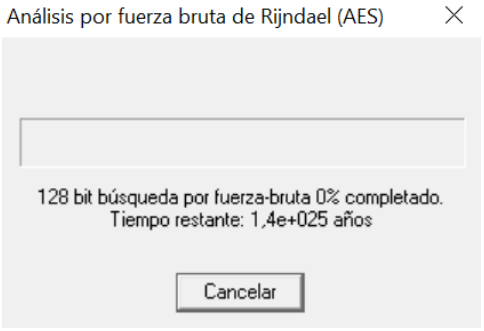


Figura 43-4: Análisis de fuerza bruta, prototipo I-E, 128 btis
Realizado por: Cushpa Ana, 2018

Prototipo II-E

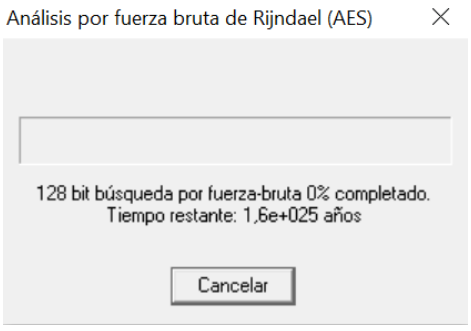


Figura 44-4: Análisis de fuerza bruta, prototipo II-E, 128 btis
Realizado por: Cushpa Ana, 2018

En el prototipo II-E se muestra un tiempo de 1.6e+025 años necesarios para determinar las combinaciones posibles en el descifrado del mensaje con una clave de 128 bits que es mayor al valor que muestra el prototipo I-E de 1.4+025 años.

4.3.1.2.2.4.2. Clave de 192 bits

Las pruebas se realizan con los mensajes cifrados por los prototipos I-E y II-E, en este caso con las pruebas de 192 bits para determinar todas las combinaciones posibles. Los resultados se muestran en las Figuras 45-4 y 46-4.

Prototipo I-E

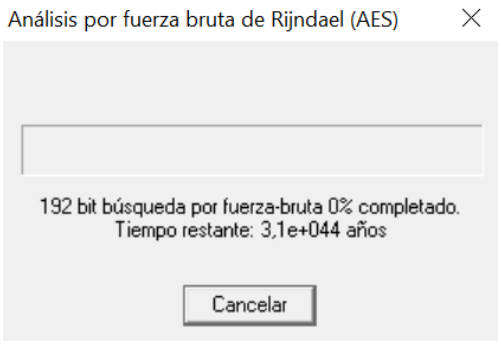


Figura 45-4: Análisis de fuerza bruta, prototipo I-E, 192 btis
Realizado por: Cushpa Ana, 2018

Prototipo II-E

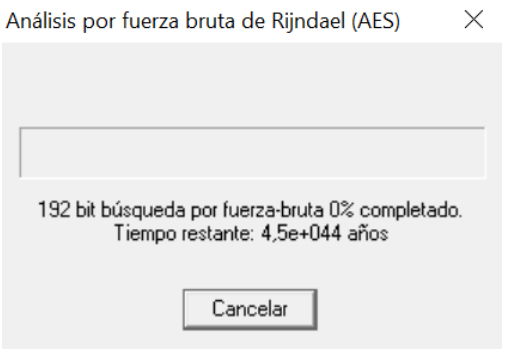


Figura 46-4: Análisis de fuerza bruta, prototipo II-E, 192 btis
Realizado por: Cushpa Ana, 2018

En el prototipo II-E se muestra un tiempo de 4.5e+044 años necesarios para determinar las combinaciones posibles en el descifrado del mensaje con una clave de 192 bits que es mayor al valor que muestra el prototipo I-E de 3.1+044 años.

4.3.1.2.2.4.3. Clave de 256 bits

Las pruebas se realizan con los mensajes cifrados por los prototipos I-E y II-E, en este caso con las pruebas de 256 bits para determinar todas las combinaciones posibles. Los resultados se muestran en las Figuras 47-4 y 48-4.

Prototipo I-E

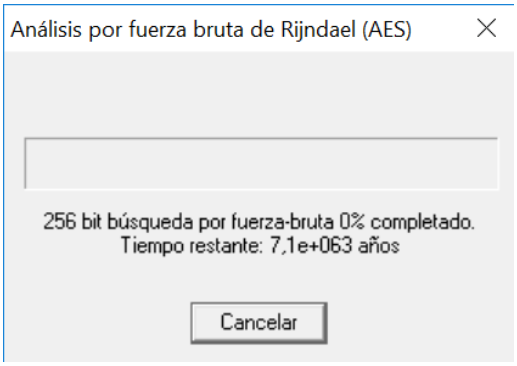


Figura 47-4: Análisis de fuerza bruta, prototipo I-E, 256 btis
Realizado por: Cushpa Ana, 2018

Prototipo II-E

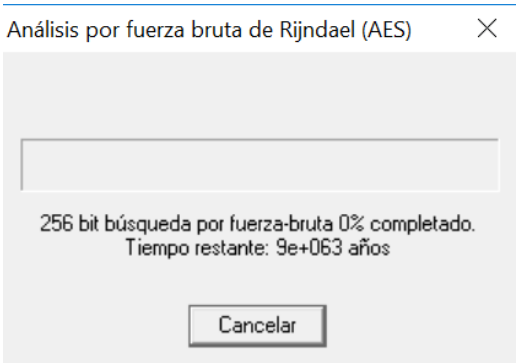


Figura 48-4: Análisis de fuerza bruta, prototipo II-E, 256 btis
Realizado por: Cushpa Ana, 2018

En el prototipo II-E se muestra un tiempo de 9e+063 años necesarios para determinar las combinaciones posibles en el descifrado del mensaje con una clave de 256 bits que es mayor al valor que muestra el prototipo I-E de 7.1+063 años.

Los resultados del análisis de fuerza bruta aplicados a los textos cifrados por los prototipos I–E y II-E se muestran en la Tabla 26-4

Tabla 26-4: Resumen del Análisis de Fuerza bruta a los Prototipos I-E y II-E

Prototipo	Tiempo estimado para descifrar (años)	Tamaño clave
Prototipo I-E	$1,4 \times 10^{25}$	128 bits
Prototipo II-E	$1,6 \times 10^{25}$	
Prototipo I-E	$3,1 \times 10^{44}$	192 bits
Prototipo II-E	$4,5 \times 10^{44}$	
Prototipo I-E	$7,10 \times 10^{63}$	256 bits
Prototipo II-E	9×10^{63}	

Realizado por: Cushpa Ana, 2018

Los valores promedios de los resultados obtenidos con la aplicación del indicador 6 Análisis de Fuerza bruta se muestran en la Tabla 27-4

Tabla 27-4: Valores promedio del indicador 6 Análisis de Fuerza bruta

No.	Indicador	Prototipo I-E	Prototipo II-E
6	Fuerza bruta	2.36×10^{63}	3.0015×10^{63}

Realizado por: Cushpa Ana, 2018

Los valores obtenidos del indicador 6 Análisis de Fuerza bruta muestra en la Figura 49-4

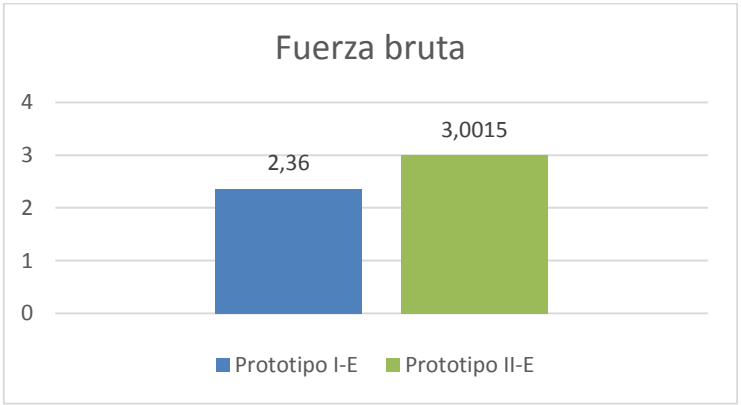


Figura 49-4: Valor promedio Indicador 6: Análisis de Fuerza Bruta: Prototipo I-E y II-E

Realizado por: Cushpa Ana, 2018

El tiempo promedio en el prototipo II-E es de 3.0015e+063 años necesarios para determinar las combinaciones posibles en el descifrado del mensaje que es mayor al valor que muestra el prototipo I-E de 2.36+063 años, permitiendo una mayor seguridad de la información.

4.3.2. Definición de escalas de calificación

Para realizar la comparación de los resultados se empleará la escala de Likert a cada uno de los indicadores seleccionados.

4.3.2.1. Indicador 1: N° de Funciones utilizadas

La escala que se emplea para evaluar el indicador No 1 se muestra en la Tabla 28-4

Tabla 28-4: Escala para medir Indicador No.1: No. de funciones

No. de funciones utilizadas	Código de escala
>= 7	4
5…6	3
3…4	2
< 3	1

Realizado por: Cushpa Ana, 2018

La escala se especifica acorde a la relación directamente proporcional entre la seguridad y el número de funciones que usa el algoritmo porque a mayor número de funciones mayor será la seguridad pues el mensaje será más difuso.

4.3.2.2. Indicador 2: N° de rondas

La escala que se emplea para evaluar el indicador No 2 se muestra en la Tabla 29-4

Tabla 29-4: Escala para medir Indicador No.2: Número de rondas

No. de rondas	Código de escala
> = 18	4
13..17	3
8…12	2
< 7	1

Realizado por: Cushpa Ana, 2018

La escala se especifica acorde a la relación directamente proporcional entre la seguridad y el número de rondas ejecutadas por el algoritmo porque a mayor número de rondas mayor será la seguridad pues el mensaje será más difuso.

4.3.2.3. Indicador 3: Entropía

La escala que se emplea para evaluar el indicador No 3: Entropía se muestra en la Tabla 30-4

Tabla 30-4: Escala para medir Indicador No.3: Entropía

Entropía	Código de escala
> = 6,22	4
5,61…6,21	3
5,01…5,60	2
< = 5,00	1

Realizado por: Cushpa Ana, 2018

La escala se especifica acorde a la relación directamente proporcional entre la seguridad y el nivel de entropía, porque a mayor entropía mayor será la seguridad pues el mensaje será más incomprensible.

4.3.2.4. Indicador 4: Histograma

La escala que se emplea para evaluar el indicador No 4: Histograma se muestra en la Tabla 31-4

Tabla 31-4: Escala para medir Indicador No. 4: Histograma

No. de caracteres	Código de escala
> = 185	4
125…184	3
65…124	2
< 65	1

Realizado por: Cushpa Ana, 2018

La escala se especifica acorde a la relación directamente proporcional entre la seguridad y el número de caracteres que utiliza el algoritmo porque a mayor número de caracteres mayor será la seguridad pues el mensaje será más difuso.

4.3.2.5. Indicador 5: Autocorrelación

La escala que se emplea para evaluar el indicador No 4: Autocorrelación se muestra en la Tabla 32-4

Tabla 32-4: Escala para medir Indicador No. 5: Autocorrelación

No. de caracteres que concuerdan	Código de escala
> = 6,00	4
4,00…5,99	3
2,00 …3,99	2
< 1,99	1

Realizado por: Cushpa Ana, 2018

La escala se especifica acorde a la relación directamente proporcional entre la seguridad y el número de caracteres que concuerdan porque si mayor es el número de caracteres que concuerdan mayor será la seguridad pues será más arduo el trabajo de descifrarlo.

4.3.2.6. Indicador 6: Análisis de Fuerza bruta

La escala que se emplea para evaluar el indicador No 6: Fuerza bruta se muestra en la Tabla 33-4

Tabla 33-4: Escala para medir Indicador No. 6: Fuerza bruta

Tiempo requerido para descifrar (años)	Código de escala
> = $3x10^{63}$	4
$2,50x10^{63}$…$2,99x\ 10^{63}$	3
$2x10^{63}$…$2,49x10^{63}$	2
< $2x10^{63}$	1

Realizado por: Cushpa Ana, 2018

La escala se especifica acorde a la relación directamente proporcional entre la seguridad y el tiempo que se demore en encontrar todas las combinaciones posibles para descifrar el mensaje porque a mayor tiempo que se tarde en descifrar mayor será la seguridad pues el mensaje será más indescifrable.

4.3.3. Ponderación de indicadores

Los datos promedios obtenidos en el punto 4.3.1 con cada indicador serán cuantificados con las escalas definidas.

4.3.3.1. Indicador 1: No. de Funciones utilizadas

Con las escalas definidas se pondera los datos promedio del Indicador 1: Numero de funciones usadas por los algoritmos implementados en el Prototipo I-E y Prototipo II-E. Los valores que se obtienen se muestran en la Tabla 34-4.

Tabla 34-4: Aplicación de escala al Indicador 1: No. de funciones usadas

No.	Indicador	Promedio		Código según la escala	
		Prototipo I-E	Prototipo II-E	Prototipo I-E	Prototipo II-E
1	No. de funciones usadas por el algoritmo	4	5	2	3

Realizado por: Cushpa Ana, 2018

Los resultados obtenidos con la aplicación de los códigos de la escala se muestran en la Figura 50-4

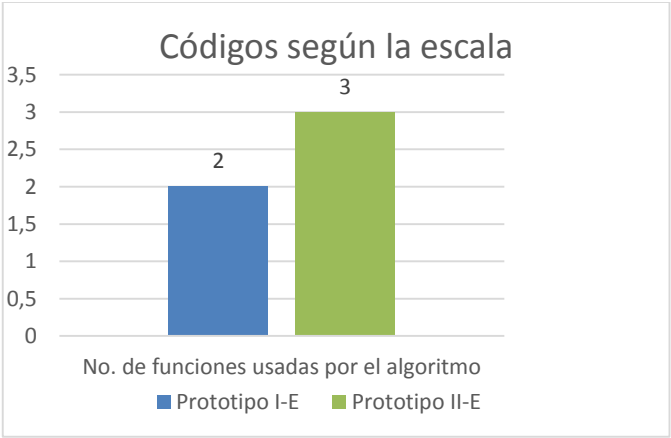


Figura 50-4: Resultados indicador 1: No. de funciones usadas por el algoritmo, según la escala

Realizado por: Cushpa Ana, 2018

De acuerdo a los valores obtenidos el Prototipo II-E obtiene un código de 3 porque utiliza 5 funciones con el incremento de la función *mixDiagonal*, contribuyendo a una mayor difusión de los mensajes y el Prototipo I-E obtiene un código de 2.

4.3.3.2. Indicador 2: No. de rondas

De acuerdo a las escalas definidas se pondera los datos promedio del Indicador 2: Numero de rondas utilizadas por los algoritmos implementados en el Prototipo I-E y Prototipo II-E. Los valores que se obtienen se muestran en la Tabla 35-4.

Tabla 35-4: Aplicación de escala al Indicador 2: No. de rondas

No.	Indicador	Promedio		Código según la escala	
		Prototipo I-E	Prototipo II-E	Prototipo I-E	Prototipo II-E
2	No. de rondas	12	18	2	4

Realizado por: Cushpa Ana, 2018

De la aplicación de los códigos de la escala se obtienen los datos que se muestran en la Figura 51-4

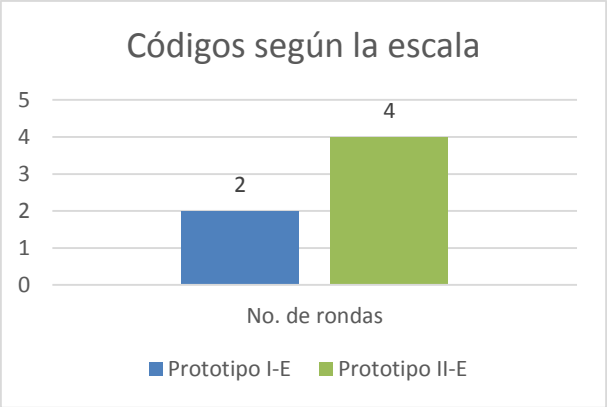


Figura 51-4: Resultados indicador 2: No. de rondas, según la escala
Realizado por: Cushpa Ana, 2018

El Prototipo I-E obtiene un código de 2 debido a que utiliza 10 rondas (128 bits), 12 rondas (192 bits) y 14 rondas (256 bits) mientras que el Prototipo II–E utiliza 15 rondas (128 bist), 18 rondas (128 bits) y 21 rondas (256 bits) por lo que obtiene el código de 4, logrando así mensajes más difusos.

4.3.3.3. Indicador 3: Entropía

Con las escalas definidas se pondera los datos promedio del Indicador 3: Entropía generada por los algoritmos implementados en el Prototipo I-E y Prototipo II-E. Los valores que se obtienen se muestran en la Tabla 36-4.

Tabla 36-4: Aplicación de escala al Indicador 3: Entropía

No.	Indicador	Promedio		Código según la escala	
		Prototipo I-E	Prototipo II-E	Prototipo I-E	Prototipo II-E
3	Entropía	6,12	6,24	3	4

Realizado por: Cushpa Ana, 2018

Los resultados obtenidos con la aplicación de los códigos de la escala se muestran en la Figura 52-4

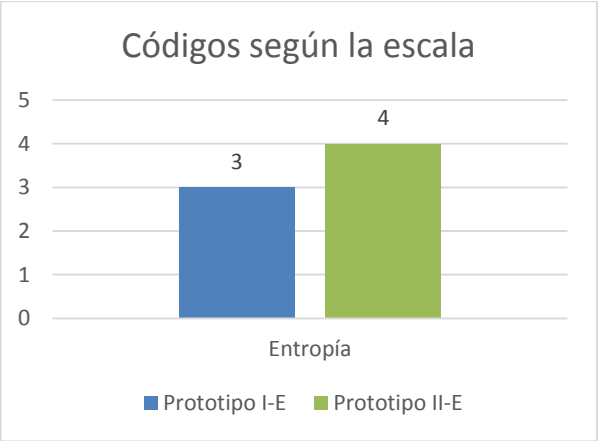


Figura 52-4: Resultados indicador 3: Entropía, según la escala
Realizado por: Cushpa Ana, 2018

El prototipo I-E obtiene un código de 3 ya que tiene un valor de entropía de 6,12 con respecto a la entropía máxima (6,61), al compararlo con el prototipo II-E que tiene un valor de entropía de 6,24 por lo cual obtiene un código de 4, contribuyendo a una mayor difusión de los mensajes.

4.3.3.4. Indicador 4: Histograma

De acuerdo con las escalas definidas se pondera los datos promedio del Indicador 4: Histograma generado por los algoritmos implementados en el Prototipo I-E y Prototipo II-E. Los valores que se obtienen se muestran en la Tabla 37-4.

Tabla 37-4: Aplicación de escala al Indicador 4: Histograma

No.	Indicador	Promedio		Código según la escala	
		Prototipo I-E	Prototipo II-E	Prototipo I-E	Prototipo II-E
4	Histograma	181,6	196,3	3	4

Realizado por: Cushpa Ana, 2018

De la aplicación de los códigos de la escala se obtienen los datos que se muestran en la Figura 53-4

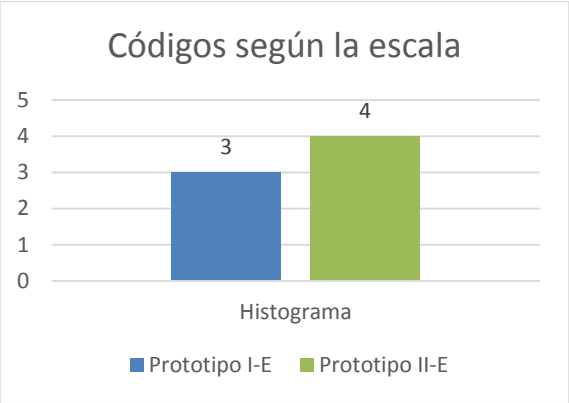


Figura 53-4: Resultados indicador 4: Histograma, según la escala
Realizado por: Cushpa Ana, 2018

Con el prototipo II-E se obtiene mayor cantidad promedio de caracteres por lo que consigue el código 4, mientras que con el prototipo I-E se consigue un código de 3, haciendo que con el Prototipo II se obtengan mensajes más difusos.

4.3.3.5. Indicador 5: Autocorrelación

Con las escalas definidas se cuantifica los datos promedio del Indicador 5: Autocorrelación generado por los algoritmos implementados en el Prototipo I-E y Prototipo II-E. Los valores que se obtienen se muestran en la Tabla 38-4.

Tabla 38-4: Aplicación de escala al Indicador 5: Autocorrelación

No.	Indicador	Promedio		Código según la escala	
		Prototipo I-E	Prototipo II-E	Prototipo I-E	Prototipo II-E
5	Autocorrelación	5,66	6	3	4

Realizado por: Cushpa Ana, 2018

Los resultados obtenidos con la aplicación de los códigos de la escala se muestran en la Figura 54-4

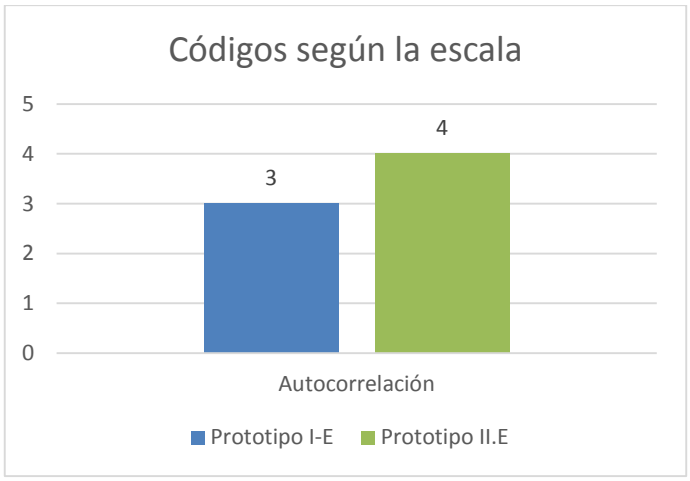


Figura 54-4: Resultados indicador 5: Autocorrelación, según la escala
Realizado por: Cushpa Ana, 2018

Con el prototipo II-E se obtiene un código de 4 ya que tiene un mayor número de caracteres que concuerdan, mientras que con el prototipo I-E se tiene un menor número de caracteres que coincidan por lo que se obtiene un código de 3.

4.3.3.6. Indicador 6: Análisis de Fuerza bruta

De acuerdo a las escalas definidas se cuantifica los datos promedio del Indicador 6: Fuerza bruta generada por los algoritmos implementados en el Prototipo I-E y Prototipo II-E. Los valores que se obtienen se muestran en la Tabla 39-4.

Tabla 39-4: Aplicación de escala al Indicador 6: Fuerza bruta

No.	Indicador	Promedio		Código según la escala	
		Prototipo I-E	Prototipo II-E	Prototipo I-E	Prototipo II-E
6	Fuerza bruta	2.36×10^{63}	3.0015×10^{63}	2	4

Realizado por: Cushpa Ana, 2018

Luego de aplicar los códigos de la escala al indicador 6 se obtienen los datos que se muestran en la Figura 55-4

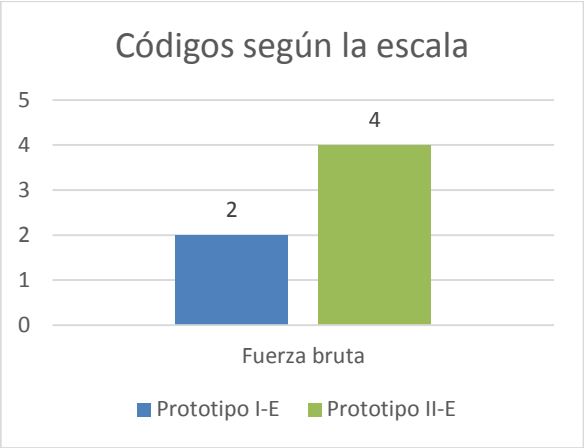


Figura 55-4: Resultados indicador 6: Fuerza bruta según la escala
Realizado por: Cushpa Ana, 2018

Con el Prototipo II-E los mensajes cifrados necesitan mayor tiempo para ser descifrados para ser comprendidos por fuerza bruta por lo que obtiene un código de 4, mientras con el prototipo I-E el tiempo es menor y obtiene un código de 2.

4.3.4. Comprobación de la hipótesis

En la presente investigación se define la hipótesis:

La implementación de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en un entorno web mejorará el nivel de seguridad de la información.

En la comprobación de la hipótesis se maneja la estadística descriptiva y también la estadística diferencial.

4.3.4.1. Estadística descriptiva

La estadística descriptiva permite cuantificar los valores adquiridos en las pruebas que se han realizado con los indicadores que servirá para la comprobación de la hipótesis. La Tabla 40-4 muestra los resultados de los indicadores.

Tabla 40-4: Resultados de los indicadores

No.	Indicadores	Prototipo I-E	Prototipo II-E
1	No. de funciones utilizadas por el algoritmo	2	3
2	No. de rondas	2	4
3	Entropía	3	4
4	Histograma	3	4
5	Autocorrelación	3	4
6	Fuerza bruta	2	4
	TOTAL	**15**	**23**

Realizado por: Cushpa Ana, 2018

A continuación, la Figura 56-4 muestra los resultados que se obtienen de comparar todos los indicadores aplicados a los prototipos I y II.

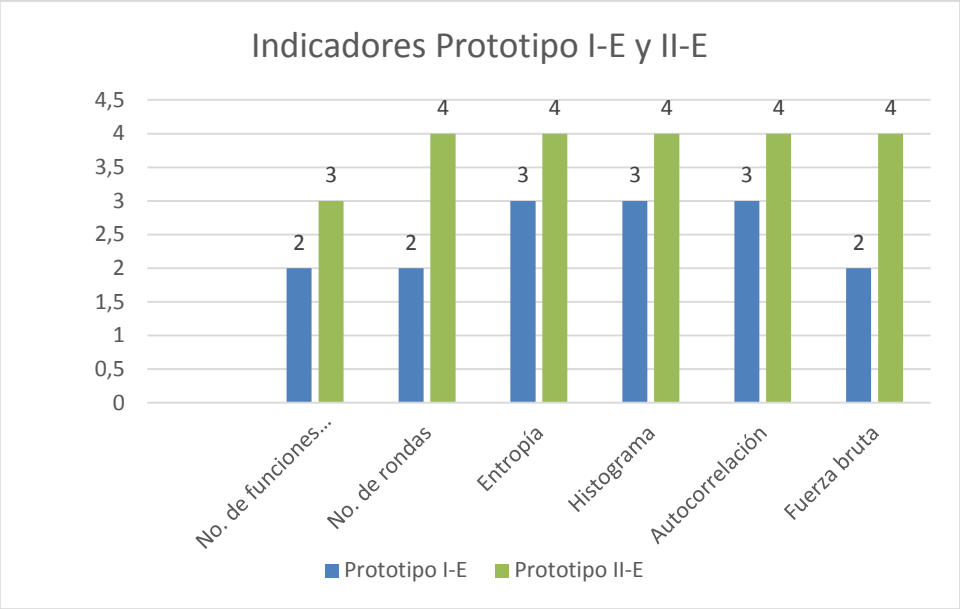


Figura 56-4: Resultados de la comparación de indicadores
Realizado por: Cushpa Ana, 2018

Para verificar los resultados totales de la comparación realizada al Prototipo I-E y Prototipo II-E se muestra la Figura 57-4

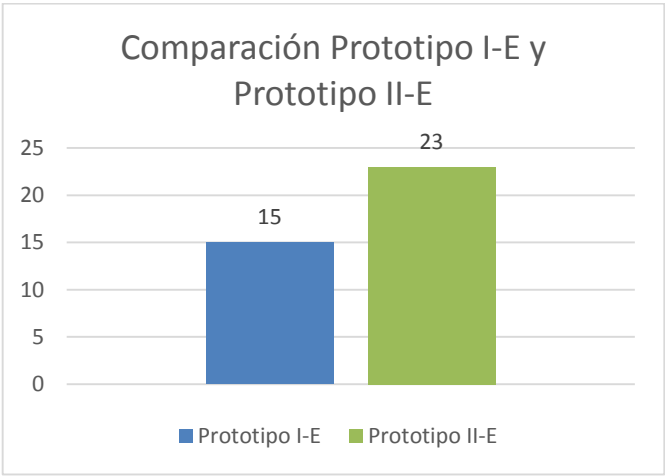


Figura 57-4: Resultados totales de la comparación de indicadores
Realizado por: Cushpa Ana, 2018

De los resultados obtenidos se concluye que el Prototipo II-E es más seguro en el cifrado de los mensajes en un 53% al compararlo con el cifrado de mensajes del Prototipo I-E.

4.3.4.2. Estadística inferencial

En la demostración de la hipótesis de la presente investigación la variable independiente denominada con *X* toma los siguientes valores:

X= seguridad

X_1 = Mejora el nivel seguridad

X_2 = No mejora el nivel de seguridad

En la variable dependiente se considera a los algoritmos criptográficos que han sido implementados en el Prototipo I y II.

En la comprobación de la

hipótesis se emplea la prueba estadística Chi cuadrado, por ser un método no paramétrico muy útil para evaluar la relación entre la variable dependiente e independiente y contrastar las frecuencias observadas con las frecuencias esperadas de acuerdo con una hipótesis nula (H_0) y la hipótesis de la investigación (H_i) que son:

- **H_i:** La implementación del nuevo algoritmo criptográfico para mensajería instantánea en un entorno web *mejora el nivel de seguridad* de la información con respecto al algoritmo criptográfico base.
- **H_0:** La implementación del nuevo algoritmo criptográfico para mensajería instantánea en un entorno web *no mejora el nivel de seguridad* de la información con respecto al algoritmo criptográfico base.

En la Tabla 41-4 se muestra la tabla de contingencia que se ha creado para realizar el cálculo de Chi cuadrado con las frecuencias observadas con cada indicador.

Tabla 41-4: Tabla de contingencia de las frecuencias observadas

V. Independiente / V. Dependiente	**Indicadores**	**Prototipo I-E**	**Prototipo II-E**
Mejora el nivel de seguridad	No. de funciones utilizadas por el algoritmo	0	3
	No. rondas	0	4
	Entropía	0	4
	Histograma	0	4
	Autocorrelación	0	4
	Fuerza bruta	0	4
No mejora el nivel de seguridad	No. funciones utilizadas por el algoritmo	2	0
	No. rondas	2	0
	Entropía	3	0
	Histograma	3	0
	Autocorrelación	3	0
	Fuerza bruta	2	0
	TOTAL	**15**	**23**

Realizado por: Cushpa Ana, 2018

Los valores presentados en la tabla de contingencia de frecuencias esperadas son los que se esperaría encontrar si las variables no estuvieran relacionadas. La prueba Chi cuadrado parte del supuesto "no relación entre variables"

La siguiente fórmula se aplica a cada una de las celdas de las frecuencias observadas para calcular las frecuencias esperadas:

$$fe = \frac{(total\_fila) * (total\_columna)}{N}$$

Donde:

N: Número total de frecuencias observadas.

Luego de aplicar la fórmula a cada uno de los datos de la Tabla 41-4 se consigue la tabla de contingencia de los valores esperados, como muestra la Tabla 42-4.

Tabla 42-4: Tabla de contingencia de frecuencias esperadas

V. Dependiente / **V. Independiente**	**Indicadores**	**Prototipo I-E**	**Prototipo II-E**
Mejora el nivel de seguridad	No. funciones utilizadas por el algoritmo	1.18	1.82
	No. de rondas	1.58	2.42
	Entropía	1.58	2.42
	Histograma	1.58	2.42
	Autocorrelación	1.58	2.42
	Fuerza bruta	1.58	2.42
No mejora el nivel de seguridad	No. funciones utilizadas por el algoritmo	0.79	1.21
	No. de rondas	0.79	1.21
	Entropía	1.18	1.82
	Histograma	1.18	1.82
	Autocorrelación	1.18	1.82
	Fuerza bruta	0.79	1.21
	TOTAL	**15**	**23**

Realizado por: Cushpa Ana, 2018

Luego de obtener la tabla de frecuencias esperadas, se emplea la siguiente fórmula de chi cuadrado.

$$X^2 = \sum \frac{(o - E)^2}{E}$$

Donde:

O: Frecuencia observada en cada celda

E: Frecuencia esperada en cada celda

La Tabla 43-4 muestra el cálculo de X^2

Tabla 43-4: Cálculo de X^2

	Indicadores	**O**	**E**	**O - E**	**(O - E)²**	$\frac{(O-E)^2}{E}$
Prototipo I-E	Mejora/ No. funciones utilizadas por el algoritmo	0	1.18	-1.18	1.39	1.18
	Mejora/No. rondas	0	1.58	-1.58	2.50	1.58
	Mejora/ Entropía	0	1.58	-1.58	2.50	1.58
	Mejora/ Histograma	0	1.58	-1.58	2.50	1.58
	Mejora/ Autocorrelación	0	1.58	-1.58	2.50	1.58
	Mejora/ Fuerza bruta	0	1.58	-1.58	2.50	1.58
Prototipo II-E	Mejora/ No. funciones utilizadas por el algoritmo	3	1.82	1.18	1.39	0.77
	Mejora/No. rondas	4	2.42	1.58	2.50	1.03
	Mejora/ Entropía	4	2.42	1.58	2.50	1.03
	Mejora/ Histograma	4	2.42	1.58	2.50	1.03
	Mejora/ Autocorrelación	4	2.42	1.58	2.50	1.03
	Mejora/ Fuerza bruta	4	2.42	1.58	2.50	1.03
Prototipo I-E	No mejora/No. funciones utilizadas por el algoritmo	2	0.79	1.21	1.46	1.85
	No mejoras/ No. rondas	2	0.79	1.21	1.46	1.85
	No mejoras/ Entropía	3	1.18	1.82	3.31	2.81
	No mejoras/ Histograma	3	1.18	1.82	3.31	2.81
	No mejoras/ Autocorrelación	3	1.18	1.82	3.31	2.81
	No mejoras/ Fuerza bruta Prototipo I	2	0.79	1.21	1.46	1.85
Prototipo II-E	No mejoras/ No. funciones utilizadas por el algoritmo	0	1.21	-1.21	1.46	1.21
	No mejoras/ No. rondas	0	1.21	-1.21	1.46	1.21
	No mejoras/ Entropía	0	1.82	-1.82	3.31	1.82
	No mejoras/ Histograma	0	1.82	-1.82	3.31	1.82
	No mejoras/ Autocorrelación	0	1.82	-1.82	3.31	1.82
	No mejoras/ Fuerza bruta	0	1.21	-1.21	1.46	1.21
	X^2					**38.07**

Realizado por: Cushpa Ana, 2018

Para establecer si el valor de X^2 es o no significativo, debemos establecer los grados de libertad con la formula siguiente:

$$GI = (f - 1)(c - 1)$$

Donde:

$\boldsymbol{f}$: Número de filas de la tabla de contingencia

$\boldsymbol{c}$: Número de columnas de la tabla de contingencia

Entonces:

$$GI = (12 - 1)(2 - 1) = 11$$

Conforme a la tabla de distribución X^2 que muestra la Tabla 44-4, en base al resultado obtenido se determina que el nivel de significancia de $\propto = 0.1\% = 0.001$ para obtener un nivel de confianza de 99.9%, se tiene como punto crítico de X^2 para 11 grados de libertad $X^2_{critico}$= 31.2635.

Tabla 44-4: Tabla de distribución de X^2

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Fuente: http://labrad.fisica.edu.uy/docs/tabla_chi_cuadrado.pdf

En la presente investigación el valor de $X^2_{calculado}$ es igual a 38.07 que es superior al valor mostrado en la tabla de distribución de 31.2635, que se muestra la Figura 58-4.

$X^2_{Crítico}$ (31.2635) < $X^2_{Calculado}$ (38.07)

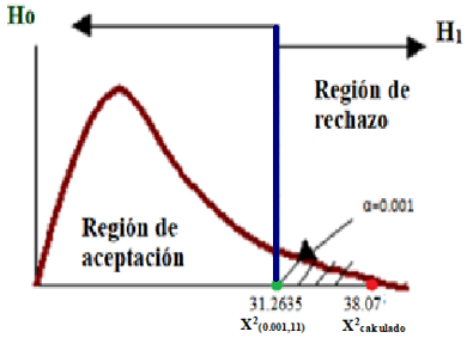


Figura 58-4: Curva de X^2
Realizado por: Cushpa Ana, 2018

De acuerdo al gráfico el valor calculado de X^2 está dentro del sector de rechazo de la hipótesis nula H_o, por lo que se acepta la hipótesis de la investigación que es significativa, con un nivel de significancia de α= 0.001 para alcanzar un nivel de confianza del 99.9%, por lo que: **la implementación del nuevo algoritmo criptográfico para mensajería instantánea en un entorno web *mejoró el nivel de seguridad* de la información con respecto al algoritmo criptográfico base.**

CONCLUSIONES

- Del análisis de algoritmos criptográficos se determinó el algoritmo AES como base para el desarrollo del nuevo algoritmo criptográfico debido a sus ventajas en la resistencia a criptoanálisis y contra fuerza bruta, además permite la utilización de claves de longitud de 128bits, 192 bits y 256 bits así como también tamaños de bloque variable.

- La incorporación de la función propuesta denominada MixDiagonal dentro de las rondas ejecutadas por el algoritmo y el incremento del número de rondas, el mensaje se tornó más difuso, logrando de esta forma mayor seguridad en comparación con el algoritmo AES base.

- Las 384 pruebas realizadas con los mensajes cifrados por los prototipos I-E y II-E permitieron validar la utilización del nuevo algoritmo en la implementación del chat web con un valor promedio de entropía de 6.11 mientras que el algoritmo AES base presentó un valor promedio de entropía de 6.06.

- Para la implementación de la mensajería instantánea en los prototipos web I y II se utilizó la herramienta de desarrollo Netbeans y PostgreSQL para la gestión de la base de datos: las mismas que son herramientas open source que brindan facilidades para el desarrollo de las aplicaciones web.

- En el análisis de las características, el nuevo algoritmo presenta un mayor número de rondas y de funciones utilizadas en comparación con el algoritmo AES base seleccionado.

- En la herramienta Cryptool se desarrollaron las pruebas de criptoanálisis para los indicadores de: entropía, autocorrelación, histograma y fuerza bruta en base a los que se determinó que el nuevo algoritmo propuesto incrementa el nivel de seguridad frente al algoritmo AES base.

- Con la estadística descriptiva y la utilización de las escalas de Likert se demostró que el prototipo II-E presenta mensajes cifrados más seguros en un 53% que el prototipo I-E.

- Con la estadística inferencial y la utilización de chi-cuadrado con α= 0,001 como nivel de significancia, en la tabla de distribución X^2 =31,2635 se consigue un valor calculado de X^2 =38,07 superior al valor que presenta la tabla de la distribución, por lo tanto, está

dentro del sector de rechazo de la hipótesis nula H_0 y consecuentemente de forma estadística es aceptable la hipótesis de investigación.

RECOMENDACIONES

- El algoritmo AES base, utiliza tamaños de bloque variable, claves de tamaño variable y ofrece mayor seguridad frente a criptoanálisis y contra ataques de fuerza bruta por lo que es recomendable su aplicación en el cifrado de datos.

- Se recomienda comprender el funcionamiento del algoritmo para determinar las posibles modificaciones que contribuyan a una mayor difusión del mensaje y mejora de la seguridad.

- Es importante determinar los escenarios de prueba donde los indicadores que se van a medir sean claramente visualizados para obtener los resultados que ayuden a definir las diferencias entre los prototipos.

- Cryptool es una herramienta muy recomendable para analizar y determinar la difusión del mensaje ofreciendo varias alternativas en cuanto a indicadores a medir.

- La modificación de las funciones que ejecuta el algoritmo o el incremento de nuevas funciones que ayuden a difuminar más el mensaje con la clave de cifrado ayuda a que el mensaje se torne más incomprensible y por lo tanto sea difícil descifrarlo por personas no autorizadas para obtener el mensaje.

- La mensajería instantánea es una aplicación muy útil en la actualidad por lo que se recomienda implementar el algoritmo propuesto en aplicaciones para dispositivos móviles.

BIBLIOGRAFÍA

AGUIRRE, J. (2006). *Seguridad Informática y criptografía.* Obtenido de http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion1.html

AGUIRRE, J. (2006). *Teoría de la complejidad algorítmica.* Obtenido de http://www.it-docs.net/ddata/3954.pdf

BLANCO, R. (2010). *Análisis de algoritmos criptográficos y su aplicación al cifrado de archivos.* Mexico: http://tesis.ipn.mx/bitstream/handle/123456789/6239/IF2.45.pdf?sequence=1.

BONILLA, E. (2012). *Implementación del algoritmo AES sobre arquitectura ARM con mejora en rendimiento y seguridad.* Madrid: https://orff.uc3m.es/bitstream/handle/10016/15402/pfc_eduardo_bonilla_palencia_2012.pdf;jsessionid=DDBC9674D3C4589F8C73F5305C51FFF8?sequence=2.

CASAS, O. (2010). *Implementación de los cifradores de bloque Rijndael, Serpent, MARS, Twofish y RC6 para su uso en sistemas embebidos.* Cali.

CASTANEDO, M. (2007). *e - reding*. Obtenido de http://bibing.us.es/proyectos/abreproy/11314/fichero/MEMORIA_FIRMA_DIGITAL_XML%252FCap%C3%ADtulo+6+Cifrado.pdf+

CASTRO, M. (2008). Plataforma tecnológica.

COMUNIDAD ECURED. (2016). *Comunidad EcuRed.* Obtenido de https://www.ecured.cu/Criptograf%C3%ADa_asim%C3%A9trica

DE LUZ, S. (16 de 11 de 2010). *Redes Zone*. Obtenido de https://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/

ECURED. (2014). *Comunidad EcuRed.* Obtenido de https://www.ecured.cu/PostGreSQL

ESPAÑOLA, R. A. (05 de 03 de 2016). *http://www.rediris.es/cert/doc/unixsec/node29.html.*

ESSLINGE, B. (2014). *ACADEMIC*. Obtenido de http://www.esacademic.com/dic.nsf/eswiki/315878

E-VOLUTION. (2012). *ESET Informa: Estudio sobre el estado de la seguridad de la información corporativa.* Obtenido de http://e-volution.cc/2012/06/04/eset-informa-estudio-sobre-el-estado-de-la-seguridad-de-la-informacion-corporativa/comment-page-1/

FERNÁNDEZ, M. (2009). *Mensajería Instantánea en Internet.* Argentina: Argentina de Creative Commons.

GARCÍA, M. (2013). *Implementación del algoritmo de cifrado AES para bajo consumo sobre FPGA.* Madrid.

GÓMEZ, M., & CERVANTES, J. (2014). *Introducción al análisis y diseño de algoritmos.* Mexico: http://www.cua.uam.mx/pdfs/conoce/libroselec/Notas_Analisis_AlgoritmosVF.pdf.

GRANADOS P, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, ISSN: 1067-6079.

GRANADOS, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, isn: 1067-6079.

GUTIÉRREZ, J. (2009). *Las redes substituciín-permutación y el AES (Advanced encryption standard).* https://grupos.unican.es/amac/articles/aes.pdf.

IEE OCC CyberSecurity SIG. (2016). Recuperado el 23 de 03 de 2017, de http://sites.ieee.org/ocs-cssig/?page_id=476

JIMENEZ, A. (2013). *Criptografía de clave secreta.*

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

LUCENA, M. (2010). *Criptografía y seguridad en computadores.* Jaén.

MATAMALA, M. (2012). *Administración de sistemas en red*. Recuperado el 18 de 04 de 2017, de http://www.mauriciomatamala.net/SAD/criptografia.php

MATHUR, M., & KESARWANI, A. (2013). Comparison Between DES, 3DES, RC2, RC6, Blowfish and DES. *Proceding of National Conference of New Horizons in IT* (págs. 143-148). IEEE.

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

MEDINA, Y., & MIRANDA, H. (2015). Comparación de algoritmos Basados en la criptografá. *Mundo FESC*, 14-21.

MÉNDEZ, P. (2015). *Nuevo algorimo criptográfico con la incorporación de la esteganografía en imágenes.* Riobamba.

MENDOZA, G. (2014). *Herramienta de desarrollo Netbeans.* Obtenido de http://www.consultorjava.com/wp/wp-content/uploads/2015/09/herramienta_desarrollo_netbeans.pdf

NETBEANS. (20 de febrero de 2015). *NetBeansIde 8.2*. Recuperado el 18 de enero de 2017, de http://www.postgresql.org.es/

PADILLA, J. (22 de 05 de 2012). *SlideShare*. Recuperado el 15 de 04 de 2017, de SlideShare: https://es.slideshare.net/jpadillaa/criptografia-asimetrica-rsa

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

ROMERO, C., & ALVARADO, Y. (24 de 09 de 2016). *Criptografía y seguridad en M-Commerce.* Recuperado el 17 de 04 de 2017, de http://aaronbernaldezgrande.blogspot.com/2012/09/algoritmo-de-cifrado-3des.html

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

SGARRO, A. (1990). Códigos Secretos. Madrid: Ediciones pirámide.

TRAYNO, V. (2016). *Ataque diferencial mediante inyección de un error en AES-128.* Barcelona.

VALLEJOS, R. (2012). *Aprendiendo RStadistical.* Obtenido de http://www.cientec.or.cr/matematica/2012/ponenciasVIII/Jose-Andrey-Zamora.pdf

VÁZQUEZ, M. (2007). *El algoritmo criptográfico AES para protección de datos.* Madrid: https://www.iit.comillas.edu/pfc/resumenes/46ea7511774d8.pdf.

VELASCO, R. (08 de 11 de 2014). *REDES@ZONE*. Obtenido de CrypTool, herramienta para experimentar con algoritmos criptográficos: http://www.redeszone.net/2014/11/08/cryptool-herramienta-para-experimentar-con-algoritmos-criptograficos/

VIGNAGA, A., & PEROVICH, D. (2010). *Arquitecturas y tecnologías para el desarrollo de aplicaciones web.* Uruguay: http://moodle2.unid.edu.mx/dts_cursos_mdl/pos/TI/LP/AM/01/Arquitecturas_y_tecnologias_para_el_desarrollo_de_aplicaciones_web.pdf.

ANEXOS

Anexo A: Pruebas realizadas

No.	Clave	Mensaje	Entropía	
			Prototipo I	Prototipo II
1	C1	M1	6.13	6.31
2	C2	M1	6.18	6.23
3	C3	M1	6.06	6.20
4	C4	M1	6.10	6.23
5	C5	M1	6.20	6.23
6	C6	M1	6.12	6.16
7	C7	M1	6.22	6.27
8	C8	M1	6.24	6.25
9	C9	M1	6.15	6.21
10	C10	M1	6.14	6.27
11	C11	M1	6.25	6.26
12	C12	M1	6.18	6.18
13	C13	M1	6.18	6.21
14	C14	M1	6.23	6.24
15	C15	M1	6.24	6.24
16	C1	M2	5.78	5.97
17	C2	M2	5.86	5.87
18	C3	M2	5.68	5.73
19	C7	M2	6.10	6.14
20	C8	M2	6.10	6.11
21	C9	M2	6.02	6.12
22	C16	M3	6.00	6.00
23	C17	M3	6.01	6.04
24	C18	M3	6.02	6.03
25	C22	M4	6.04	6.04
26	C23	M4	6.09	6.17
27	C24	M4	6.08	6.09
28	C25	M5	6.14	6.15
29	C26	M5	5.93	6.09
30	C27	M5	6.13	6.17
31	C28	M6	6.06	6.09
32	C29	M6	5.91	5.92
33	C30	M6	6.20	6.20
34	C31	M7	5.99	6.05
35	C32	M7	6.09	6.15
36	C33	M7	6.15	6.20
37	C34	M8	6.28	6.28
38	C35	M8	6.21	6.24
39	C36	M8	6.17	6.18
40	C19	M9	6.15	6.20

41	C20	M9	6.03	6.20
42	C21	M9	6.11	6.30
43	C20	M10	6.01	6.06
44	C20	M5	6.15	6.20
45	C21	M5	6.03	6.20
46	C22	M5	6.11	6.30
47	C22	M10	6.04	6.04
48	C23	M10	6.09	6.17
49	C16	M1	5.79	5.96
50	C17	M1	5.85	5.87
51	C18	M1	5.65	5.7
52	C19	M1	6.09	6.12
53	C20	M1	6.09	6.11
54	C21	M1	6.02	6.12
55	C22	M1	6.00	6.01
56	C23	M1	6.02	6.05
57	C24	M1	6.02	6.03
58	C25	M1	6.01	6.04
59	C26	M1	6.07	6.15
60	C27	M1	6.08	6.09
61	C28	M1	6.13	6.15
62	C29	M1	5.91	6.05
63	C30	M1	6.13	6.17
64	C31	M1	6.04	6.08
65	C32	M1	5.90	5.92
66	C33	M1	6.10	6.10
67	C34	M1	5.98	6.04
68	C35	M1	6.08	6.14
69	C36	M1	6.14	6.21
70	C37	M1	6.13	6.2
71	C38	M1	6.11	6.21
72	C4	M2	5.79	5.96
73	C5	M2	5.85	5.87
74	C6	M2	5.65	5.7
75	C10	M2	6.09	6.12
76	C11	M2	6.09	6.11
77	C12	M2	6.02	6.12
78	C13	M2	6.00	6.02
79	C14	M2	6.02	6.05
80	C15	M2	6.02	6.03
81	C16	M2	6.01	6.04
82	C17	M2	6.07	6.15
83	C18	M2	6.08	6.09
84	C19	M2	6.18	6.18
85	C20	M2	6.18	6.21
86	C21	M2	6.23	6.24

87	C22	M2	6.24	6.24
88	C23	M2	5.78	5.97
89	C24	M2	5.86	5.87
90	C25	M2	5.68	5.73
91	C26	M2	6.10	6.14
92	C27	M2	6.22	6.27
93	C28	M2	6.24	6.25
94	C29	M2	6.15	6.21
95	C30	M2	6.14	6.27
96	C31	M2	6.25	6.26
97	C32	M2	6.18	6.18
98	C33	M2	6.10	6.23
99	C34	M2	6.20	6.23
100	C35	M2	6.12	6.16
101	C36	M2	6.13	6.17
102	C37	M2	6.11	6.20
103	C38	M2	6.10	6.15
104	C1	M3	6.04	6.08
105	C2	M3	5.90	5.92
106	C3	M3	6.10	6.10
107	C4	M3	6.04	6.05
108	C5	M3	5.87	5.97
109	C6	M3	6.13	6.31
110	C7	M3	6.18	6.23
111	C8	M3	6.06	6.20
112	C9	M3	6.10	6.23
113	C10	M3	6.20	6.23
114	C11	M3	6.12	6.16
115	C12	M3	6.22	6.27
116	C16	M3	6.24	6.25
117	C17	M3	6.15	6.21
118	C18	M3	6.14	6.27
119	C19	M3	6.25	6.26
120	C20	M3	5.79	5.96
121	C21	M3	5.85	5.87
122	C22	M3	5.65	5.70
123	C23	M3	6.09	6.12
124	C24	M3	6.09	6.11
125	C25	M3	6.02	6.12
126	C26	M3	6.00	6.00
127	C27	M3	6.02	6.05
128	C28	M3	6.02	6.03
129	C29	M3	6.01	6.04
130	C30	M3	6.07	6.15
131	C31	M3	6.08	6.09
132	C32	M3	6.13	6.15

133	C33	M3	5.91	6.05
134	C34	M3	6.13	6.17
135	C35	M3	6.04	6.08
136	C36	M3	5.90	5.92
137	C37	M3	6.00	6.08
138	C38	M3	6.10	6.20
139	C1	M4	6.10	6.10
140	C2	M4	5.98	6.04
141	C3	M4	6.08	6.14
142	C4	M4	6.14	6.21
143	C5	M4	5.79	5.96
144	C6	M4	5.85	5.87
145	C7	M4	5.65	5.70
146	C8	M4	6.09	6.12
147	C9	M4	6.09	6.11
148	C10	M4	6.02	6.12
149	C11	M4	6.00	6.02
150	C12	M4	6.02	6.05
151	C13	M4	6.02	6.03
152	C14	M4	6.01	6.04
153	C15	M4	6.07	6.15
154	C16	M4	6.08	6.09
155	C17	M4	6.17	6.18
156	C18	M4	6.18	6.21
157	C19	M4	6.19	6.24
158	C20	M4	5.80	5.96
159	C21	M4	5.85	5.88
160	C25	M4	5.66	5.7
161	C26	M4	6.09	6.13
162	C27	M4	6.10	6.11
163	C28	M4	6.02	6.11
164	C29	M4	6.00	6.01
165	C30	M4	6.02	6.05
166	C31	M4	6.03	6.03
167	C32	M4	6.01	6.04
168	C33	M4	6.07	6.14
169	C34	M4	6.08	6.09
170	C35	M4	6.15	6.17
171	C36	M4	6.18	6.22
172	C37	M4	6.09	6.18
173	C38	M4	6.06	6.15
174	C1	M5	6.20	6.24
175	C2	M5	5.79	5.96
176	C3	M5	5.86	5.88
177	C4	M5	5.65	5.70
178	C5	M5	6.10	6.12

179	C6	M5	6.09	6.11
180	C7	M5	6.02	6.13
181	C8	M5	6.01	6.06
182	C9	M5	6.02	6.05
183	C10	M5	6.01	6.03
184	C11	M5	6.01	6.04
185	C12	M5	6.05	6.15
186	C13	M5	6.08	6.09
187	C14	M5	6.17	6.2
188	C15	M5	6.18	6.21
189	C16	M5	6.17	6.24
190	C17	M5	6.19	6.25
191	C18	M5	6.13	6.3
192	C19	M5	6.17	6.23
193	C23	M5	6.06	6.20
194	C24	M5	6.10	6.24
195	C28	M5	6.20	6.23
196	C29	M5	6.13	6.16
197	C30	M5	6.22	6.27
198	C31	M5	6.24	6.26
199	C32	M5	6.15	6.21
200	C33	M5	6.15	6.27
201	C34	M5	6.25	6.26
202	C35	M5	6.18	6.18
203	C36	M5	6.19	6.21
204	C37	M5	6.13	6.20
205	C38	M5	6.10	6.20
206	C1	M6	6.23	6.24
207	C2	M6	6.24	6.25
208	C3	M6	5.78	5.97
209	C4	M6	5.87	5.87
210	C5	M6	5.68	5.73
211	C6	M6	6.10	6.15
212	C7	M6	6.10	6.11
213	C8	M6	6.03	6.12
214	C9	M6	6.01	6.01
215	C10	M6	6.01	6.05
216	C11	M6	6.03	6.04
217	C12	M6	6.04	6.04
218	C13	M6	6.08	6.16
219	C14	M6	6.08	6.09
220	C15	M6	6.23	6.24
221	C16	M6	6.25	6.25
222	C17	M6	5.77	5.97
223	C18	M6	5.86	5.87
224	C19	M6	5.68	5.74

225	C20	M6	6.10	6.14
226	C21	M6	6.10	6.12
227	C22	M6	6.04	6.12
228	C23	M6	6.00	6.01
229	C24	M6	6.01	6.04
230	C25	M6	6.03	6.03
231	C26	M6	6.02	6.04
232	C27	M6	6.18	6.20
233	C31	M6	6.17	6.24
234	C32	M6	6.20	6.25
235	C33	M6	6.13	6.3
236	C34	M6	6.17	6.23
237	C35	M6	6.07	6.20
238	C36	M6	6.10	6.24
239	C37	M6	6.10	6.18
240	C38	M6	6.11	6.21
241	C1	M7	6.2	6.24
242	C2	M7	6.13	6.16
243	C3	M7	6.23	6.27
244	C4	M7	6.24	6.26
245	C5	M7	6.15	6.22
246	C6	M7	6.14	6.27
247	C7	M7	6.25	6.26
248	C8	M7	6.18	6.18
249	C9	M7	6.18	6.21
250	C10	M7	6.23	6.25
251	C11	M7	6.26	6.27
252	C12	M7	5.78	5.97
253	C13	M7	5.89	5.91
254	C14	M7	5.68	5.73
255	C15	M7	6.10	6.15
256	C16	M7	6.02	6.12
257	C17	M7	6.00	6.02
258	C18	M7	6.01	6.04
259	C19	M7	6.02	6.03
260	C20	M7	6.04	6.05
261	C21	M7	6.11	6.17
262	C22	M7	6.08	6.09
263	C23	M7	6.14	6.15
264	C24	M7	5.93	6.10
265	C25	M7	6.13	6.17
266	C26	M7	6.07	6.09
267	C27	M7	5.91	5.93
268	C28	M7	6.20	6.20
269	C29	M7	5.99	6.05
270	C30	M7	6.10	6.15

271	C34	M7	6.15	6.20
272	C35	M7	6.27	6.28
273	C36	M7	6.21	6.24
274	C37	M7	6.10	6.17
275	C38	M7	6.12	6.22
276	C39	M7	6.03	6.21
277	C1	M8	6.17	6.18
278	C2	M8	6.15	6.20
279	C3	M8	6.03	6.19
280	C4	M8	6.11	6.29
281	C5	M8	6.04	6.05
282	C6	M8	5.87	5.97
283	C7	M8	6.13	6.31
284	C8	M8	6.18	6.23
285	C9	M8	6.06	6.20
286	C10	M8	6.10	6.23
287	C11	M8	6.20	6.23
288	C12	M8	6.12	6.16
289	C13	M8	6.22	6.27
290	C14	M8	6.24	6.25
291	C15	M8	6.15	6.21
292	C16	M8	6.14	6.27
293	C17	M8	6.25	6.26
294	C18	M8	5.79	5.96
295	C19	M8	5.85	5.87
296	C20	M8	5.65	5.7
297	C21	M8	6.09	6.12
298	C22	M8	6.09	6.11
299	C23	M8	6.02	6.12
300	C24	M8	6.00	6.00
301	C25	M8	6.02	6.05
302	C26	M8	6.02	6.05
303	C27	M8	6.01	6.04
304	C28	M8	6.07	6.15
305	C29	M8	6.06	6.09
306	C30	M8	6.13	6.15
307	C31	M8	5.91	6.04
308	C32	M8	6.13	6.17
309	C33	M8	6.04	6.08
310	C37	M8	6.11	6.18
311	C38	M8	6.10	6.20
312	C39	M8	6.03	6.20
313	C1	M9	5.90	5.94
314	C2	M9	6.10	6.10
315	C3	M9	5.99	6.04
316	C4	M9	6.08	6.14

317	C5	M9	6.14	6.21
318	C6	M9	5.79	5.96
319	C7	M9	5.85	5.87
320	C8	M9	5.65	5.70
321	C9	M9	6.09	6.12
322	C10	M9	6.10	6.11
323	C11	M9	6.02	6.12
324	C12	M9	6.00	6.00
325	C13	M9	6.02	6.05
326	C14	M9	6.02	6.03
327	C15	M9	6.01	6.04
328	C16	M9	6.07	6.14
329	C17	M9	6.08	6.09
330	C18	M9	6.17	6.18
331	C22	M9	6.18	6.21
332	C23	M9	6.09	6.24
333	C24	M9	5.80	5.90
334	C25	M9	5.98	6.04
335	C26	M9	6.08	6.14
336	C27	M9	6.15	6.21
337	C28	M9	5.79	5.97
338	C29	M9	5.86	5.87
339	C30	M9	5.65	5.71
340	C31	M9	6.09	6.12
341	C32	M9	6.10	6.11
342	C33	M9	6.02	6.12
343	C34	M9	6.00	6.02
344	C35	M9	6.02	6.05
345	C36	M9	6.05	6.07
346	C37	M9	6.13	6.2
347	C38	M9	6.11	6.21
348	C39	M9	6.03	6.2
349	C1	M10	6.01	6.04
350	C2	M10	6.08	6.15
351	C3	M10	6.08	6.09
352	C4	M10	6.18	6.19
353	C5	M10	6.18	6.21
354	C6	M10	6.22	6.24
355	C7	M10	6.24	6.24
356	C8	M10	5.78	5.96
357	C9	M10	5.86	5.87
358	C10	M10	5.69	5.73
359	C11	M10	6.10	6.14
360	C12	M10	6.22	6.27
361	C13	M10	6.24	6.26
362	C14	M10	6.15	6.21

363	C15	M10	6.15	6.27
364	C16	M10	6.25	6.26
365	C17	M10	6.18	6.19
366	C18	M10	6.10	6.23
367	C19	M10	6.21	6.23
368	C21	M10	6.12	6.16
369	C24	M10	6.13	6.17
370	C25	M10	6.04	6.08
371	C26	M10	5.90	5.93
372	C27	M10	6.11	6.13
373	C28	M10	5.80	5.96
374	C29	M10	5.86	5.89
375	C30	M10	5.68	5.73
376	C31	M10	6.01	6.05
377	C32	M10	6.05	6.07
378	C33	M10	6.01	6.04
379	C34	M10	6.08	6.14
380	C35	M10	6.07	6.09
381	C36	M10	6.18	6.19
382	C37	M10	6.12	6.19
383	C38	M10	6.10	6.20
384	C39	M10	6.04	6.21

Anexo B: Código fuente

Código fuente del algoritmo AES base del Prototipo de escritorio

Proceso principal de Cifrado:

```
addRoundKey(output, current);

for (current = 1; current < Nr; current++) {
    subBytes(output);
    shiftRows(output);
    mixColumns(output);
    addRoundKey(output, current);
}
subBytes(output);
shiftRows(output);
addRoundKey(output, current);
return output;
```

Proceso principal de Descifrado

```
addRoundKey(output, current);
invShiftRows(output);
invSubBytes(output);
for (current = Nr - 1; current > 0; current--) {
    addRoundKey(output, current);
    invMixColumns(output);
    invShiftRows(output);
    invSubBytes(output);
}
addRoundKey(output, current);
return output;
```

Proceso principal de ejecución de Cifrado / Descifrado

```
if ((sourcejTextPane.getText().length() > 0) || (convertjTextPane.getText().length() > 0)) {
    try {
        if (getOriginalText() == null) {
            this.setOriginalText(sourcejTextPane.getText());
        }
        if (exportjComboBox.getSelectedIndex() == 0) {

            bytes_cipherText = ConversionHex.hexToBytes((ConversionHex.asciitoHEX(aes.validateText(this.getCypherText()))));
            if (bytes_cipherText == null) {
                JOptionPane.showMessageDialog(null, "No existe texto para guardar");
            } else {
                try {
                    fileManagement.saveFileBytes(bytes_cipherText);
                    JOptionPane.showMessageDialog(null, "Exportación exitosa");
                } catch (Exception ex) {
                    JOptionPane.showMessageDialog(null, "Error al guardar el archivo");
                }
            }
        } else {
            bytes_plaintText = ConversionHex.hexToBytes((ConversionHex.asciitoHEX(aes.validateText(this.getOriginalText()))));
            if (bytes_plaintText == null) {
                JOptionPane.showMessageDialog(null, "No existe texto que guardar");
                return;
            } else {
                try {
                    fileManagement.saveFileBytes(bytes_plaintText);
                    JOptionPane.showMessageDialog(null, "Exportación exitosa");
                } catch (Exception ex) {
                    JOptionPane.showMessageDialog(null, "Error al guardar el archivo");
                }
            }
        }
    } catch (Exception ex) {
        ex.printStackTrace();
    }
} else {
    JOptionPane.showMessageDialog(null, "No existe texto para guardar");
}
```

Código fuente para la creación del nuevo algoritmo del Prototipo de escritorio

Implementación principal de la nueva función mixDiagonal

```
protected int[][] mixDiagonal(int[][] est) {
    int z = 0;

    Xaux = 0;
    Yaux = 0;
    //Aux= null;
    for (int diag = 3; diag >= 0; diag--) {
        z = 0;
        for (int x = diag; x <= 3; x++) {
            llenarMatriz(est[z][x]);
            z++;
        }
    }

    for (int diag = 1; diag <= 3; diag++) {
        z = 0;
        for (int y = diag; y <= 3; y++) {
            llenarMatriz(est[y][z]);
            z++;
        }
    }
    for (int x = 0; x <= 3; x++) {
        for (int y = 0; y <= 3; y++) {
            est[x][y] = Aux[x][y];
        }
    }
    return est;
}
```

Proceso principal de Cifrado

```
addRoundKey(output, current);
mixDiagonal(output);
for (current = 1; current < Nr; current++) {
    subBytes(output);
    shiftRows(output);
    mixColumns(output);
    addRoundKey(output, current);
}
ciclo = Nr / 2;
for (int y = 1; y <= ciclo; y++) {
    subBytes(output);
    shiftRows(output);
    mixColumns(output);
}
mixDiagonal(output);
addRoundKey(output, current);
return output;
```

Implementación principal de la nueva función InvmixDiagonal

```
protected int[][] invMixDiagonal(int[][] est) {
    int z;
    XauxInv = 3;
    YauxInv = 3;
    for (int x = 0; x <= 3; x++) {
        for (int y = 0; y <= 3; y++) {
            Aux[x][y] = est[x][y];
        }
    }
    for (int diag = 0; diag < 3; diag++) {
        int numAux = 0;
        z = 3;
        for (int y = diag; y >= 0; y--) {
            numAux = devolverMatrizInversa();
            AuxInv[z][y] = numAux;
            z--;
        }
    }
    for (int diag = 3; diag >= 0; diag--) {
        int numAux = 0;
        z = 3;
        for (int x = diag; x >= 0; x--) {
            numAux = devolverMatrizInversa();
            AuxInv[x][z] = numAux;
            z--;
        }
    }
    for (int x = 0; x <= 3; x++) {
        for (int y = 0; y <= 3; y++) {
            est[x][y] = AuxInv[x][y];
        }
    }
    return est;
```

Proceso principal de Descifrado

```
    current = Nr;
    ciclo = Nr / 2;
    addRoundKey(output, current);
    invMixDiagonal(output);
    for (int y = ciclo; y > 0; y--) {
        invMixColumns(output);
        invShiftRows(output);
        invSubBytes(output);
    }
    for (current = Nr - 1; current > 0; current--) {
        addRoundKey(output, current);
        invMixColumns(output);
        invShiftRows(output);
        invSubBytes(output);
    }
    invMixDiagonal(output);
    addRoundKey(output, current);
    return output;
```

Proceso principal de ejecución Cifrado / Descifrado

```
if ((sourcejTextPane.getText().length() > 0) || (convertjTextPane.getText().length() > 0)) {
    try {
        if (getOriginalText() == null) {
            this.setOriginalText(sourcejTextPane.getText());
        }
        if (exportjComboBox.getSelectedIndex() == 0) {

            bytes_cipherText = ConversionHex.hexToBytes((ConversionHex.asciitoHEX(aes.validateText(this.getCypherText()))));
            if (bytes_cipherText == null) {
                JOptionPane.showMessageDialog(null, "No existe texto para guardar");
            } else {
                try {
                    fileManagement.saveFileBytes(bytes_cipherText);
                    JOptionPane.showMessageDialog(null, "Exportación exitosa");
                } catch (Exception ex) {
                    JOptionPane.showMessageDialog(null, "Error al guardar el archivo");
                }
            }
        } else {
            bytes_plaintText = ConversionHex.hexToBytes((ConversionHex.asciitoHEX(aes.validateText(this.getOriginalText()))));
            if (bytes_plaintText == null) {
                JOptionPane.showMessageDialog(null, "No existe texto que guardar");
                return;
            } else {
                try {
                    fileManagement.saveFileBytes(bytes_plaintText);
                    JOptionPane.showMessageDialog(null, "Exportación exitosa");
                } catch (Exception ex) {
                    JOptionPane.showMessageDialog(null, "Error al guardar el archivo");
                }
            }
        }
    } catch (Exception ex) {
        ex.printStackTrace();
    }
} else {
    JOptionPane.showMessageDialog(null, "No existe texto para guardar");
}
```

Código fuente del algoritmo AES base, Prototipo web

Proceso principal de envío de mensajes:

```
byte[] key = ConversionHex.hexToBytes(HexKey);
    if (mensajePlano.length() > 0) {
        if (HexKey != null) {
            try {
                cad_val_pT = Codigo.FuncionesAES.validateText(mensajePlano);
                FuncionesAES aes = new FuncionesAES();
                //AES clave
                aes.setKeyAES(key);
                aes.processKey(key.length);
                String aesEncription1 = aes.encryptionAES(cad_val_pT);
                String CypherText = aesEncription1;
                Mensaje m = new Mensaje();
                m.setMensaje(CypherText);
                m.setUsuario(user);
                m.setDestino(destino);

                ChatBLL chB = new ChatBLL();
                int res = chB.ingresarMensaje(m);
                if(res==-1){
                    out.println("Error al ingresar mensaje");
                }else{

                }
            } catch (Exception ex) {
                ex.printStackTrace();
            }
        }
    } else {
        out.println("No existe texto para procesar");
        return;
    }
```

Proceso principal de la visualización de mensajes:

```
if (lista.size()==0 ){
    out.println("<span style='color:red; font-size:14px;'>No existe mensajes para mostrar.!</span>");
}else{

        for(Mensaje m :lista ){
            String cad_val_pT;
            String CypherText = null;
            String OriginalText= m.getMensaje();
            String HexKey =ConversionHex.asciitoHEX(claveEncrip);
            byte[] key = ConversionHex.hexToBytes(HexKey);
            if (HexKey != null) {
                try {
                    cad_val_pT = Codigo.FuncionesAES.validateText((OriginalText));
                    FuncionesAES aes = new FuncionesAES();
                    aes.setKeyAES(key);
                    aes.processKey(key.length);
                    String aesDescription1 = aes.decryptionAES(cad_val_pT);
                    CypherText= aesDescription1;
                } catch (Exception ex) {
                    ex.printStackTrace();
                }
            }
            if (m.getUsuario().equals(usuario))
            {
                out.println("<b><span style='color:#2471a3; font-size:14px;'> Para "+m.getDestino()+":</b> "+CypherText+"</span><br><hr>");
            }else{
            out.println("<b>"+m.getUsuario()+" dice:</b> "+CypherText+"<br><hr>");
            }
        }
    }
```

Código fuente del nuevo algoritmo, Prototipo web

Proceso principal de envío de mensajes:

```
if (mensajePlano.length() > 0) {
    if (HexKey != null) {
        try {
            cad_val_pT = codigo.FuncionesAES.validateText(mensajePlano);
            FuncionesAES aes = new FuncionesAES();
            //clave nuevo algoritmo
            aes.setKeyAES(key);
            aes.processKey(key.length);
            String aesEncription1 = aes.encryptionAES(cad_val_pT);
            String CypherText = aesEncription1;
            Mensaje m = new Mensaje();
            m.setMensaje(CypherText);
            m.setUsuario(user);
            m.setDestino(destino);

            ChatBLL chB = new ChatBLL();
            int res = chB.ingresarMensaje(m);
            if(res==-1){
                out.println("Error al ingresar mensaje");
            }else{

            }
        } catch (Exception ex) {
            ex.printStackTrace();
        }
    }
} else {
    out.println("No existe texto para procesar");
    return;
}
```

Proceso principal de la visualización de mensajes:

```
if (lista.size()==0 ){
    out.println("<span style='color:red; font-size:14px;'>No existe mensajes para mostrar.!</span>");
}else{

        for(Mensaje m :lista ){
            String cad_val_pT;
            String CypherText = null;
            String OriginalText= m.getMensaje();
            String HexKey =ConversionHex.asciitoHEX(claveEncrip);
            byte[] key = ConversionHex.hexToBytes(HexKey);
            if (HexKey != null) {
                try {
                    cad_val_pT = codigo.FuncionesAES.validateText((OriginalText));
                    FuncionesAES aes = new FuncionesAES();
                    //clave nuevo algoritmo
                    aes.setKeyAES(key);
                    aes.processKey(key.length);
                    String aesDescription1 = aes.decryptionAES(cad_val_pT);
                    //AES clave A
                    CypherText= aesDescription1;
                   // out.println("Descifrado exitoso");
                } catch (Exception ex) {
                    ex.printStackTrace();
                }
            }
            if (m.getUsuario().equals(usuario))
            {
                out.println("<b><span style='color:#2471a3; font-size:14px;'> Para "+m.getDestino()+":</b> "+CypherText+"</span><br><hr>");
            }else{
            out.println("<b>"+m.getUsuario()+" dice:</b> "+CypherText+"<br><hr>");
            }
        }
    }
```