COMPARACIÓN DE MÉTODOS CRIPTOGRÁFICOS PARA LA SEGURIDAD INFORMÁTICA.

HERNÁN DARÍO SERRATO LOSADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO-HUILA, COLOMBIA
2019

COMPARACIÓN DE MÉTODOS CRIPTOGRÁFICOS PARA LA SEGURIDAD INFORMÁTICA.

HERNÁN DARÍO SERRATO LOSADA

Monografía presentada como requisito parcial para optar al título de:
Especialista en Seguridad Informática.

Director:
Hernando José Peña Hidalgo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIA BÁSICAS DE TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO-HUILA, COLOMBIA
2019

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pitalito, Huila. 28/09/2019

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

En la actualidad compartir información a través de internet se ha vuelto cada vez más necesario y a la vez se convierte en un asunto critico por los problemas de seguridad que esto acarrea. De tal manera se necesitan conocer los métodos o técnicas con los que se puede compartir información de forma más segura

El presente trabajo se enfoca en la comparación de tres (3) métodos criptográficos, de tal modo que permita identificar cual es el más eficiente y brinde más seguridad a los datos en tránsito. La comparación se realizará con los algoritmos criptográficos DES, AES y RSA; Se ejecutará el proceso de cifrado y descifrado con cada uno de los algoritmos mencionados utilizando archivos de diferentes tamaños y se comparará su rendimiento basados en los tiempos de cifrado y descifrado. Todo el proceso se realiza utilizando la herramienta Cryptool.

Palabras clave: Criptografía, Criptología, Cifrado, Firma digital. Claves, seguridad

INTRODUCCIÓN

La criptografía ha existido desde tiempos inmemorables y la humanidad sigue haciendo uso de ella casi sin percatarse; la criptografía nace de la necesidad del hombre por transmitir o enviar un mensaje y que en el camino no fuera interceptado y conocido por otro ajeno a su destinatario, ya que esto podría generar múltiples problemas dependiendo del grado de sensibilidad del mensaje. Esta necesidad motivó la creación o invención de los primeros métodos de cifrado que consistía en que solo el emisor y el receptor sabrían cómo interpretar el mensaje, desde entonces se ha venido evolucionando en aras de hacer cada vez más segura la trasmisión de información.

En la actualidad se debe destacar la importancia de la criptografía como una rama fundamental de la seguridad informática la cual no solo proporciona protección, sino que también custodia la confidencialidad lo cual es un aspecto muy importante para todas las organizaciones de hoy en día. La criptografía es una herramienta primordial en la formación y continuidad de una organización debido a que en el tránsito de información o en su almacenamiento el riesgo está latente, pueden suceder robos de información o violación de contraseñas y accesos no autorizados entre otros. Actualmente se cuenta con sofisticados algoritmos de cifrado cada uno con características particulares, pero todos con un fin en común, el de proteger la información.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

Debido a la importancia de los algoritmos de cifrado en la seguridad informática y ante la necesidad de saber escoger sabiamente alguno de ellos para su implementación, se han realizado diversas investigaciones o estudios relacionados con los algoritmos criptográficos. Algunos estudios similares a la presente monografía son:

Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES. Yuri Tatiana Medina Vargas, Haider Andrés Miranda Mnedez. (2015) Publicaron en la revista Mundo FESC, un estudio comparativo de los algoritmos más comunes en la criptografía simétrica: DES, AES y 3DES. esta comparación se enfoca principalmente en determinar la capacidad para asegurar datos y su velocidad, llegando a la conclusión que el algoritmo AES es mejor que DES y 3DES.[1]

Análisis de Comparativo de diferentes algoritmos de cifrado, Lourdes Sánchez, Mariem Hernaine, Víctor Gómez, realizaron un análisis comparativo de los algoritmos de cifrado que utiliza SSH en la transferencia de datos. observando su velocidad y uso de la CPU llegando a la conclusión que los algoritmos más veloces son aes*cbc, blowfishcbc y arcfour. este último es el que menos uso de CPU requiere.[2]

Estudio comparativo de los algoritmos de cifrado de flujo RC4, A5 y SEAL (2002) Silvana Bravo, realizo una descripción de los algoritmos de cifrado de flujo RC4, A5 y SEAL. Adicionalmente realizó pruebas a cada uno de los algoritmos para identificar la velocidad descifrado de los mismos, llegando a la conclusión que SEAL es el más rápido

---

1

MEDINA, Yuri. MIRANDA, Haider (2015) Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES, disponible en: http://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55/97

2

SANCHEZ Lourdes, HERNAINE Mariem, Gómez Víctor, Análisis de Comparativo de diferentes algoritmos de cifrado, disponible en: http://simposio.somece.org.mx/2006/contenido/grupo4/pdf/4_SanchezGuerreroLourdes_analisis2.pdf

para cifrar, pero toma mucho tiempo para pre-procesar la llave. RC4 presenta similar que SEAL, pero existen patrones en la llave que debilitan su seguridad y por último A5 que es el más lento de los tres algoritmos, pero pasa todas las pruebas realizadas lo cual indica un buen nivel de seguridad.[3]

1.2 DESCRIPCIÓN

La criptografía existe desde hace miles de años, se podría decir que desde que la humanidad comenzó a comunicarse, los primeros métodos de cifrado tuvieron su origen en las primeras grandes civilizaciones, los cuales se basaban en el uso de lápiz y papel, estos métodos pasaron a la historia hoy pertenecen a la criptografía antigua o clásica. Siglos después se produjo la invención de máquinas que brindaron métodos de cifrado más elaborados y seguros. Posteriormente se produjo la introducción de la computación permitiendo la elaboración de sistemas de métodos de cifrado más sofisticados.

La criptografía ha ido evolucionando siempre en aras de brindar comunicaciones seguras, sin embargo, casi simultáneamente también se han ido desarrollando diferentes estrategias para lograr vulnerar los códigos y los cifrados como por ejemplo: en criptoanálisis, el cual consiste en buscar las debilidades de los métodos de cifrado con la finalidad de romper o vulnerar su seguridad, no con la finalidad de obtener la información cifrada, sino de encontrar la debilidad del algoritmo para posteriormente diseñar formas de atacar las vulnerabilidades encontradas para lograr obtener la información secreta.

Hasta los años 70, la criptografía segura era dominio casi exclusivo de los gobiernos. Desde entonces, dos sucesos la han colocado de lleno en el dominio público: la creación de un estándar de cifrado público (DES), y la invención de la criptografía asimétrica.

3

BRAVO, Silvana. (2002) Estudio comparativo de los algoritmos de cifrado de flujo RC4, A5 y SEAL, disponible en: http://delta.cs.cinvestav.mx/~francisco/arith/Flujo.pdf

De acuerdo a lo anteriormente mencionado, la criptografía ha existido desde tiempos remotos y surge ante la necesidad del hombre por comunicarse, ya sea en cortas o largas distancias, en muchas ocasiones el mensaje o la información enviada es privada o confidencial y solo la debería conocer el receptor, sin embargo, se corre un alto riesgo de que el mensaje sea interceptado mientras llega a su destino, por lo cual se hace necesario ocultar la información haciéndola ilegible para quien pudiera interceptarla. El objetivo primordial de la criptografía ayudar a conservar el secreto o la privacidad de la comunicación entre el emisor y receptor o receptores, ya sea distorsionando o cambiando de forma aparente la estructura y el contenido del mensaje original, de tal forma que sea ilegible o incompresible para alguien distinto a su receptor.

1.3 FORMULACIÓN

Todas las organizaciones emiten, envían y reciben mensajes o información de una u otra forma, y dicho mensaje o información solo le concierne al destinatario, pero ¿Qué pasaría si alguien intercepta el mensaje? ¿Qué pasaría si alguien descifra la contraseña del correo electrónico, o de cualquier contraseña que autentique un sistema en la organización? Se vería afectada la confidencialidad e integridad de la información, debido a que las empresas desconocen la importancia de la criptografía y su utilidad para crear entornos de comunicación y autenticación más seguros que garanticen la disponibilidad, integridad y confidencialidad de la información.

Dicho lo anterior, se halla la necesidad de realizar esta monografía para comparar y conocer los métodos criptográficos utilizados en la seguridad informática, para que sirva como documento de estudio a las organizaciones y profesionales de seguridad informática, y brinde un conocimiento más amplio sobre la criptografía, así mismo, se hace necesario que las organizaciones conozcan los riesgos a los que se exponen al no contar con herramientas criptográficas que eviten que los delincuentes informáticos puedan descifrar información confidencial y vulnerar la organización. Se crearán campos de culturización en los entornos laborales, permitiendo una mejoría en el tratamiento de la información y ante todo creando una barrera a los atacantes informáticos.

La presente monografía se enfoca en los métodos criptográficos funcionales en seguridad informática, se evalúan los algoritmos criptográficos identificando sus ventajas y desventajas, probando su capacidad de cifrado y descifrado, con el fin de brindar un punto de referencia al momento de seleccionar un método de cifrado para su posterior implementación en algún sistema informático.

Particularmente el desarrollo de esta monografía busca dar respuesta al siguiente interrogante**: ¿Cuál de los métodos criptográficos comparados es el más eficaz y funcional en seguridad informática?**

2. JUSTIFICACIÓN

La criptografía se ha convertido en una necesidad en la actualidad, debido a la entrada de los sistemas informáticos, las tecnologías de la información y la comunicación, junto con la globalización que surge por el auge del internet que hace que casi todo gire en torno a él, ha hecho de la criptografía un requisito indispensable en la comunicaciones, cotidianamente la mayoría de las personas hacen uso del correo electrónico, redes sociales, realizan operaciones bancarias en línea o por cajero electrónico, entre muchas otras actividades, todas las anteriores se encuentran protegidas por contraseñas codificadas electrónicamente, y es así como la criptografía se encuentra presente en el diario vivir y se hace uso de ella casi sin percatarse.

Es hora de percatarse y de conocer la importancia de la criptografía, debido a que ni siquiera las empresas se han percatado de ello. Según ESET Security[4] tan solo el 20% de las organizaciones de América latina usan algún método de cifrado para salvaguardar sus datos, es un porcentaje muy bajo que indica que aún se desconocen los riesgos a los que se está expuesto y también se desconocen los beneficios y la protección que brindan los métodos de cifrado.

Esta monografía pretende evaluar la eficiencia de los métodos criptográficos más usados actualmente, por lo que se han elegido tres métodos criptográficos con la finalidad de indagar sobre las ventajas y desventajas de cada uno de ellos, al igual que conocer su capacidad y velocidad en los procesos de cifrado y descifrado de archivos, logrando identificar en cada uno diferentes características que resultan útiles para la seguridad informática.

De esta manera se proporcionará un punto de referencia en la elección de un método criptográfico u otro, brindando a los profesionales de seguridad informática datos relevantes sobre algunos de los métodos criptográficos más utilizados actualmente, para que tengan un criterio y sirva como documento base o guía para determinar cuál es el método criptográfico más adecuado para su

4 ESET Security Report (2013). Cifrado de la información. Recuperado de http://www.eset-la.com/centro-amenazas/descarga/Latinoamérica- 2013/

implementación. La criptografía para los profesionales de seguridad informática es tema de mucha importancia y se debe ser sumamente cuidadoso con las implementaciones de métodos criptográficos basándose no solo en el diseño de los sistemas, sino también en las especificaciones y necesidades de lo que se desea proteger.

Para ello es preciso establecer variables de comparación que permitan evidenciar las diferentes características con las que cuenta cada uno. Esas variables se enfocan principalmente en su simplicidad y funcionamiento, algunas variables pueden ser: Valor de longitud de clave, tipo de algoritmo, relación de cifrado, problemas de seguridad, velocidad de simulación, escalabilidad, clave utilizada, consumo de energía, implementación, funcionalidad. Al igual que el tiempo de cifrado y descifrado de cada algoritmo, el cual se medirá realizando los procesos de cifrado y descifrado a archivos de diferentes tamaños capturando los tiempos utilizados por cada algoritmo en cada tamaño de archivo. Tales parámetros servirán para comparar los métodos criptográficos entre sí, facilitando la elección del más adecuado entre la gran variedad de algoritmos que ofrecen solución a un mismo problema.

Por lo tanto, se hace necesaria la realización de esta monografía, debido a que por la gran cantidad de algoritmos que existen ofreciendo funcionalidades similares es complicado discernir cual es el más apropiado para lo que se desea implementar o proteger, de tal forma esta monografía pretende servir como guía o referencia para la elección de métodos criptográficos según su funcionalidad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL.

Realizar un análisis comparativo de métodos criptográficos utilizados actualmente en la seguridad informática que permita identificar el nivel de seguridad y rendimiento para su implementación.

3.2 OBJETIVOS ESPECÍFICOS.

- Realizar la identificación de los diferentes algoritmos criptográficos utilizados actualmente en la seguridad informática.

- Seleccionar tres (3) de los algoritmos criptográficos identificados, para realizar la comparación de las ventajas y desventajas de cada uno de ellos.

- Determinar la eficiencia de los algoritmos criptográficos en los procesos de cifrado y descifrado de archivos, calculando el tiempo utilizado por cada uno de ellos en dichos procesos.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La criptografía es considerada como el arte de ocultar o disfrazar la información, sin embargo, abarca una cantidad de conceptos y teorías relacionadas con la información que detallan su complejidad y revelan su funcionalidad en la seguridad de la información, de acuerdo a esto se enuncian algunos conceptos y teorías:

4.1.1 **Teoría de Números.** Esta teoría comprende el estudio de las propiedades de los números específicamente de los enteros, Su utilidad en la criptografía se le atribuye a que utiliza un grupo finito de números enteros sobre el que se permiten cálculos complejos y problemas interesantes. Además de la existencia de operaciones inversas (algoritmos de cifrado y descifrado). números primos para elaborar claves más seguras.[5]

4.1.2 **Teoría de la información.** Esta teoría se enfoca en la labor de cuantificar la información específicamente en la transmisión y el procesamiento de la información y se encarga de la medición de la información y de la representación de la misma, así como también de la capacidad de los sistemas de comunicación para transmitir y procesar información.[6]

---

5 JIMENES, Ernesto (2014) Teoría de números, disponible en: https://sites.google.com/site/2014scjimenezcoronaernesto/4-marco-teorico/4-5-bases-teoricas

6 ECURED, Teoría de la información, disponible en: https://www.ecured.cu/Teor%C3%ADa_de_la_informaci%C3%B3n

4.1.3 **Teoría de complejidad computacional.** Se enfoca en la clasificación de los problemas computacionales según a su complejidad propia, y en la relación entre dichas clases de complejidad. Un problema se cataloga como "inherentemente difícil" si su solución requiere de una cantidad significativa de recursos computacionales, sin importar el algoritmo utilizado. Esta teoría formaliza dicha aseveración, introduciendo modelos de cómputo matemáticos para el estudio de estos problemas y la cuantificación de la cantidad de recursos necesarios para resolverlos, como tiempo y memoria.

Uno de los roles de la teoría de la complejidad computacional es determinar los límites prácticos de qué es lo que se puede hacer en una computadora y qué no. Otros campos relacionados con la teoría de la complejidad computacional son el análisis de algoritmos y la teoría de la computabilidad. Una diferencia significativa entre el análisis de algoritmos y la teoría de la complejidad computacional, es que el primero se dedica a determinar la cantidad de recursos requeridos por un algoritmo en particular para resolver un problema, mientras que la segunda, analiza todos los posibles algoritmos que pudieran ser usados para resolver el mismo problema.[7]

4.1.4 **Teoría de la complejidad algorítmica.** El análisis de algoritmo es una parte muy importante de la ciencia de la computación, de modo que la medida de la eficiencia de u algoritmo será uno de los factores fundamentales. Por consiguiente, es importante poder analizar los requisitos de tiempo y espacio de u algoritmo para ver si existe dentro de límites aceptables.

Es difícil realizar un análisis simple de un algoritmo que determine la cantidad exacta de tiempo requerida para ejecutarlo. La primera complicación es que la cantidad exacta de tiempo dependerá de la implementación del algoritmo y de la maquina en que se ejecuta. El análisis normalmente debe ser independiente del lenguaje o máquina que se utilice para implementar el algoritmo. El análisis del algoritmo tratará de obtener el orden de magnitud de tiempo requerido para la ejecución del mismo y cada algoritmo tendrá un

7

WIKIPEDIA, Teoría de complejidad computacional, Actualizado el 5 de junio 2019, disponible en: https://es.wikipedia.org/wiki/Teor%C3%ADa_de_la_complejidad_computacional

coste computacional diferente la eficiencia es un criterio que se debe utilizar en la selección de un algoritmo y su implementación[8]

4.2 MARCO CONCEPTUAL

4.2.1 **Criptografía.** criptografía es el uso de métodos, algoritmos o técnicas que permitan la protección de archivos y datos, ya sea a través de contraseñas o modificando aparentemente su contenido, La función principal de la criptografía establecer comunicaciones seguras haciendo incomprensible la información para cualquier tercero y solo podrá ser conocida por su destinatario o recepto garantizando la confidencialidad e integridad del mensaje.

4.2.2 **Firmas Digitales.** La firma digital se basa en un algoritmo de cifrado que relaciona la identidad de un sujeto o un sistema informático con el mensaje o el archivo, esto garantiza la integridad de la información transmitida además del no repudio en caso de que el remitente niegue él envió del mensaje. El algoritmo utilizado para el cifrado de las firmas digitales se denomina Funciones hash.

4.2.3 **Esteganografía.** Este término suele confundirse en su concepto con la definición de criptografía, sin embargo, son diferentes. Mientras que la criptografía se encarga de que la información sea ilegible o incomprensible para algún atacante, la esteganografía se encarga de que el atacante o el intruso ni siquiera note la existencia de la información. En eso consiste la esteganografía en ocultar objetos, documentos o mensajes dentro de otros denominados contenedores o portadores de manera que no se conozca su existencia.[9]

8

SAAVEDRA, Jhersi. Teoria de complejidad algorítmica, disponible en: https://www.academia.edu/29765295/Teor%C3%ADa_de_complejidad_Algor%C3%ADtmica

9

GUZMAN Anggie (2011) Esteganografía, disponible en: http://seguridadanggie.blogspot.com/2011/11/esteganografia.html

4.2.4 **Llave simétrica.** La llave simétrica o también denominada clave secreta, la cual consta de una sola llave con la que se cifra y se descifra la información, esto es visto como una desventaja debido a que obligatoriamente debe transmitirle la llave al receptor para que pueda ver la información y muchas veces no se distribuye por canales seguros y termina siendo interceptada y conocida.

4.2.5 **Llave asimétrica.** Por el contrario de la llave simétrica, la llave asimétrica utiliza dos llaves; una publica que es la que se comparte y sirve solo para realizar en cifrado de la información y una privada que solo la conoce su creador quien viene haciendo las veces de receptor y se utiliza para descifrar la información.

4.2.6 **Criptoanálisis.** El criptoanálisis consiste en buscar vulnerabilidades de los métodos criptográficos para posteriormente romper su seguridad sin conocer la información secreta.

4.2.7 **Criptosistema.** Un criptosistema son el conjunto de técnicas o procesos que se utilizan para convertir un texto o un archivo del texto plano a texto cifrado y de igual forma aplica para transformar el texto cifrado en texto plano. Se denomina cifrado o encriptación al proceso de transformar el texto plano en algo incomprensible y se le llama descifrado o desencriptación al proceso de volver el texto a su estado original, ambos procesos son controlados por una o más llaves criptográficas.

4.2.8 **Certificado digital.** Es un archivo informático emitido por un ente certificador que ofrece los servicios de certificación digital, que acredita la identidad del titular y asocia dicha entidad con un par de claves, una pública y otra privada esta última solo es conocida por el titular del certificado, de tal forma se tendrá una identificación digital que puede ser utilizada en internet.

4.2.9 **Contraseñas inseguras.** Las personas del común (sin conocimientos mínimos de seguridad informática) no tienen idea del gran riesgo que se corre al utilizar contraseñas muy débiles que son fáciles de descifrar para los delincuentes informáticos, actualmente los expertos en seguridad y las organizaciones optan por establecer políticas para la creación de contraseñas como, por ejemplo: exigir un mínimo de 8 caracteres, que debe incluir al menos una letra mayúscula y otra minúscula y deben ser cambiadas periódicamente.

4.2.10 **SSL/TLS**. Estos protocolos criptográficos brindan comunicaciones seguras a través de la red. Son los encargados de proteger todos los datos ingresados en las páginas web que cuenten con un certificado SSL brindando confidencialidad de la información, los sitios que no cuentan con un certificado de confianza SSL/TLS no es seguro por tal razón no es recomendable introducir información sensible en ellas debido a que no se cuenta con ningún tipo de protección y sus datos podrían ser revelados.

4.3 ESTADO ACTUAL

Algunos estudios similares a la presente monografía son:

- **Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información.** En el 2018 Ana Liz Samaniego le realizo pruebas a los algoritmos RC5, IDEA y AES junto con un algoritmo de diseño propio denominado ANN. Esto con la finalidad de identificar los niveles de seguridad y rendimiento de cada uno ellos adicional a eso le permitió determinar si son mejores los algoritmos globalmente conocidos o si vale la pena invertir en la creación de un algoritmo propio.[10]

- **Una encuesta sobre el análisis de rendimiento de DES, AES y RSA Algoritmo junto con LSB Sustitución,** B. Padmavathi, S. Ranjitha Kumari (2013) han implementado tres técnicas cifrar como DES, AES y RSA algoritmo junto con

10

Samaniego Zanabria, Ana Liz (2018) Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información, disponible en: http://repositorio.urp.edu.pe/bitstream/handle/URP/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

algoritmos como LSB técnica de sustitución y se compara su rendimiento de técnicas de cifrar basadas en el análisis de su tiempo estimulación en el momento de cifrado y proceso de descifrado y también su tamaño de búfer experimentalmente.[11]

- **Análisis Comparativo de Cifrado Asimétrico algoritmos RSA y ElGamal** (2017) TOMÁS-MARIANO, Víctor Tomás, ESCUDERO-CISNEROS, José y HERNÁNDEZ, Iván. Publicaron en la revista de sistemas computacionales Tics una comparación de dos de los algoritmos asimétricos más conocidos, su comparación se basa en realizar los procesos de cifrado y descifrado con diferentes tipos y tamaños de archivo (txt, pdf, doc, xls) y con varias longitudes de clave en bit. Como resultado de este análisis comparativo permitieron observar que al utilizar el algoritmo RSA el archivo encriptado aumenta su tamaño hasta un 400%, y el algoritmo ElGamal hasta un 1800%, sin embargo, este último últimos es más veloz en el proceso de cifrado.[12]

11

B. Padmavathi, S. Ranjitha Kumari (2013) *A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique* disponible en: https://www.ijsr.net/archive/v2i4/IJSRON120134.pdf

12

TOMÁS-MARIANO, Víctor Tomás, ESCUDERO-CISNEROS, José y HERNÁNDEZ HERNÁNDEZ, Iván. Análisis Comparativo de Cifrado Asimétrico algoritmos RSA y ElGamal.RevistadeSistemas Computacionales y TIC'S2017,3-10:42-49

5. IDENTIFICACIÓN DE ALGORITMOS CRIPTOGRÁFICOS UTILIZADOS ACTUALMENTE EN LA SEGURIDAD INFORMÁTICA

5.1 CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica comprende la agrupación de técnicas o métodos en busca de brindar seguridad en las comunicaciones, la palabra simétrica en este caso hace referencia a que se usa una sola llave para cifrar y descifrar, lo cual es considerado como una desventaja debido a que obligatoriamente debe transmitirle la llave al receptor para que pueda ver la información y muchas veces no se distribuye por canales seguros y termina siendo interceptada y conocida. Es por ello que la seguridad del algoritmo consiste conservar la clave en secreto. Su principal característica es la rapidez y facilidad de implementación. Esta clase de criptografía también es denominada criptografía de llave secreta o de llave privada. A su vez la criptografía de clave simétrica puede ser clasificada en tres grandes grupos:

- Criptografía simétrica de lluvia.
- Criptografía simétrica de bloques.
- Criptografía simétrica de resumen.

Este tipo de criptografía se ha considerado la más utilizada en toda la historia, se la puede implementar en distintos dispositivos, manuales, eléctricos, manuales, mecánicos, así como en los algoritmos configurable en cualquier sistema informático. Generalmente se busca aplicar diversas funciones a la información a cifrar de manera que sólo sabiendo la clave se podrá descifrarlos.

La velocidad de estos sistemas es mucho mayor comparados con los de llave publica, y son muy eficientes para el encriptado de grandes volúmenes de información. Un aspecto que juega en contra de este sistema es que necesariamente se debe compartir la clave entre el remitente y el receptor lo cual representa un riesgo a la seguridad por que la clave puede ser interceptada.

Estos sistemas son muy utilizados para el cifrado de correos electrónicos o en donde se requiera el intercambio de información en las comunicaciones digitales. Algunos de los algoritmos empleados para ello son:

- NCT
- IDEA
- RC5
- RC4
- RC2
- 3DES
- DES

5.1.1 **Cifrado de Flujo.** La intención principal este cifrado es dividir los que se desea cifrar en partes pequeñas específicamente con una longitud de un bit, posteriormente cada parte es codificada según los bloques anteriores, este método usa una llave de codificación distinta, este valor debe ser especificado en el algoritmo para cada uno de los fragmentos, de este modo cada vez que se realiza la codificación el algoritmo creara un texto cifrado.

5.1.2 **Cifrado en Bloque.** Por el contrario que el cifrado de flujo que busca dividir el texto en partes pequeñas, Es tipo de cifrado busca crear fragmentos o bloques relativamente grandes aproximadamente de 64 o 128 bits, utilizando una sola clave de cifrado la cual es empleada en cada bloque. Y con esta clave se establece el orden de ejecución de las funciones matemáticas del algoritmo para cada bloque.

5.1.3 **Cifrado de Feistel.** Así son llamados los métodos de cifrado que consisten dividir los bloques de datos en dos partes o fragmentos y en cada ronda de cifrado se utiliza de manera alterna una de las partes.

5.1.4 **AES (*Advanced Encryption Estándar*)** El estándar de cifrado avanzado es usado con la finalidad de proteger los datos mediante el cifrado de los mismos, evitando los accesos o divulgaciones no autorizadas. Una de las características favorables de este algoritmo criptográfico es que cuenta con una longitud de clave variable las cuales son: 128, 192 y 256 bits.

Actualmente este algoritmo es considerado uno de los más seguros, eficientes y funcionales para la seguridad informática, y es empleado para cifrar casi cualquier tipo de datos razón por la cual ya se encuentra implementado en gran cantidad de protocolos por ejemplo es utilizado para el cifrado de clave wifi en el protocolo WPA2, También es utilizado por el protocolo SSH para el cifrado de canales de comunicación, entre otras muchas implementaciones que se han realizado. Adicionalmente su uso es totalmente libre lo que aumenta mucho más su popularidad. Además, los requerimientos en cuanto a hardware y almacenamiento no son altos y su implementación es relativamente fácil.

Este estándar utiliza el llamado algoritmo Rijndael en combinación con el cifrado bloque simétrico como método de cifrado. Las longitudes de bloque y de clave están definidas respectivamente. De este modo, la longitud de bloque es p.ej. de 128 bit y la longitud de clave es de 128, 192 o 256 bit.[13]

5.1.5 **DES. (*Data Encryption Standard*)** Es un algoritmo criptográfico adoptado como estándar en los Estados Unidos, y se hizo mundialmente conocido. Desde sus inicios genero controversias debido a la longitud de su clave considerada corta, Además de las sospechas de la agencia nacional de seguridad sobre la existencia de algún backdoor en el algoritmo. Actualmente este método es considerado inseguro debido a que su longitud de clave de 56 bits es corta lo cual facilita el rompimiento de la misma existen casos en que la clave ha sido rota en menos de 24 horas.

13 NFON, AES, disponible en: https://www.nfon.com/es/servicio/base-de-conocimiento/base-de-conocimiento-destacar/aes/

Seguridad en DES: Como se mencionó anteriormente fue demostrado que gracias a la evolución de la informática y a la gran capacidad de computo actual este algoritmo es vulnerable a ataques de fuerza bruta. Es preciso aclarar que en si el algoritmo no es débil, su debilidad su corta longitud de clave.

Variantes del DES: Debido a que DES ya no inspiraba confianza y teniendo en cuenta que el algoritmo en particular no era malo sino solo su clave se crear los métodos conocidos como variantes DES consiste en utilizar el algoritmo DES, pero asignándole una longitud de clave más larga. Algunos de estos algoritmos son: 3-DES con una longitud de clave de 168 bits y el algoritmo IDEA con una longitud de clave de 128.[14]

5.1.6 **IDEA (*International Data Encryption Algorithm*).** En este método criptográfico la información original y los datos encriptados están constituidos por bloques de 64 bits, con una longitud de clave 128 bits. Este algoritmo surge como alternativa a DES. Se ejecutan ocho rondas de cifrado iguales con una transformación de salida. Este proceso es similar al de DES, pero con un mayor grado de complejidad en las rondas. En cada ronda de cifrado, se dividen los bloques de entrada en 4 sub-bloques de 16 bits. Y son utilizadas 6 subclaves para cada ronda. Este método es considerado seguro debido a que actualmente aún no se pueden computar 10^{38} claves.[15]

5.2 CRIPTOGRAFÍA ASIMÉTRICA

También llamada de clave publica basa su seguridad principalmente en la factorización de números enteros en números primos, lo cual hace la clave demasiado extensa como para ser descifrada a fuerza bruta. Por el contrario de la criptografía simétrica, la criptografía asimétrica utiliza dos llaves: una publica que es la que se comparte y sirve solo para realizar el cifrado de la información y una

---

14

ARRIAZU SANCHEZ, Jorge (1999) Descripción del Algoritmo DES, disponible en: https://www.academia.edu/15633436/Descripción_del_algoritmo_DES_Data_Encryption_Standard

15

BADILLO, Verónica, GALLARDO, Luis, HERNANDEZ, Leticia, MENDOZA, Jeanette, PACHECO, José (2009) ALGORITMO IDEA (Algoritmo Internacional de Cifrado de Datos) disponible en: https://es.scribd.com/document/116145945/Algoritmo-Idea

privada que solo la conoce su creador quien viene haciendo las veces de receptor y se utiliza para descifrar la información.

Este método soluciona el problema que presenta la criptografía simétrica, debido a que la clave puede ser compartida sin tomar medidas adicionales, no importa si es interceptada ya que la clave es publica y puede ser conocida por cualquiera, pero solo servirá para cifrar, y la información que se cifre con esa clave publica solo podrá ser descifrada por el que conozca la clave privada. De esta forma la criptografía asimétrica garantiza que la información enviada solo pueda ser revelada por su destinatario o receptor. La principal desventaja de la criptografía asimétrica es la demora en los procesos de cifrado y descifrado además de otros inconvenientes que se detallaran en esta monografía. Los algoritmos asimétricos más conocidos son:

5.2.1 **RSA.** Este método es el pionero y más usado algoritmo de la criptografía asimétrica y es muy útil tanto para cifrar datos o archivos como para firmas digitales. Su seguridad se basa en la gran longitud de sus claves utilizando la factorización de números enteros, la información enviada se muestra mediante números y su funcionamiento consiste en el resultado de 2 números primos extensos seleccionados aleatoriamente y conservados en secreto. Como todo método asimétrico, cada persona de generar su par de llaves la pública y la privada. cuando se necesite enviar algún mensaje, el remitente puede utilizarla llave publica para cifrar este mensaje y de esta forma solo el creador de la llave publica podrá descifrar el mensaje utilizando la llave privada.[16] El proceso resumido que se sigue es el siguiente:

El servidor genera dos números que son públicos n y e

El cliente cifra el mensaje M usando la siguiente operación:

$$C = (M^e)_{mod\ n}$$

El servidor recibe el mensaje cifrado C y lo descifra usando la siguiente operación:

16

SEGU.INFO, Criptología - Algoritmos Asimétricos (Llave Privada - Pública) disponible en: https://www.segu-info.com.ar/criptologia/asimetricos.htm

$$M = (C^d) \, mod \, n$$

Bien, ahora una explicación de lo anterior:

El servidor genera dos números primos grandes p y q. En la actualidad cada uno tiene 1024 bits, es decir, 309 dígitos decimales. Los multiplica y obtiene el número n

$$n = p * q$$

Por otro lado, obtiene el indicador de phi de Euler

$$F = (p-1)(q-1)$$

Genera la clave pública e que es primo relativo de F. Esto significa que e y F no tienen divisores comunes más allá del 1. Además, el número e tiene que ser mayor que 1 y menor que F, es decir

$$1 < e < F$$

Por cuestiones de eficiencia y seguridad, se elige siempre el valor $e = 65537$ que es un número primo y es el número 4 de Fermat. De esta forma el servidor no tiene que enviar dos números al cliente, sólo su clave pública.

$$2^{2^4} + 1 = 2^{16} + 1$$

Ahora, se genera la clave privada d que cumpla que

$$e * d \, mod \, F = 1$$

Las operaciones anteriores contienen un concepto que pocos conoceréis, la aritmética modular. En la aritmética modular lo que nos interesa es el resto de la división, no el cociente. En la operación $a = b \, mod \, n$, a es el resto de dividir b por n. Por ejemplo, $58 \, mod \, 9 = 4$, porque $58/9 = 6.44...$, $9 * 6 = 54$, entonces $58 - 54 = 4$

Como se puede ver, generar la clave pública y privada es muy costoso computacionalmente, y factorizar un número grande para poder reventar la clave es increíblemente complicado. No es imposible, pero lleva un tiempo altísimo.[17]

5.2.2 **Algoritmo Asimétrico ElGamal.** Este método criptográfico está basado en la función unidireccional exponencial discreta. Este criptosistema sirvió como apoyo para la creación de un algoritmo alternativo al RSA y al DSA utilizados en la criptografía asimétrica. Este método está constituido por tres elementos que son: el generador de claves, el algoritmo de cifrado y el de descifrado.[18]

Es muy similar a RSA respecto a su utilidad, debido a que los dos pueden ser empleados tanto para firmas digitales como para el cifrado y descifrado de datos. La seguridad de este método se fundamenta en el supuesto de usar un único sentido y la complejidad de computar un logaritmo discreto. En la actualidad se puede decir que este método es muy efectivo, Aunque sería posible romper este cifrado si se cuenta con la capacidad de cálculo adecuada. Actualmente los algoritmos de computo de logaritmos existentes son incapaces de realizar esta labor en números grandes, por lo menos en un tiempo razonable.[19]

17 SEGU.INFO, Criptología - Algoritmos Asimétricos (Llave Privada - Pública) disponible en: https://www.segu-info.com.ar/criptologia/asimetricos.htm

18 ECURED (2013) ElGamal, disponible en: https://www.ecured.cu/ElGamal

19 WIKIMEDIA FOUNDATION (2010) Cifrado ElGamal, disponible en: https://esacademic.com/dic.nsf/eswiki/263781

5.2.3 ***Digital Signature Algorithm*** **(DSA).** Traducido al español significa algoritmo de firma digital perteneciente al grupo de la criptografía asimétrica o de clave pública. Únicamente puede ser utilizado para firmas digitales, permite verificar la autenticidad de un mensaje dada la clave pública y la firma del mensaje, también se pueden generar pares de claves una publica y otra privada y generar firmas de datos utilizando la llave privada generada. Este método se fundamenta en la función exponencial discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente reversible (logaritmo discreto).

Un ejemplo práctico de este método y de la mayoría de los algoritmos asimétricos es: Juan desea enviar información a pedro, Para eso previamente pedro debió crear su par de llaves, la llave publica será la que le compartirá a Juan para que cifre la información y se la envié, de este modo se garantiza la confidencialidad e integridad del mensaje debido que la llave privada solo la conoce pedro. De igual manera si alguien más desea enviarle información a pedro podrá utilizar la misma llave pública.

5.2.4 **Funciones Hash.** Los hash o funciones de resumen son algoritmos que se basan en crear una entrada a partir de cualquier dato puede ser un archivo, una contraseña. Y genera una salida alfanumérica lo cual es el resumen de la información, pero en caracteres que son incomprensibles, es decir a partir de los datos de entrada se crea una cadena que solo puede volverse a crear con esos mismos datos. Las funciones hash son bastante utilizadas para la protección de la confidencialidad de contraseñas ya que en la mayoría de los casos estas son almacenadas e introducidas en texto plano lo cual representa un gran riesgo a la seguridad estas funciones tiene un propósito diferente a los de los métodos simétricos y asimétricos, y pueden ser utilizados para varios objetivos como por ejemplo: garantizar que los archivos no han sido modificados en tránsito, proteger las contraseñas y para firmas digitales. Algunos algoritmos son:MD2, MD4, MD5, SHA/SHA-1 [20]

20

GUTIERREZ, Pedro (enero 15, 2013) ¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales, disponible en: https://www.genbeta.com/desarrollo/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

6. ESTUDIO COMPARATIVO DE TRES ALGORITMOS CRIPTOGRÁFICOS

Con la entrada de las computadoras y el internet, y ante la necesidad de mantener comunicaciones seguras, se dio paso a la creación de algoritmos criptográficos en aras de lograr este objetivo, uno de los primeros algoritmos criptográficos es el denominado DES (*Data Encryption Standard*) el cual fue desarrollado en el año 1976 y será objeto de esta comparación por su antigüedad con la finalidad de determinar las diferencias con algoritmos modernos, uno de esos métodos modernos y que pertenece a la criptografía simétrica al igual que el anterior es el algoritmos AES (*Advanced Encryption Standard*) el cual fue adoptado como estándar en el año 2001 y actualmente es considerado uno de los más utilizados y seguros, razones por las cuales fue seleccionado para este estudio.

De igual manera, existen otros métodos criptográficos pertenecientes a la criptografía asimétrica, los cuales utilizan una llave privada y una publica, dentro de este tipo de criptografía resalta el algoritmo RSA (Rivest Shamir Aldeman) debido a su funcionalidad puede ser utilizado para cifrado archivos y firmas digitales, la inclusión de este algoritmo permitirá identificar tanto las diferencias entre los algoritmos, como las diferencias entre la criptografía simétrica y asimétrica.

De acuerdo a lo anterior los algoritmos criptográficos a comparar son:

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- RSA (Rivest Shamir Aldeman)

Para la comparación se utilizan los siguientes valores:

- **Desarrollado**: establece sobre la línea de tiempo del algoritmo.
- **Valor de longitud de clave**: desempeña un papel vital que muestra cómo se encriptan los datos.
- **Tipo de algoritmo**: Existen dos tipos de algoritmo. Basado en el proceso y la clave, se segrega como simétrico y asimétrico.

- **Relación de cifrado:** mide la cantidad de datos que se van a cifrar. Se debe minimizar para reducir la complejidad. En este análisis se señalan tres niveles como bajo, medio, alto.
- **Problemas de seguridad:** la técnica de encriptación debe satisfacer la seguridad criptográfica, como el texto sin formato, el ataque de texto cifrado.
- **Velocidad de simulación:** Velocidad utilizada en los procesos de cifrado y descifrado.
- **Escalabilidad:** el tamaño de la clave y la variación del tamaño del bloque se conoce como escalabilidad.
- **Clave utilizada:** para especificar si se utiliza la misma clave para el proceso de cifrado y descifrado o una clave diferente.
- **Consumo de energía:** se mide la energía en unidades cuando se lleva a cabo el proceso. Se indica en dos niveles, como alto y bajo.
- **Implementación:** el hardware y el software son efectivos en AES en comparación con DES y RSA
- **Uso o Utilidad:** En que se utilizan.
- **Funcionalidad:** ¿Para qué sirve?

Tabla 1. Valores comparativos

Factor Analizado	DES	AES	RSA
Desarrollado	1977	2000	1978
Valor de longitud de Clave	56 bits.	128, 192,256 bits.	>1024 bits
Tipo de Algoritmo	Simétrica	Simétrica	Asimétrica
Relación de Cifrado	Low	High	High
Seguridad	Inadecuado	Altamente Seguro	Ataque de Tiempo
Velocidad de Simulación	Rápido	Rápido	lento
Escalabilidad	Algoritmo escalable	No escalable	No escalable
Clave Utilizada	Una sola llave para el cifrado y	Una sola llave para el cifrado y	Utiliza dos llaves una para cifrar y otra para

	descifrado.	descifrado.	descifrar.
Consumo de Energía	Bajo	Bajo	Bajo
Implementación Hardware y software	Mejor en hardware que en software.	Mas rápido y eficiente.	Alto costo computacional
Numero de rondas	16	10-12-14	N/A
Utilidad	Confidencialidad, integridad.	Confidencialidad, integridad.	Confidencialidad, integridad, autenticidad de origen, no repudio.

Tabla 1. Continuación

Funcionalidad	Cifrado de mensajes, cifrado de archivos.	Cifrado de mensajes, cifrado de archivos, cifrado de contraseñas.	Cifrado de mensajes, firma digital, intercambio de claves.

Fuente: B. Padmavathi, S. Ranjitha Kumari (2013) A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique, disponible en: https://www.ijsr.net/archive/v2i4/IJSRON120134.pdf

En la Tabla 1. Valores comparativos, se encuentran establecidas las variables anteriormente descritas para cada uno de los algoritmos y en la cual se puede evidenciar que el algoritmo más reciente según su año de creación es AES, El algoritmo RSA cuenta con una longitud de clave mucho más grande que AES y DES, este último con la longitud de clave más corta y por lo tanto es considerado inseguro en comparación con AES y RSA. los algoritmos simétricos son mucho más rápidos en los procesos de cifrado y descifrado y consumen menos energía.

7. EVALUACIÓN Y RESULTADO EXPERIMENTAL

Los resultados experimentales se implementan utilizando la herramienta cryptool. Los algoritmos de encriptación mencionados anteriormente se probaron cifrando y descifrando diferentes tamaños de archivo y los resultados se muestran en la Tabla 2. Resultados evaluación, El desempeño de esos algoritmos se evalúa considerando la velocidad de cifrado y descifrado para cada tamaño de archivo.

Las cifras o tiempos mostrados en la siguiente tabla fueron obtenidos a través de las pruebas realizadas con la herramienta cryptool. La cual permite experimentar con algoritmos criptográficos clásicos y modernos, en este caso el experimento consistió en cifrar y descifrar archivos de diferentes tamaños y por medio de la aplicación se obtienen los tiempos utilizados en cada proceso. Las pruebas o imágenes del proceso realizado se encuentran en los anexos de este documento.

Tabla 2. Resultados evaluación

ALGORITMO	TAMAÑO DE ARCHIVO (kb)	TIEMPO DE CIFRADO (Segundos)	TIEMPO DE DESCIFRADO (Segundos)
AES	2048	0,562	0,815
DES		0,620	0,997
RSA		2,636	30,779
AES	4096	1,006	1,293
DES		1,238	1,561
RSA		4,508	64,319
AES	6144	1,658	1,971
DES		1,863	2,107
RSA		6,785	95,254
AES	8192	2,137	2,417
DES		2,476	2,768
RSA		9,032	126,594
AES	10240	2,819	3,096
DES		3,002	3,289
RSA		11,294	160,164

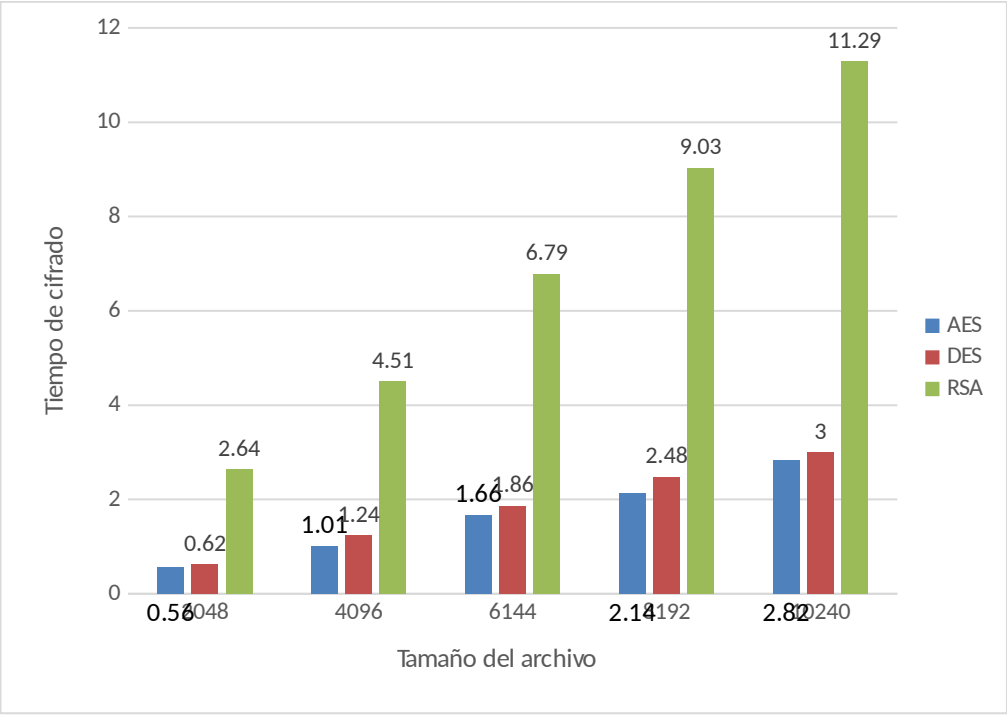
Fuente: Autor

Al analizar la Tabla 2. Resultados evaluación, se puede observar que a partir del tiempo utilizado con el archivo 2048 kb el tiempo empleado aumenta gradualmente según el tamaño del archivo, es decir a modo de ejemplo, si para cifrar un archivo de 2048 Kb demoro 2 segundos para cifrar un archivo de 4096 demorara 4 segundos y así sucesivamente. Aunque los resultados en la tabla no son tan exactos, si se aproximan a lo anteriormente explicado.

También es evidente que el tiempo tomado por el algoritmo RSA para el proceso de cifrado y descifrado es mucho mayor en comparación con el tiempo tomado por el algoritmo AES y DES, estos dos últimos utilizan tiempos muy similares la diferencia es muy pequeña, siendo AES el algoritmo de cifrado más rápido, seguido por DES y como se mencionó anteriormente RSA es el más lento con una notoria diferencia (aunque eso no quiere decir que el algoritmo no sea funcional). También se observó los usos de la memoria por el algoritmo AES, DES y RSA y se determinó que los usos del tamaño del búfer del algoritmo RSA son más altos para todos los tamaños de archivo de documento.

A continuación, en la figura 1 se representan los tiempos empleados por cada algoritmo en el cifrado de archivos con diferentes tamaños, se inicia con un archivo de 2 MB y se va incrementando de 2 MB en 2 MB hasta llegar a 10 MB, con los tiempos obtenidos en la primera medición se puede observar que aproximadamente este mismo tiempo es el que aumenta para cada tamaño de archivo, esto quiere decir que los tiempos necesarios para el proceso cifrado son directamente proporcionales al tamaño de la información a cifrar, entre más grande sea el archivo más tardara cada proceso. También se evidencia que los algoritmos simétricos AES y DES, son mucho más veloces en el proceso de cifrado y que el algoritmo asimétrico RSA tarda hasta cuatro veces más que los otros algoritmos comparados.

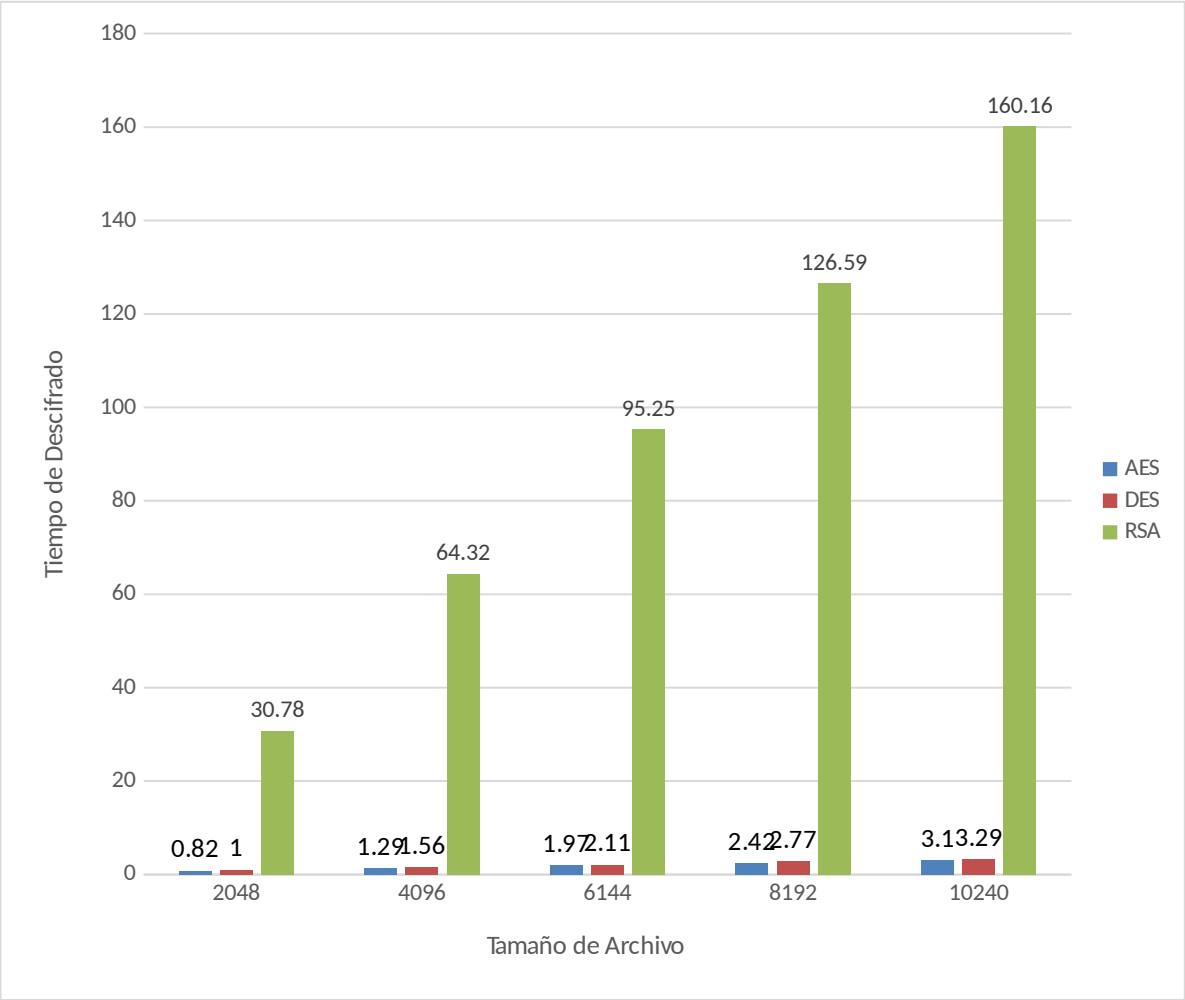
Figura 1. Tiempos de cifrado.



Fuente: Autor

De igual manera, en la figura 2 se muestran los tiempos utilizados por cada algoritmo para el descifrado, este proceso se realizó con los mismos archivos cifrados en el paso anterior, cabe resaltar que este procedimiento tarda más para cada algoritmo debido a que se debe interpretar el texto cifrado y revelar el texto claro. Es notorio que el algoritmo RSA es el que emplea más tiempo, hasta más de 14 veces del tiempo que utilizo para el cifrado y hasta 37 veces del tiempo utilizado por los algoritmos AES y DES. Los algoritmos simétricos también tardan un poco más para realizar este proceso, pero con una diferencia muy mínima en comparación a la anterior.

Figura 2. Tiempos de descifrado



Fuente: Autor

A través de las figuras anteriores se pudo determinar que el algoritmo AES es el más rápido tanto en el cifrado como en el descifrado de archivos, seguido por el algoritmo DES, aunque por una muy pequeña diferencia y por último se ubica el algoritmo asimétrico RSA el cual tarda hasta 4 veces más en el cifrado y hasta 37 veces más en el descifrado respecto a los demás algoritmos comparados.

8. CUADRO COMPARATIVO VENTAJAS Y DESVENTAJAS

Al momento de elegir un método criptográfico a implementar es importante conocer sus ventajas y desventajas de manera tal que permitan identificar sus fortalezas, debilidades y funcionalidades. De esta forma se tiene un punto de partida para realizar una sabia elección de un algoritmo que se ajuste a lo necesitado y logre desempeñar correctamente su propósito.

En la tabla 3 se plasman las ventajas y desventajas más relevantes de cada uno de los algoritmos, se obtienen a través de la consulta documental. Cada algoritmo ha sido diseñado para un fin en específico y cumplen a cabalidad con su función, por tal razón, hay aspectos a tener en cuenta al momento de seleccionar un método criptográfico para su implementación.

Tabla 3. Ventajas y desventajas

ALGORITMO	VENTAJAS	DESVENTAJAS
AES	• No es vulnerable al criptoanálisis o diferencial. • Hasta la fecha no se conoce de ningún ataque a gran escala que haya sido exitoso. • Es efectivo para cifrar grandes cantidades de información en un tiempo relativamente corto. • Permite aumentar los bits de la clave para mayor seguridad. 128, 192 y 256 bits. • Gran velocidad de cifrado y descifrado. • No aumenta el tamaño del mensaje.	• La comunicación de la clave puede representar una debilidad al sistema, pues un tercero puede obtenerla. • El número de rondas usadas por clave y la cantidad de rondas de los ataques son relativamente cortas entre sí. • El uso de este método puede poner en riesgo las partes involucradas en una comunicación punto a punto.
DES	• Es uno de los algoritmos más conocidos en el mundo. • Económico • Fácil implementación.	• La clave solo es de solo 56 bits y es considerada muy corta para garantizar seguridad.

Tabla 3. Continuación

ALGORITMO	VENTAJA	DESVENTAJA
DES	• Aún no ha sido roto con un sistema practico. • Gran velocidad de cifrado y descifrado. • No aumenta el tamaño del mensaje. Bajo consumo de recursos	• Con el acelerado avance de la tecnología se presume que con la potencia de cálculo adecuada se puede violar el algoritmo, aunque en un tiempo que no resulta peligroso • Es muy limitado en cuanto a sus posibilidades de configuración debido a que su clave no es variable.
RSA	• Soluciona el inconveniente del envió de las llaves • Se puede usar para el manejo de firmas digitales. • La seguridad de este algoritmo radica en la longitud de la clave.	• Los procesos de cifrado y descifrado suelen ser lentos dependiendo del tamaño del mensaje. • El mensaje cifrado aumenta de tamaño en comparación con el mensaje original. • La llave privada debe ser cifrada por algún algoritmo simétrico. • Costo computacional elevado para el proceso de generación de claves • Es una necesario una autoridad de Certificación en el proceso.

Fuentes: LEXLER, James. (2015) Algoritmo AES, disponible en: https://es.slideshare.net/Ayares/algoritmo-aes; DES, disponible en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html; BRONANO, Torres. (2015) Criptografía Asimétrica el RSA, disponible en: https://es.slideshare.net/juancarlosbroncanotorres/critografia-asimetrica-el-rsa

Las características principales del Algoritmo AES son la rapidez, seguridad, eficiencia y facilidad de implementación. Esta diseñado de manera que se pueda aumentar la longitud de clave según las necesidades, de manera que las claves podrán variar siempre entre 128, 192 y 256 bits. Es implementable tanto en software como en hardware, como todos los métodos simétricos su principal debilidad se debe a la comunicación de la clave.

El algoritmo criptográfico DES comparte algunas características con AES, en cuanto a su rapidez, eficiencia y facilidad de implementación. Sin embargo, su seguridad se ha visto expuesta debido a su corta longitud de clave, y sumado a que se posee una única clave y debe ser compartida hicieron que este algoritmo sea considerado inseguro y se encuentre obsoleto en la actualidad

Por otro lado, los algoritmos asimétricos no se caracterizan por su rapidez, pero si son considerados muy seguros. El algoritmo RSA es uno de los más conocidos y usados de la criptografía asimétrica, permite longitudes de clave variable, siendo aconsejable actualmente el uso de llaves de no menos de 1024 bits. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para cifrar y enviar la llave simétrica que se usará posteriormente en la comunicación cifrada.

9. CONCLUSIONES

A través de la indagación se lograron identificar gran variedad de métodos criptográficos existentes en la actualidad, los cuales principalmente se diferencian en que fueron diseñados para cumplir un objetivo en específico, como, por ejemplo: cifrar contraseñas, cifrar archivos, firmas digitales, entre otros. Cada algoritmo desempeña una función muy importante para la seguridad informática.

De esa gran variedad de algoritmos identificados se destacan: el algoritmo DES por su historia, el algoritmo AES por su funcionalidad y el algoritmo RSA por su seguridad. Por lo cual fueron objeto de esta comparación logrando conocer sus ventajas y desventajas concluyendo que: el algoritmo DES posee una longitud de clave muy corta, por lo cual es considerado inseguro y en la actualidad declarado obsoleto; por consiguiente, el algoritmo AES es uno de los más utilizados actualmente, cuenta con una longitud de clave variable de hasta 256 bits lo que ofrece mayor seguridad además de su excelente rendimiento en los procesos de cifrado y descifrado. Y por último el algoritmo RSA, que es el más conocido de la criptografía asimétrica y es considerado uno de los más seguros debido a su proceso de generación de claves de más de 1024 bits. Resulta muy útil en firmas digitales, aunque para su implementación tiene un alto costo computacional.

En la prueba realizada para calcular el tiempo que utiliza cada algoritmo en el cifrado y descifrado de archivos se logró determinar que los algoritmos simétricos DES y AES son muchos más veloces cifrando y descifrando, mientras que el algoritmo asimétrico RSA tarda hasta 14 veces más ejecutando los mismos procesos. Como conclusión general, cada algoritmo criptográfico ha sido diseñado con diferentes características y con distintas funcionalidades, pero todos coinciden en que su principal objetivo es proteger la información.

10. RECOMENDACIONES

- Para el cifrado de archivos, mensajes y contraseñas se recomienda la utilización del algoritmo AES, debido a que se ha comprobado su capacidad y gran velocidad en el cifrado y descifrado y su longitud de clave variable es garantía de seguridad, dado que hasta el momento no es posible romper este algoritmo por lo menos en un tiempo razonable.

- Aunque el algoritmo asimétrico RSA es demasiado lento en comparación con los métodos simétricos, cabe resaltar que este método proporciona un alto nivel de seguridad debido a la gran longitud de sus claves, siendo prácticamente imposible de computar en la actualidad. Su uso es muy recomendado en el cifrado de archivos y firma digital, debido a que con la utilización de una llave publica y una privada garantiza la confidencialidad, integridad y no repudio de la información.

- El algoritmo DES está considerado obsoleto debido a que fue roto en un tiempo menor de 24 horas, culpando a su corta longitud de clave; Por lo cual no se recomienda su utilización para futuras implementaciones, Sin embargo, a raíz de esto surgieron variantes de este algoritmo, corrigiendo las debilidades presentadas en el mismo, de tal manera se recomienda la utilización de las variantes del algoritmo DES, algunos de estos son: 3-DES e IDEA.

- Debido al vertiginoso avance de la tecnología, lo que hoy se considera seguro, en un futuro puede no serlo, de tal manera se recomienda mantenerse al tanto sobre la actualizaciones y novedades de los métodos criptográficos.

BIBLIOGRAFÍA

ALCOCER y MARTINEZ, Mariano. (2006). Criptografía Española. Recuperado de http://www.cervantesvirtual.com/nd/ark:/59851/bmcqr5g8

AMIEVA, Eneko. (2015). Criptografía: simétrica, asimétrica e híbrida. Obtenido de https://enekoamieva.com/criptografia-simetrica-asimetrica-e-hibrida/

ANGEL ANGEL, José de Jesús. (2005). Advanced Encryption Standard. México. Recuperado de www.criptored.upm.es/guiateoria/gt_m117i.htm

ARRIAZU SANCHEZ, Jorge. (1999) Descripción del Algoritmo DES, disponible en: https://www.academia.edu/15633436/Descripción_del_algoritmo_DES_Data_Encryption_Standard

ALFONSO BELTRAN, Julián Ignacio. (2015). Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. Recuperado de https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1

CÁMARA DE COMERCIO DE BOGOTÁ. ¿Qué no es una firma digital? Disponible en línea: http://www.ccb.org.co/contenido/contenido.aspx?catID=107&conID=5087

CANTO NÚÑEZ, Emily. (Oct 28, 2016), ¿Qué es finalmente la criptografía y por qué es importante? Disponible en: https://iq.intel.la/que-es-finalmente-la-criptografia-y-por-que-es-importante/

ELDINERO (2016). Firma digital. Recuperado de https://www.eldinero.com.do/20543/camara-de-comercio-presenta-al-mercado-certificado-de-firma-digital/

DALTABUIT, Enrique. (2015). Consideraciones sobre la Seguridad de la Información Digital. Obtenido de https://www.amazon.com/Consideraciones-Seguridad-Informaci%C3%B3n-Digital-Spanish-ebook/dp/B00VVQIUZO/ref=sr_1_5?qid=1569631498&refinements=p_27%3AEnrique+Daltabuit&s=digital-text&sr=1-5&text=Enrique+Daltabuit#reader_B00VVQIUZO

DÍAZ, Gabriel. MUR, Francisco. SAN CRISTÓBAL, Elio. (2004). Seguridad en las comunicaciones y en la información. Recuperado de: https://www.casadellibro.com/ebook-seguridad-en-las-comunicaciones-y-en-la-informacion-ebook/9788436247893/2004015

DUARTE, Eugenio. (2014). Mejores herramientas para cifrado de información de OpenSource. Recuperado de http://blog.capacityacademy.com/2014/10/20/ las-8-mejores- herramientas-de-cifrado-de-información/

LLANOS, Julia. MD5: vulnerabilidades y evoluciones (y II). Disponible en línea: http://blog.elevenpaths.com/2013/11/md5-vulnerabilidades-y-evoluciones-y-ii.html

ENCRIPTADOS, (Nov 18, 2011), La criptografía en la actualidad, disponible en: https://encriptados.wordpress.com/2011/11/18/la-criptografia-en-la-actualidad/

DIAZ DE SOLIZ, Juan. (2013) ESET Security Report, Cifrado de la información. Recuperado de http://www. eset-la.com/centro-amenazas/descarga/Latinoamérica-2013/

FÚSTER SABATER, Amparo. MONTOYA VITINI, Faus. DE LA GUÍA MARTÍNEZ, Dolores. HERNANDEZ ENCINAS, Luis. (2004) Técnicas criptográficas de Protección de Datos. Editorial RA-MA, Madrid, España, disponible en: http://www.ra-ma.es/libros/TECNICAS-CRIPTOGRAFICAS-DE-PROTECCION-DE-DATOS-3-EDICION-ACTUALIZADA-INCLUYE-CD-ROM/124/978-84-7897-594-5

GÁLVEZ ZARAZAÚ, Javier. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles. México D.F. Obtenido de http://148.204.210.201/tesis/1404316762511NPGMTesisAn.pdf.

GÓMEZ VIETES, Álvaro. (2007). Enciclopedia de la Seguridad Informática, Obtenido de https://books.google.com.pe/books/about/Enciclopedia_de_la_seguridad_inform %C3%A1tic.html?id=MQ_kOgAACAAJ &redir_esc=y

GUTIÉRREZ, Pedro. (2013). Tipos de criptografía. Recuperado de https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia- simetrica-asimetrica-e-hibrida

HERCIGONJA, Zoran. DRUGA, Gimnazija. (2016). Análisis Comparativo de Algoritmos Criptográficos. Revista Internacional de TECNOLOGÍA DIGITAL Y ECONOMÍA. Obtenido de https://hrcak.srce.hr/177886

HERRERA, Eduard. (2014). Principios fundamentales que se busca proteger con la seguridad informática - CIA. Recuperado de https://informaticaseguraupc.wordpress.Com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/

LITWAK, Noelia Desiree. ESCALANTE, Jaquelina Edith, (2004) Seguridad informatica y criptografia, Recuperado de: http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf

LUCENA LOPEZ, Manuel José. (2014) Criptografía y Seguridad en Computadores. Recuperado de http://index-of.co.uk/INFOSEC/84.criptografia-y-seguridad-en-computadores.pdf

MARRERO TRAVIESO, Yran. (2003). La Criptografía como elemento de la seguridad informática. ACIMED, 11(6) Recuperado en 05 de marzo de 2019, de

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012&lng=es&tlng=es.

MORENO, Blanca. (2015). Tipos de Criptografía. Obtenido de https://plus.google.com/111785202907101039542

MORENO, Johnny. (2012). Criptografía. Recuperado de https://morenojhonny.wordpress.com/ 2012/06/14/unidad-4-criptografia.

MOZILLA DEVELOPER NETWORK – MDN. Contraseñas Inseguras. Disponible en línea: https://developer.mozilla.org/es/docs/Seguridad/Contrase%C3%B1asInseguras

MUÑOZ, Alfonso. RAMIÓ AGUIRRE, Jorge. (2013). Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo RSA, disponible en: https://0xword.com/libros/36-libro-cifrado-comunicaciones-rsa.html

NFON, Advanced Encryption Standard, Recuperado de: https://www.nfon.com/es/acerca-de-nfon/recursos/glosario/advanced-encryption-standard/

OSAMA, Kashan. (2010). Implementing RC5 Encryption Algotrithm. Obtenido de https://www.amazon.co.uk/IMPLEMENTING-RC5-ENCRYPTION-ALGORIT HM-CONSULTATION/dp/3639243234

PACHECO, Federico. (2014). Criptografía. Recuperado de https://www.amazon.com/Criptograf%C3%ADa-Spanish-Pacheco-Federico-G/dp/9871949359

PADILLA HERNANDEZ, Javier Enrique. (Dic 9, 2014) Criptografía y Seguridad, Disponible en: http://ing.javierpadilla.over-blog.es/2014/12/criptografia-y-seguridad.html

PERAZA, Adarve. DIAZ, Levano. (2012). La Criptografía: "Una guerra de Piratas y Corsarios". Obtenido de https://egov.ufsc.br/portal/conteudo/la-criptograf %C3%ADa-una-guerra-de-piratas-y-corsarios

PEREZ, Simón. (2013). International Data Encryption Algorithm. Recuperado de https://sistemasumma.com/2010/09/14/algoritmo-de-encriptacion -idea/

PRIYADARSHINI, Patil. PARSHANT, Naranyakar., NARAYAN, DG. MEENA, SM. (2016). Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish. Publicada en http://www.sciencedirect.com/science/article/pii/S1877050916 001101

RAMIÓ AGUIRRE, Jorge. (2006). Seguridad Informática y Criptografía. Madrid, España: OxWord
Red Académica y de Investigación Española REDIRIS (2013). Criptología. Obtenido de http://www.rediris.es/ cert/doc/unixsec/node29.html

RODRÍGUEZ, Jaime. (2011). Tipos de violación a la seguridad informática. Obtenido de: http://wwwcomputacion95.blogspot.com/2011/04/tipos-de-violacion-la-seguridad.html

SANTANA OSORIO, Adriana. (2014). Formas de romper la seguridad. Obtenido de http://criptografias utp.blogspot.pe
Santana, A. (2012). Diseño de un algoritmo de cifrado de clave privada. (Tesis de Pregrado). Universidad Nacional Autónoma de México. México.

SÁNCHEZ ARRIAZU, Jorge. Descripción del Algoritmo DES. España, 1999. Disponible en: https://www.academia.edu/15633436/Descripci %C3%B3n_del_algoritmo_DES_Data_Encryption_Standard

SHIKATA, Junji. (2009). "Unconditional security". Obtenido de https://link.springer.com/chapter/10.1007/978-3-642-02002-5_7

TECNOLOGÍA & INFORMÁTICA, ¿Qué es la Criptografia? Disponible en: https://tecnologia-informatica.com/que-es-la-criptografia/

URAZAN BUENO, Rohwinzon. QUINTERO ECHEVERRY, José Manuel. Criptografía y Cifrado, disponible en: https://encriptados.files.wordpress.com/2011/11/criptografia.pdf

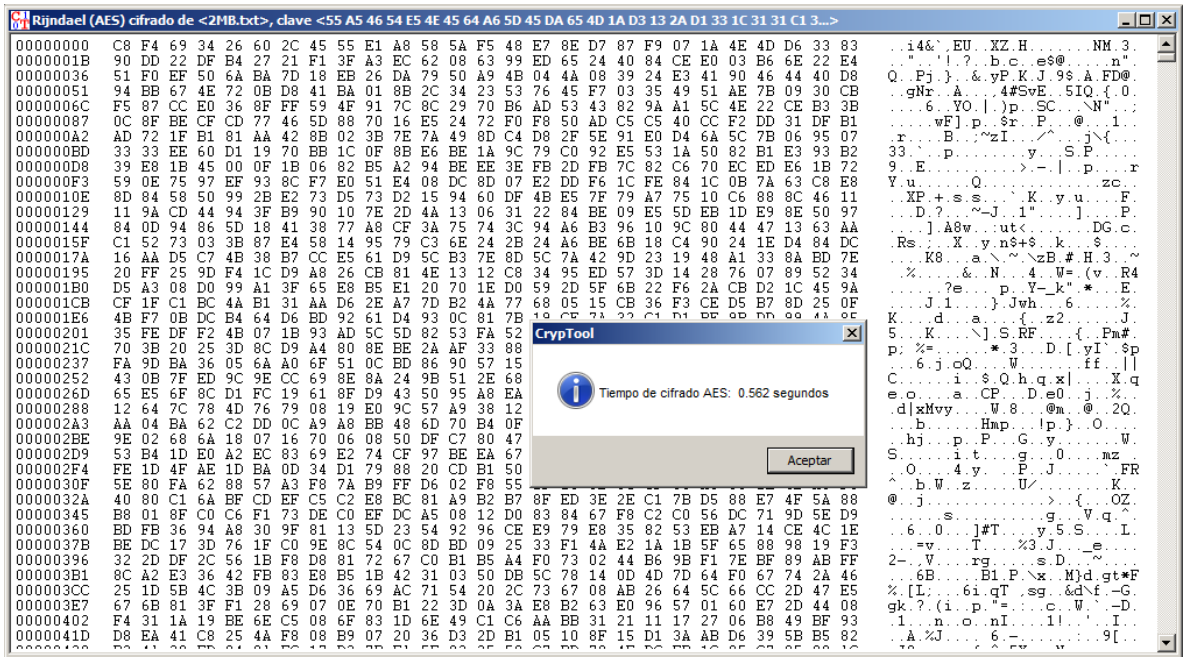
VILLEGAS GÓMEZ, Roberto. (2009). Comparativa de Seguridad de Algoritmos de cifrado Asimétrico.
México D.F. Recuperado de http://hdl.handle.net/12345 6789/8613.

WIKIPEDIA, (Julio 2018) Historia de la criptografía, recuperado de: https://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa

XIFRÉ SOLANA, Patricia. (2009). Antecedentes y perspectivas de estudio en historia de la criptografía. Universidad Carlos III de Madrid. Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/6173/PFC_Patricia_Xifre_Solana.pdf?sequence=1&isAllowed=y

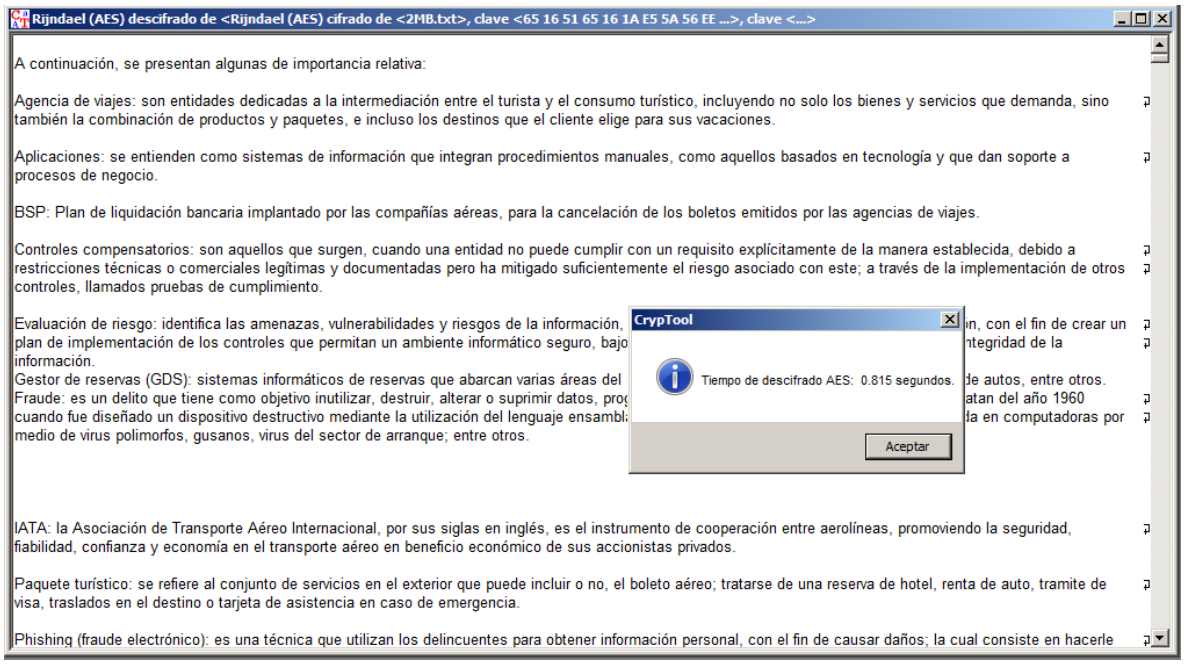
ANEXO A. CIFRADO Y DESCIFRADO AES A ARCHIVO DE 2048 KB

A1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

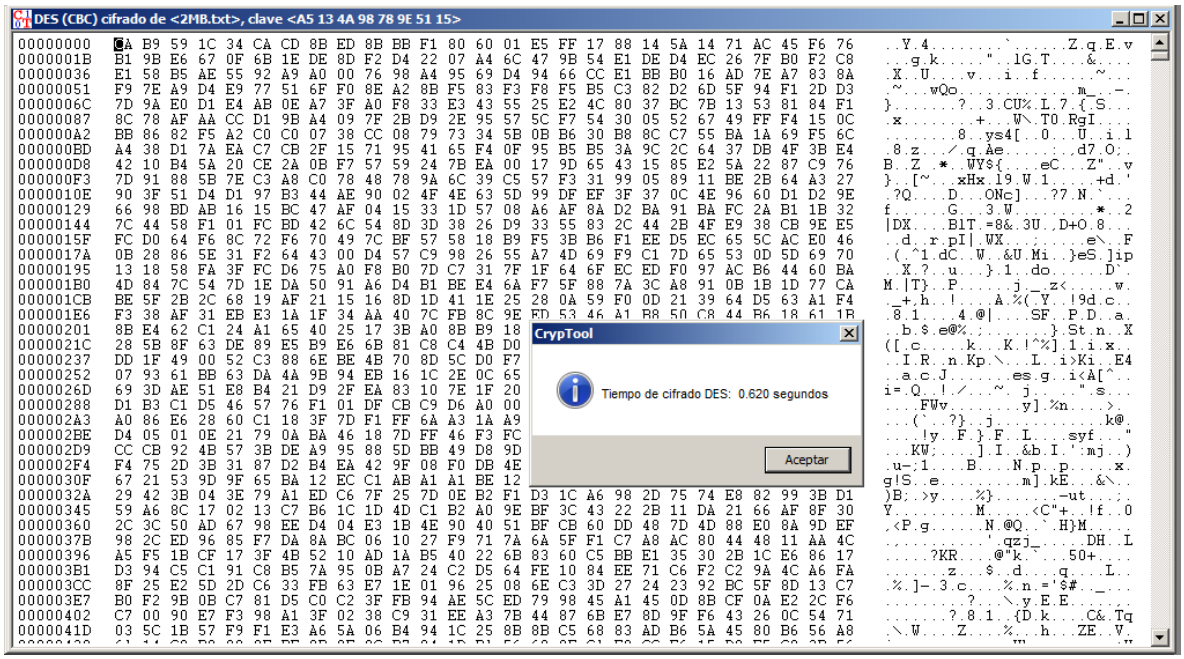
A2. Tiempo de descifrado.



Fuente: autor, herramienta cryptool.

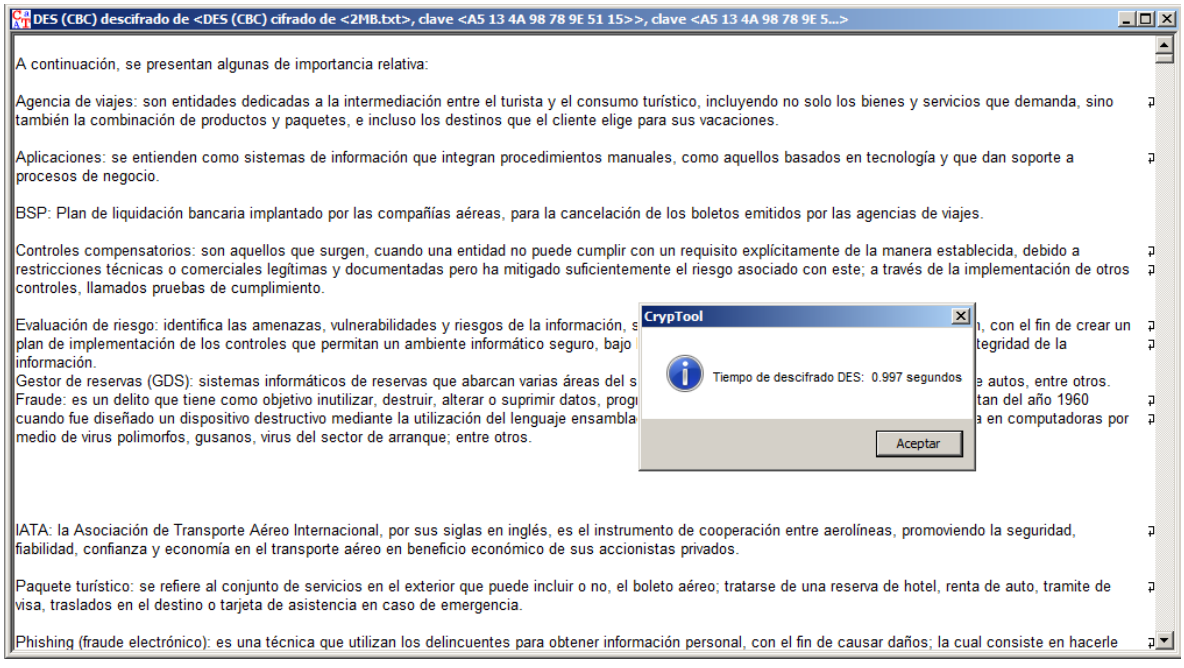
ANEXO B. CIFRADO Y DESCIFRADO DES CON ARCHIVO DE 2048 KB

B1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

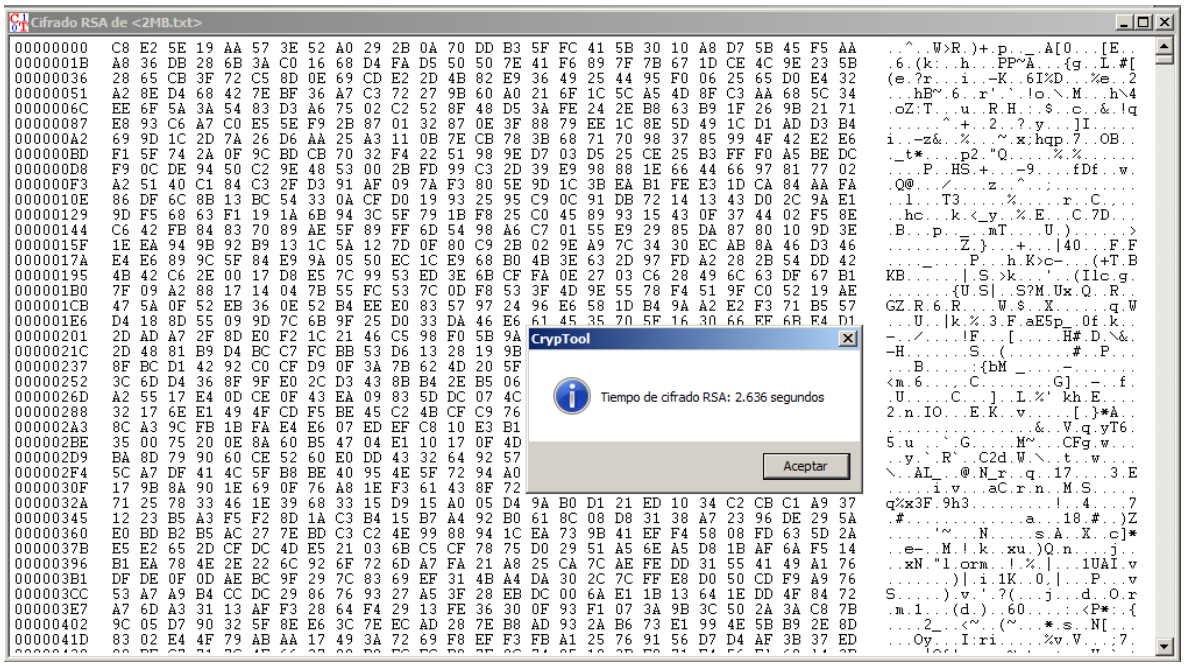
B2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

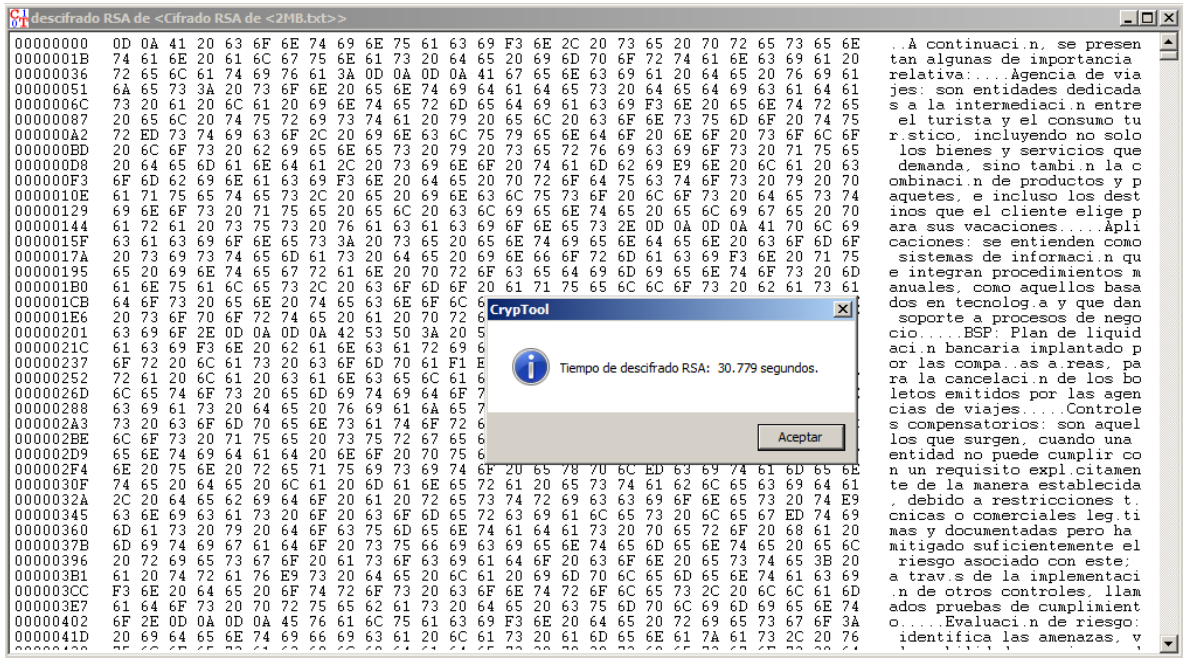
ANEXO C. CIFRADO Y DESCIFRADO RSA CON ARCHIVO DE 2048 KB

C1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

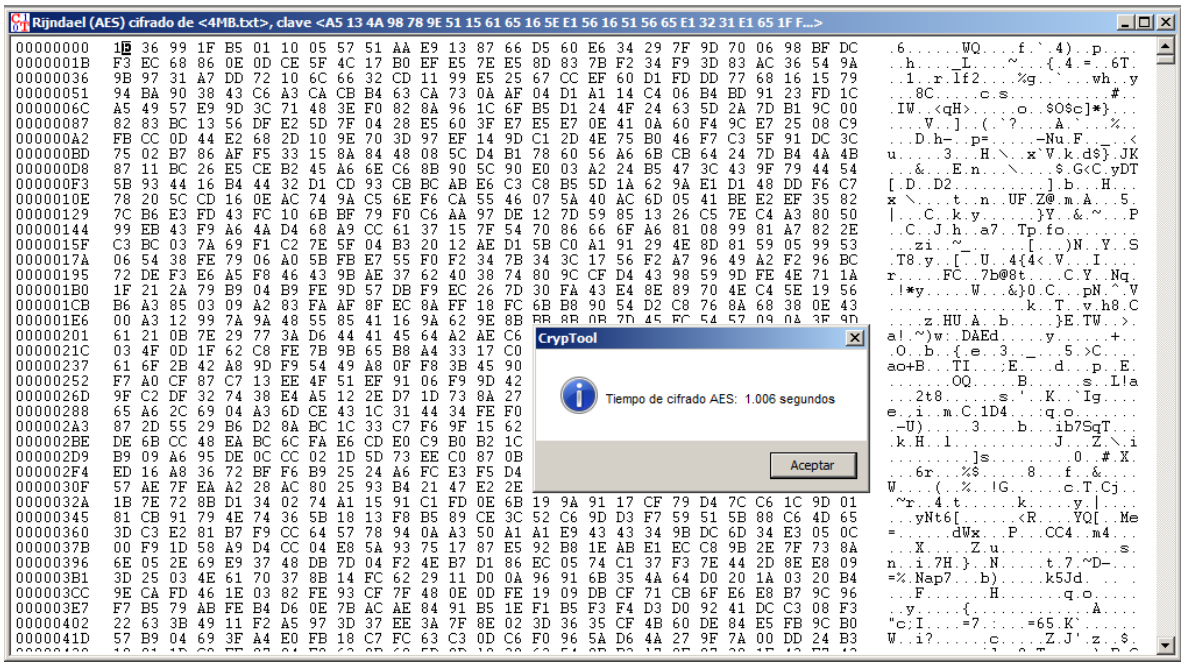
C2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

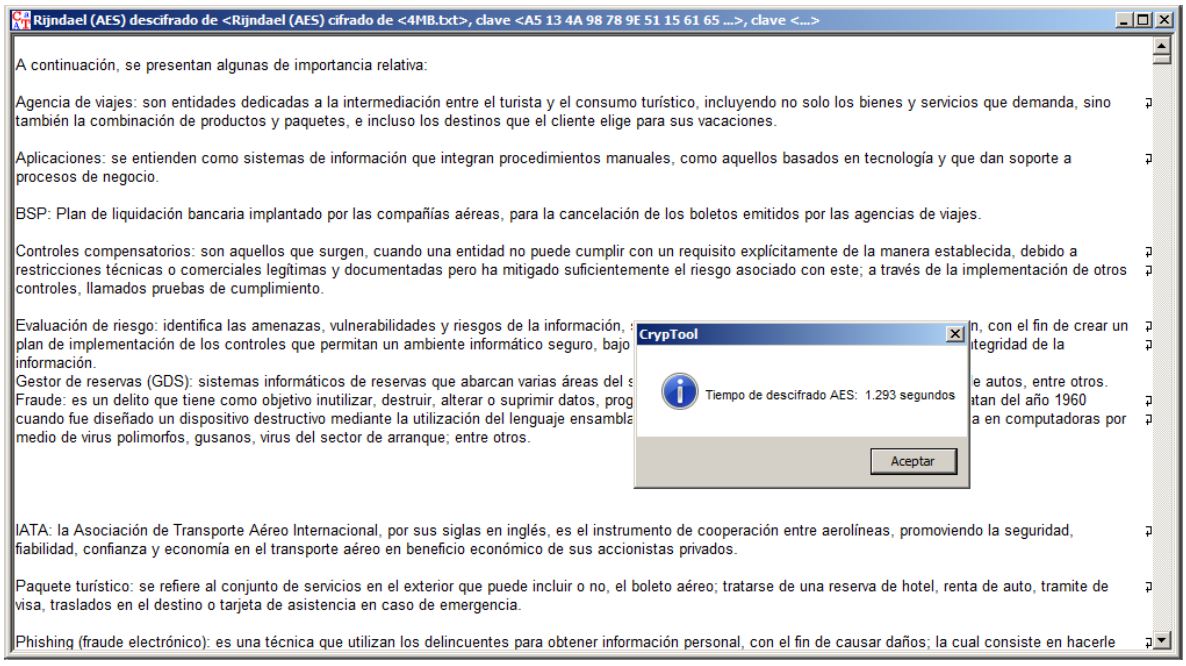
ANEXO D. CIFRADO Y DESCIFRADO AES DE ARCHIVO DE 4096 KB

D1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

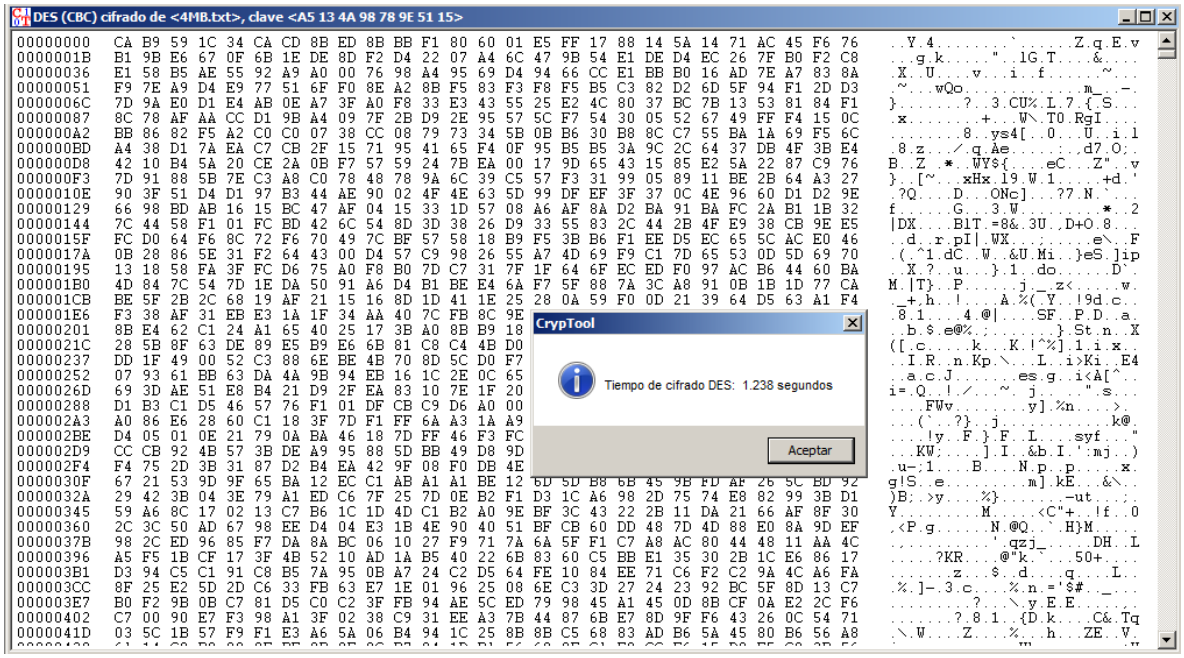
D2. Tiempo de descifrado.



Fuente: autor, herramienta cryptool.

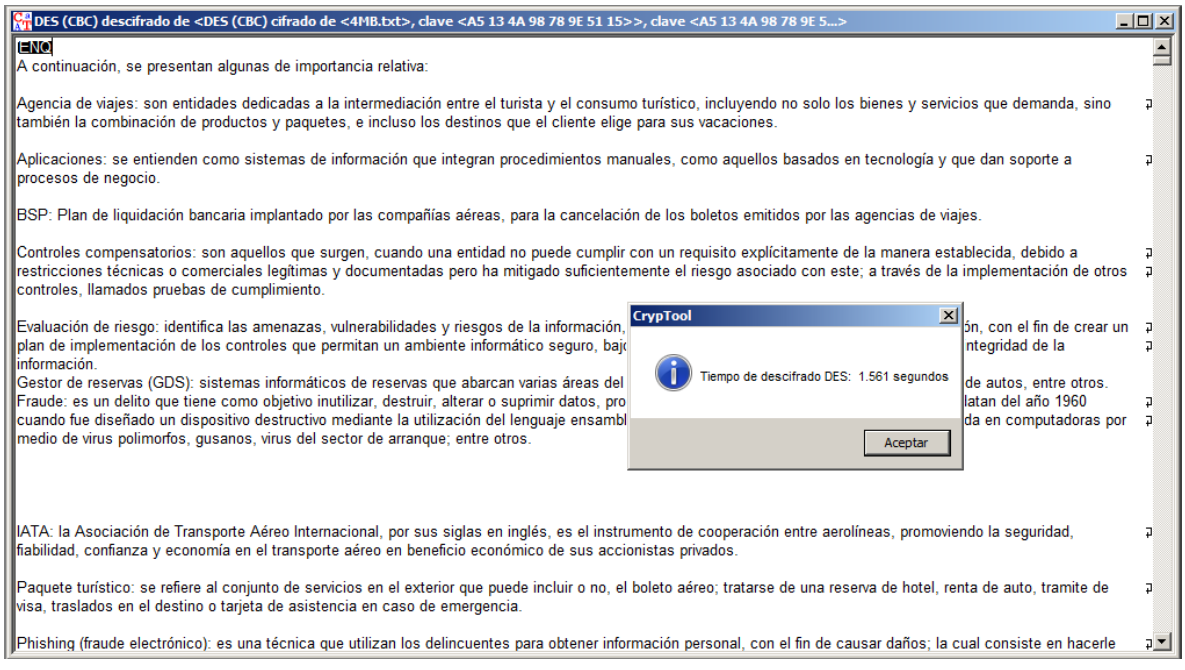
ANEXO E. CIFRADO Y DESCIFRADO DES DE ARCHIVO DE 4096 KB

E1. Tiempo de Cifrado



Fuente: autor, herramienta cryptool.

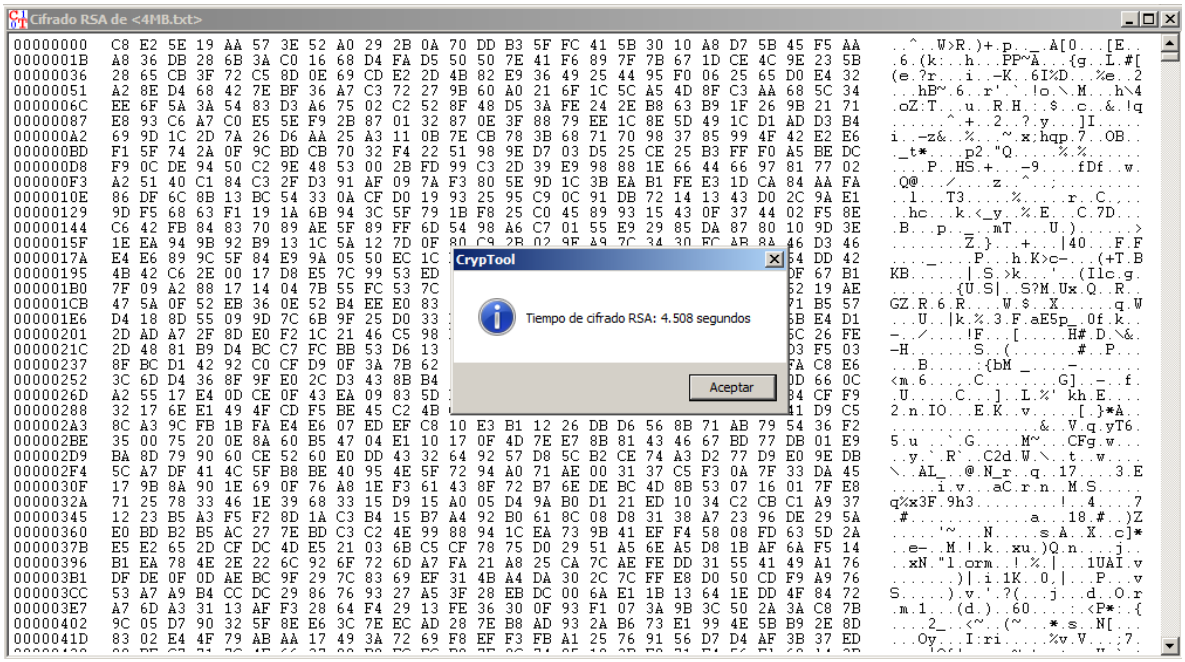
E2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

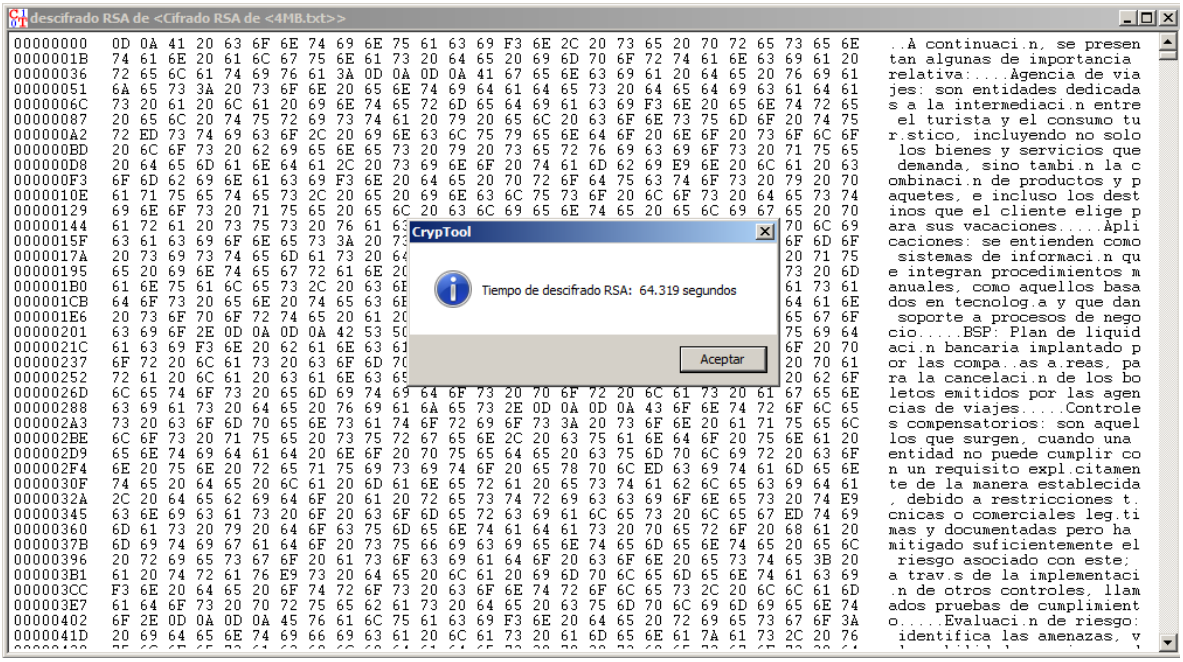
ANEXO F. CIFRADO Y DESCIFRADO RSA DE ARCHIVO DE 4096 KB

F1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

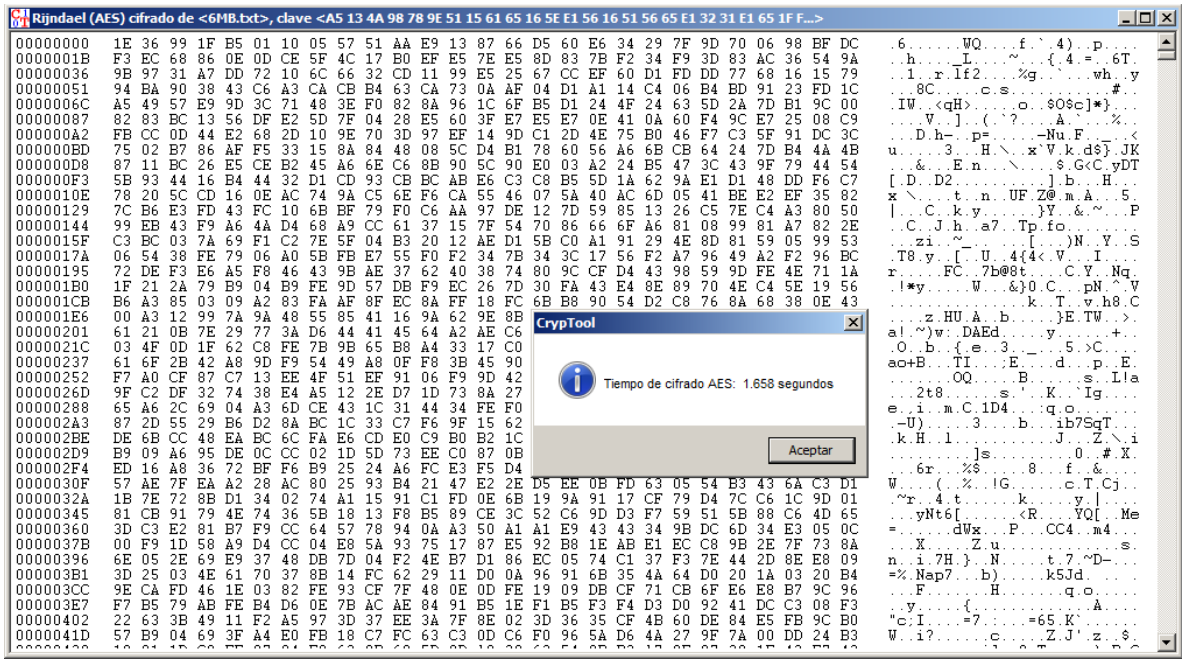
F2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

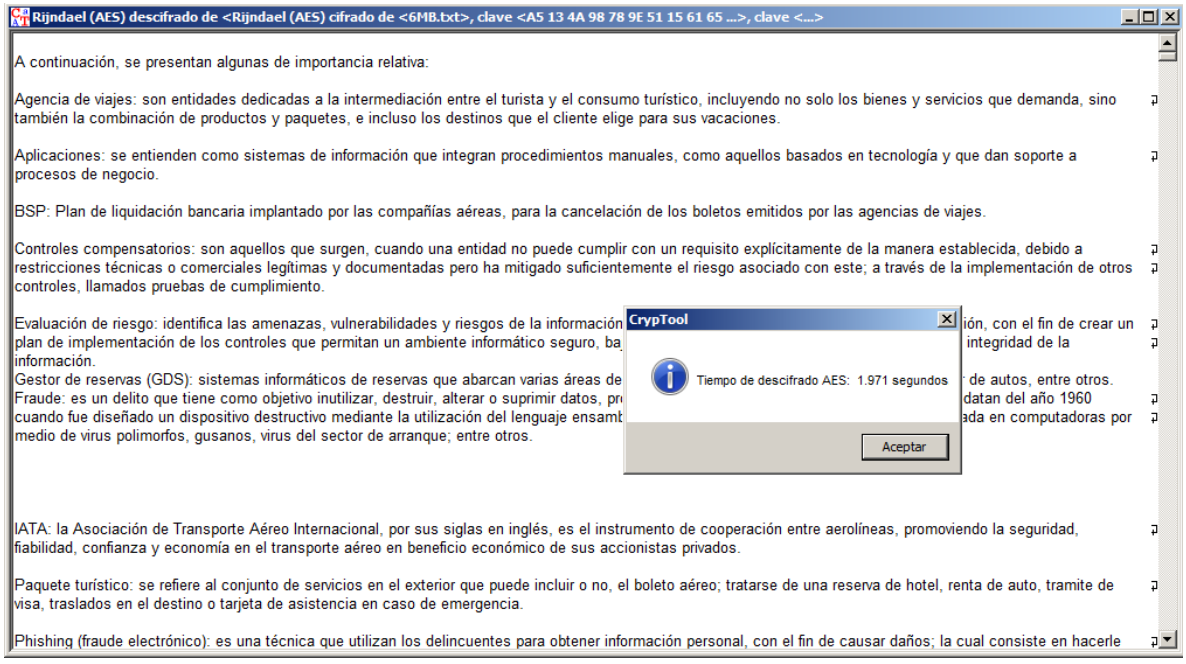
ANEXO G. CIFRADO Y DESCIFRADO AES DE ARCHIVO DE 6144 KB

G1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

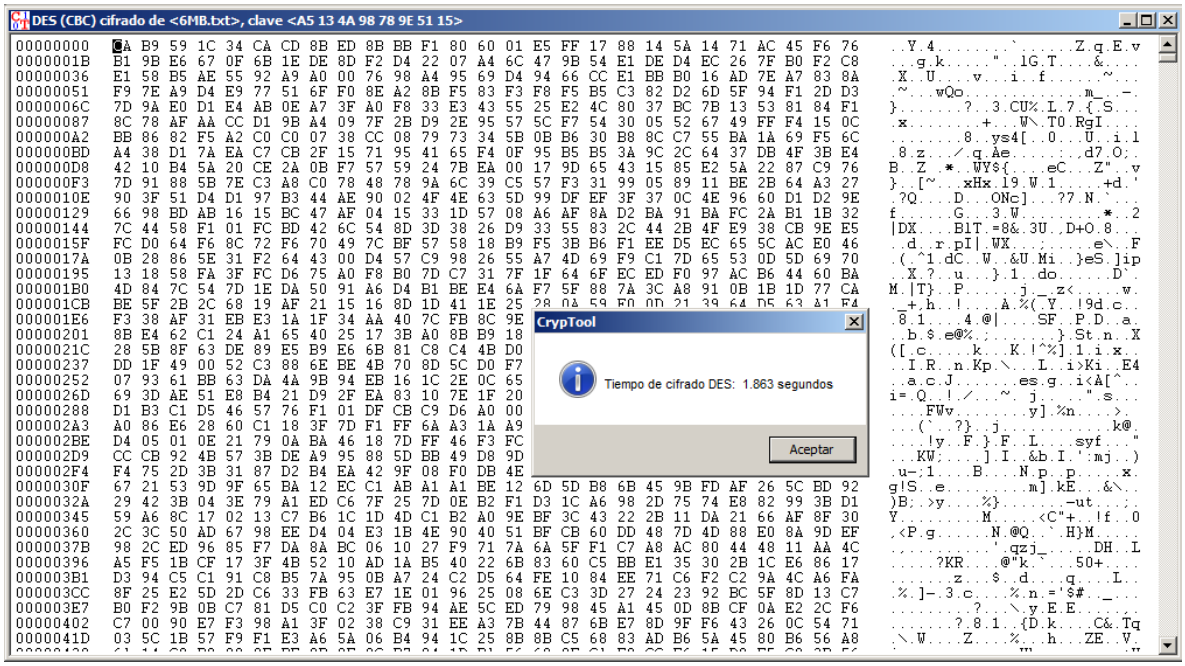
G2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

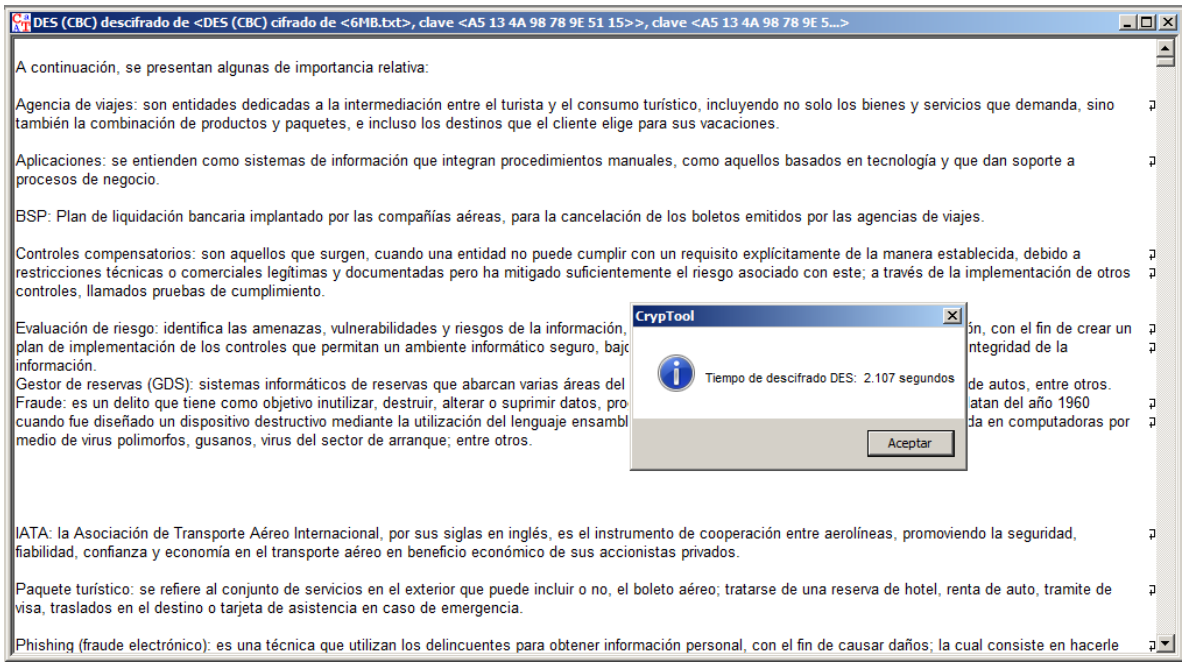
ANEXO H. CIFRADO Y DESCIFRADO DES DE ARCHIVO DE 6144 KB

H1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

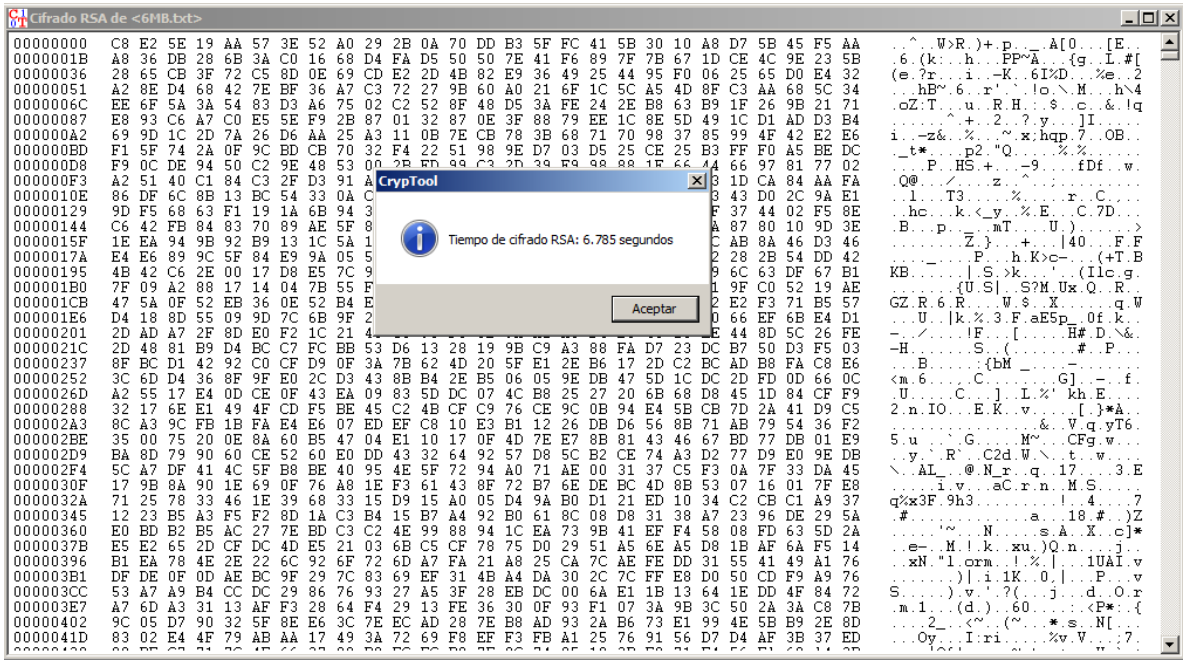
H2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

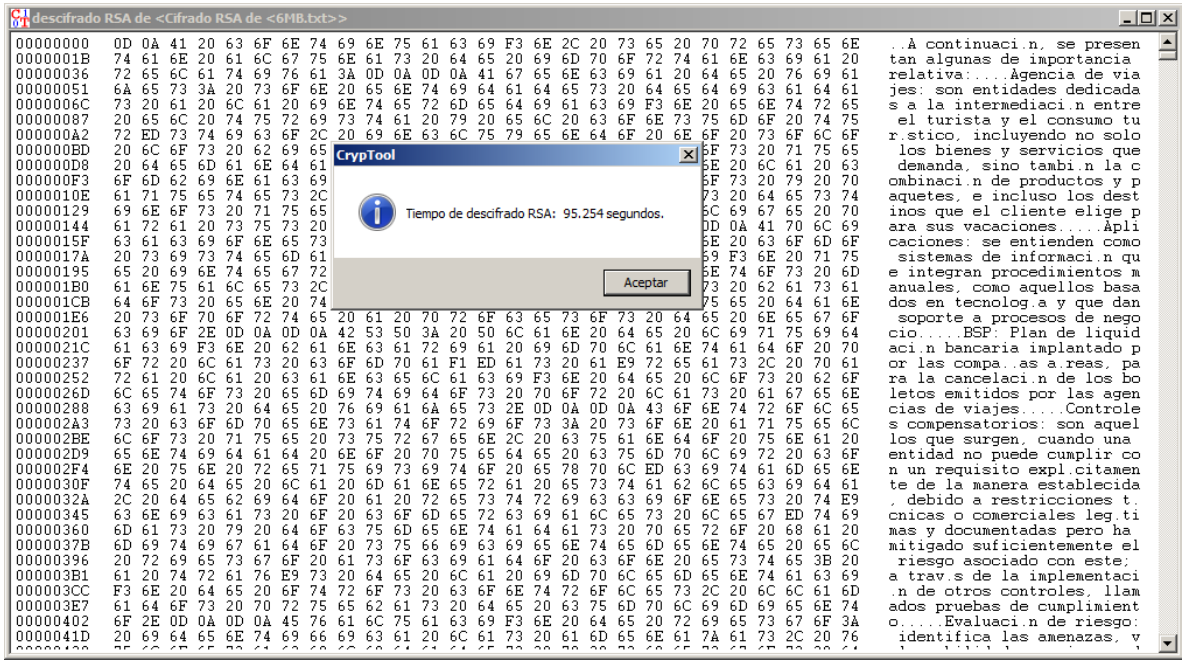
ANEXO I. CIFRADO Y DESCIFRADO RSA DE ARCHIVO DE 6144 KB

I1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

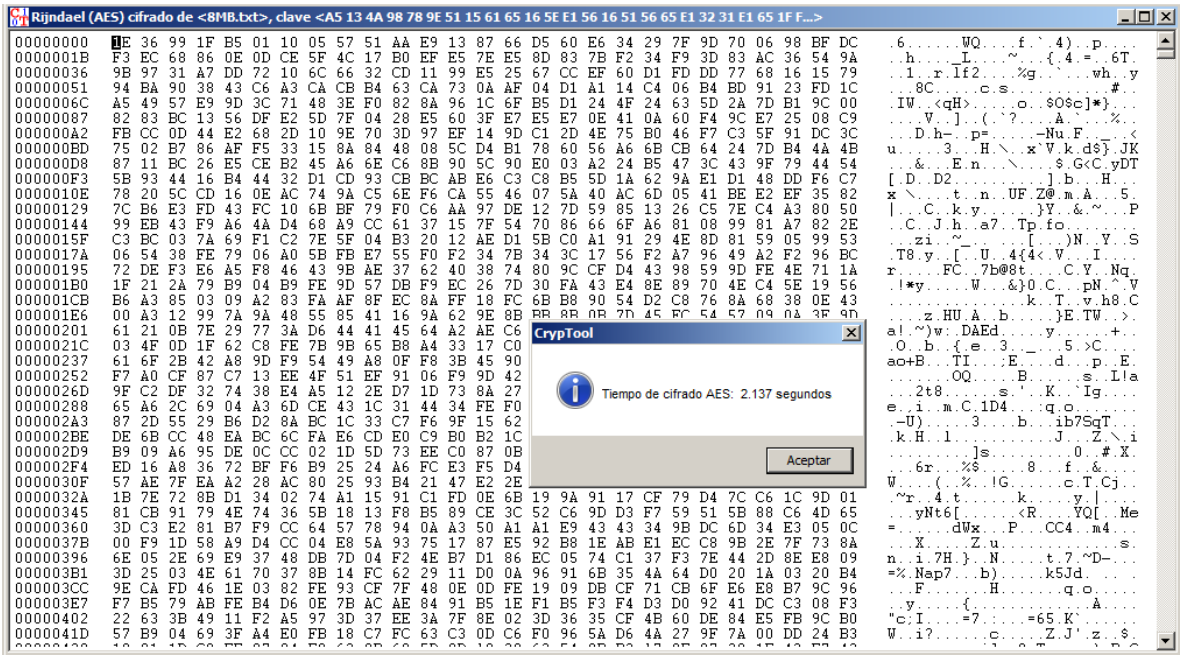
I2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

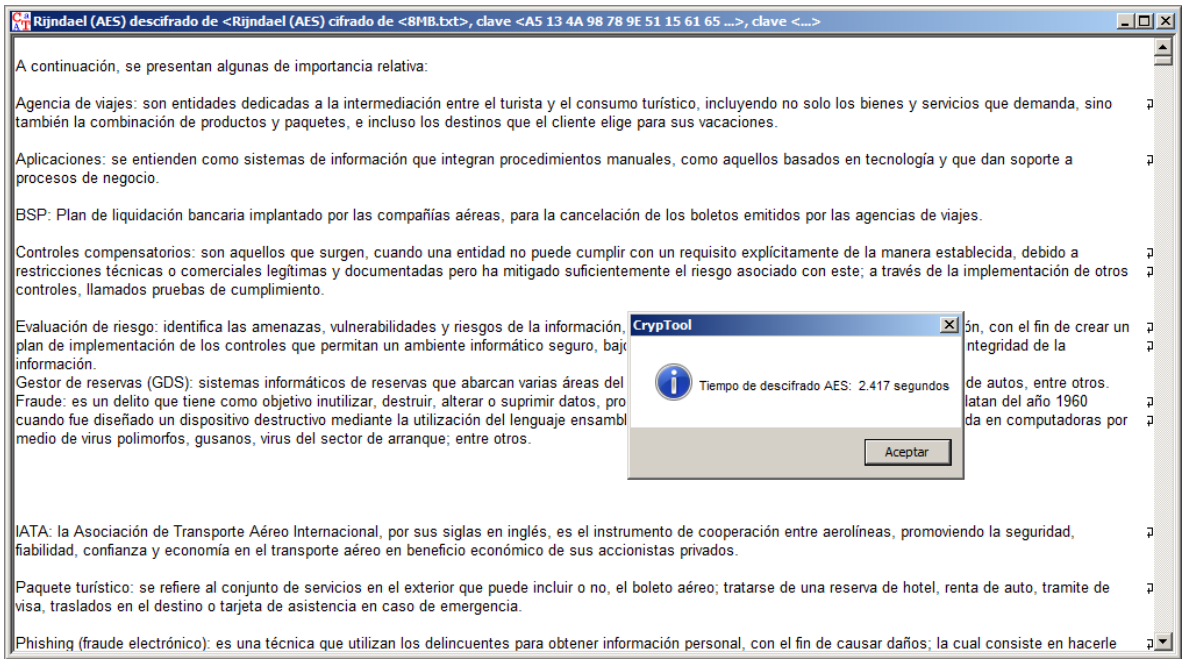
ANEXO J. CIFRADO Y DESCIFRADO AES DE ARCHIVO DE 8192 KB

J1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

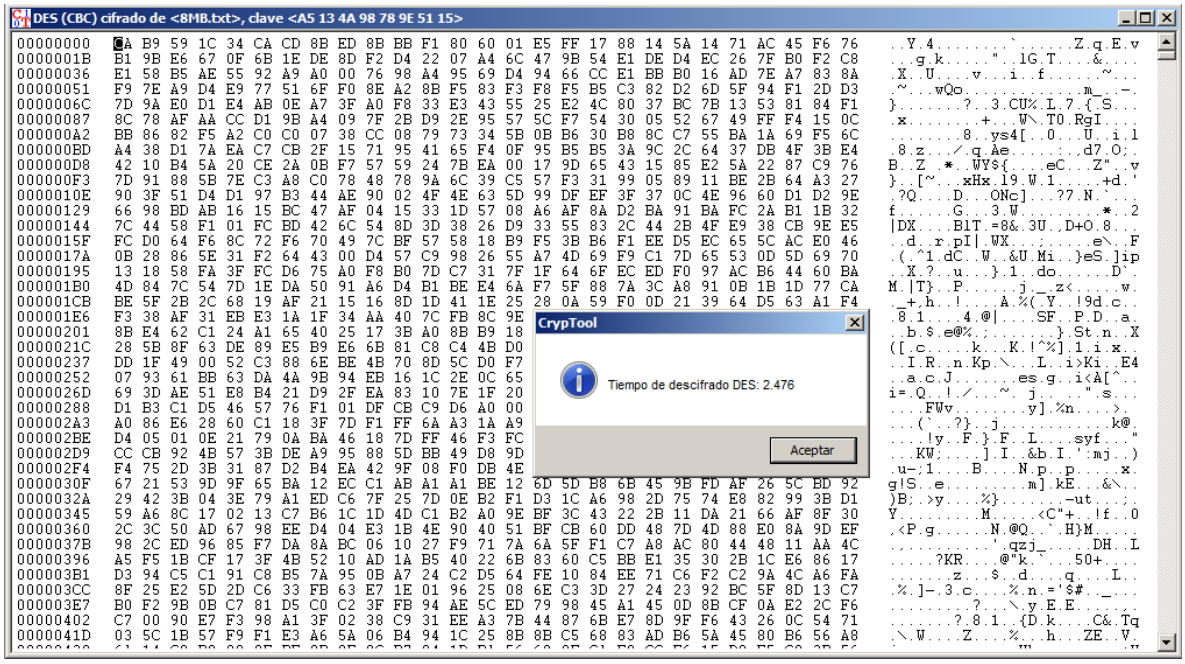
J2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

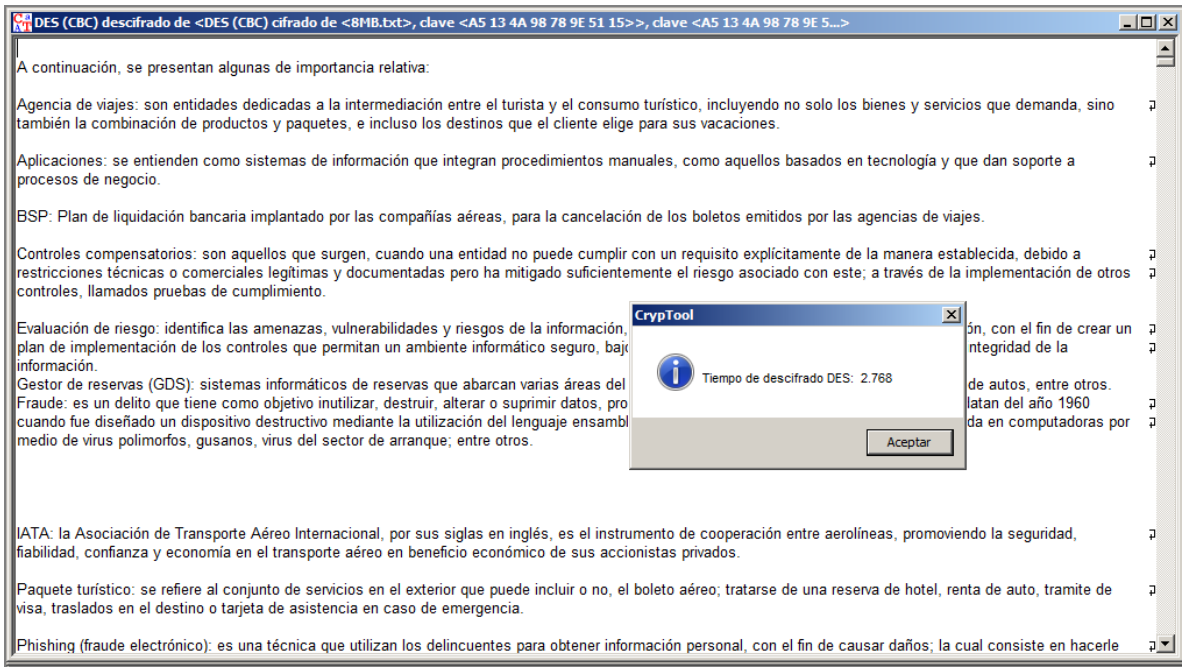
ANEXO K. CIFRADO Y DESCIFRADO DES DE ARCHIVO DE 8192 KB

K1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

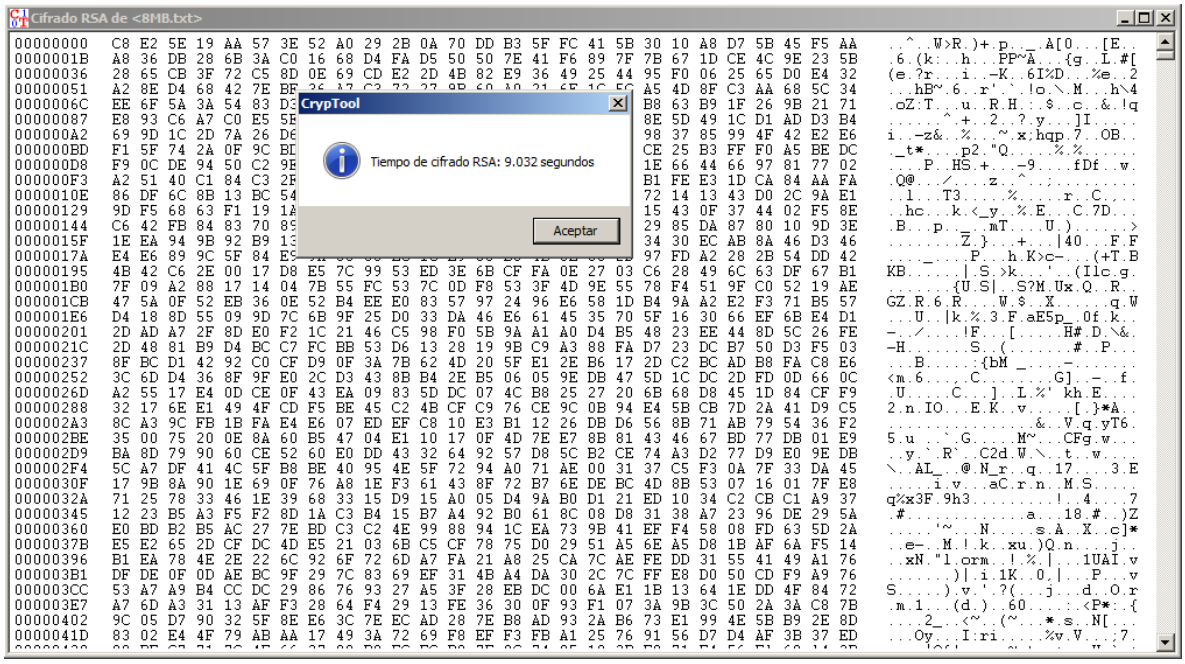
K2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

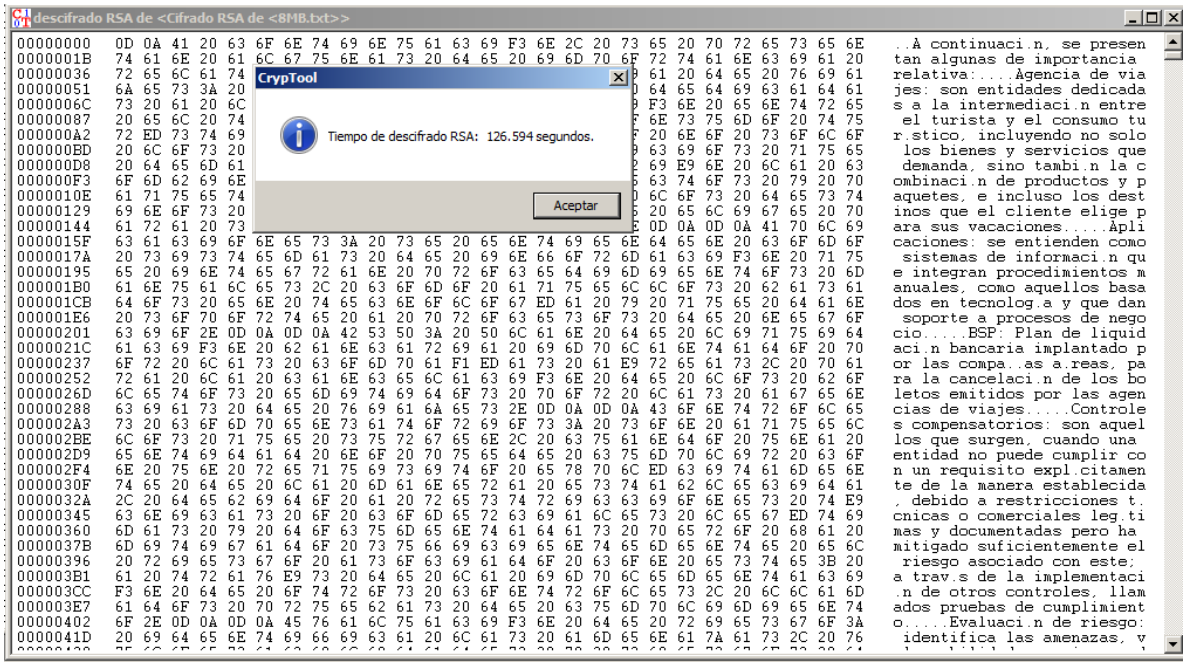
ANEXO L. CIFRADO Y DESCIFRADO RSA DE ARCHIVOS DE 8192 KB

L1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

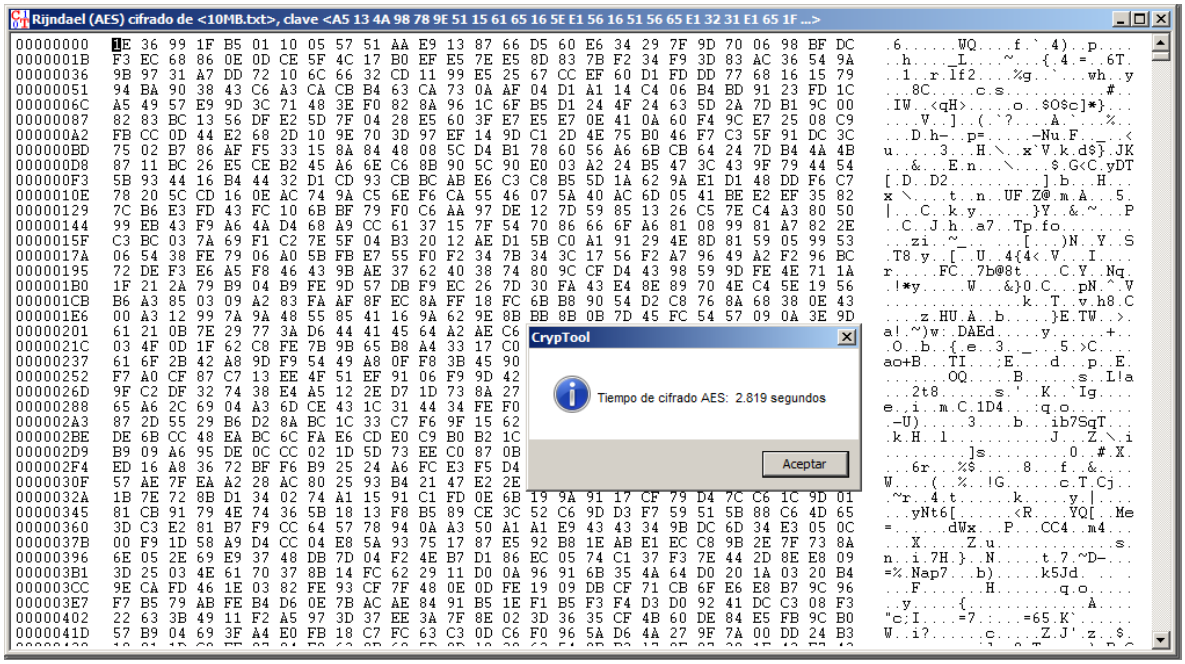
L2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

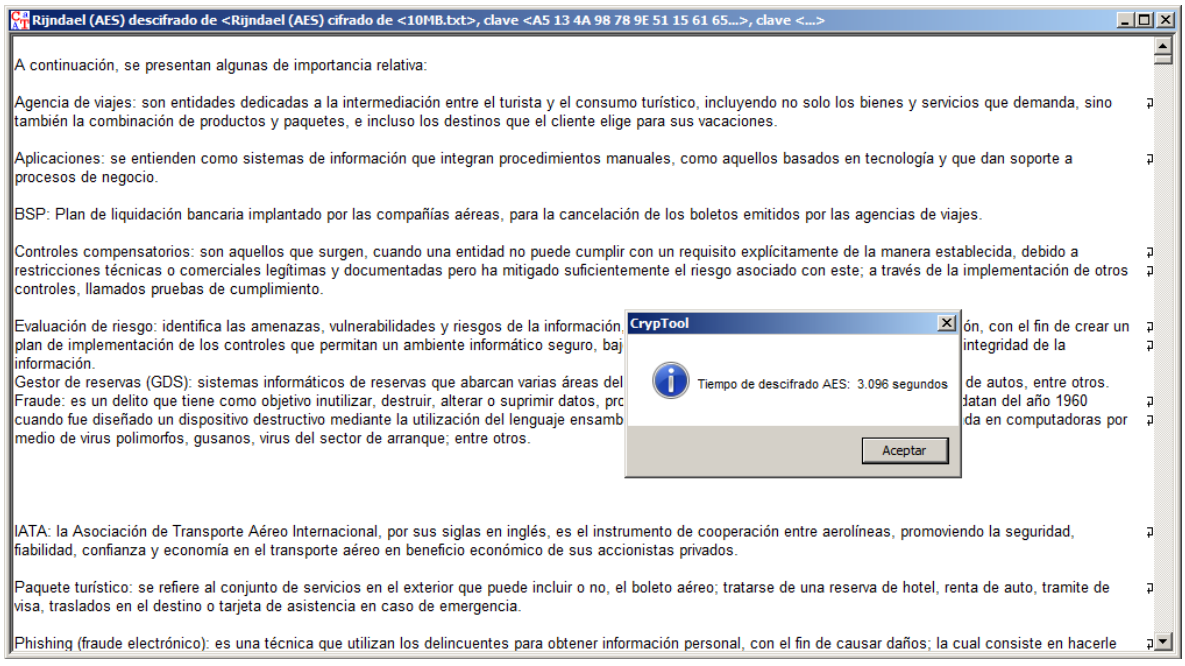
ANEXO M. CIFRADO Y DESCIFRADO AES DE ARCHIVO DE 10240 KB

M1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

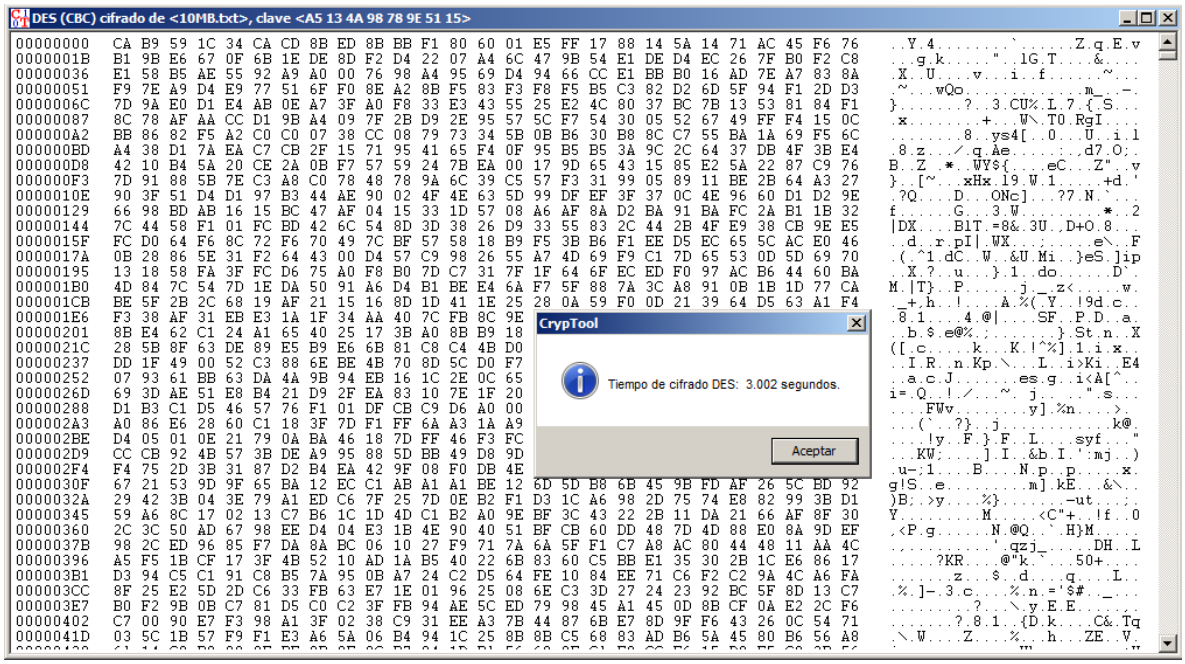
M2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

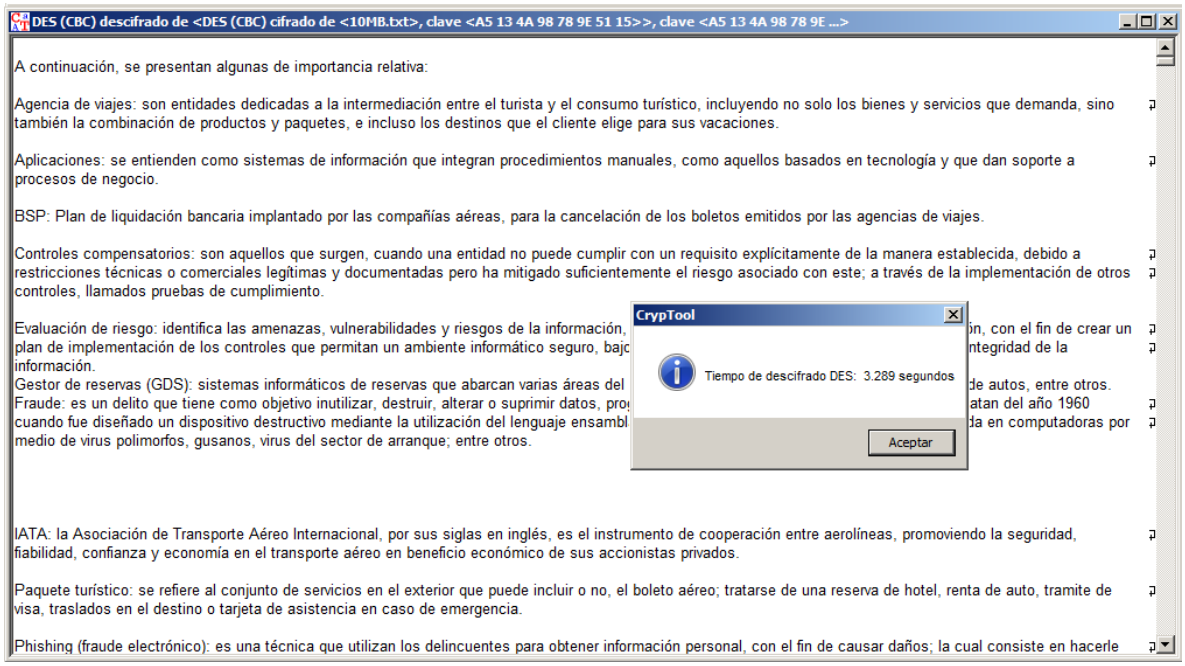
ANEXO N. CIFRADO Y DESCIFRADO DES DE ARCHIVO DE 10240 KB

N1. Tiempo de cifrado.



Fuente: autor, herramienta cryptool.

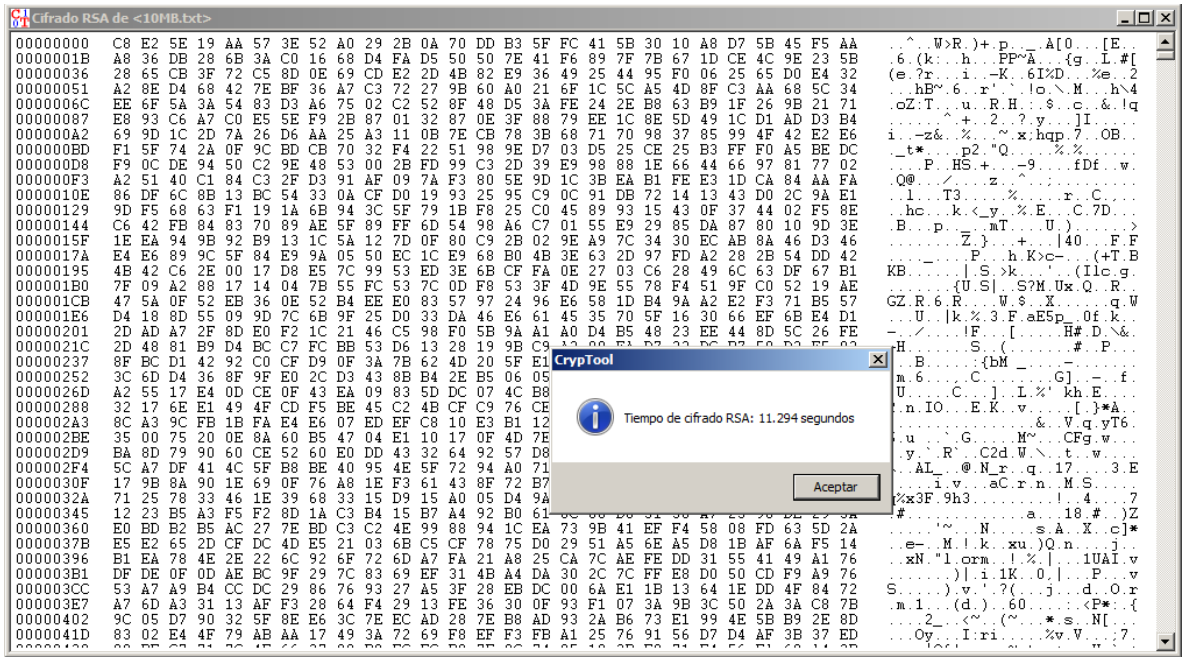
N1. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

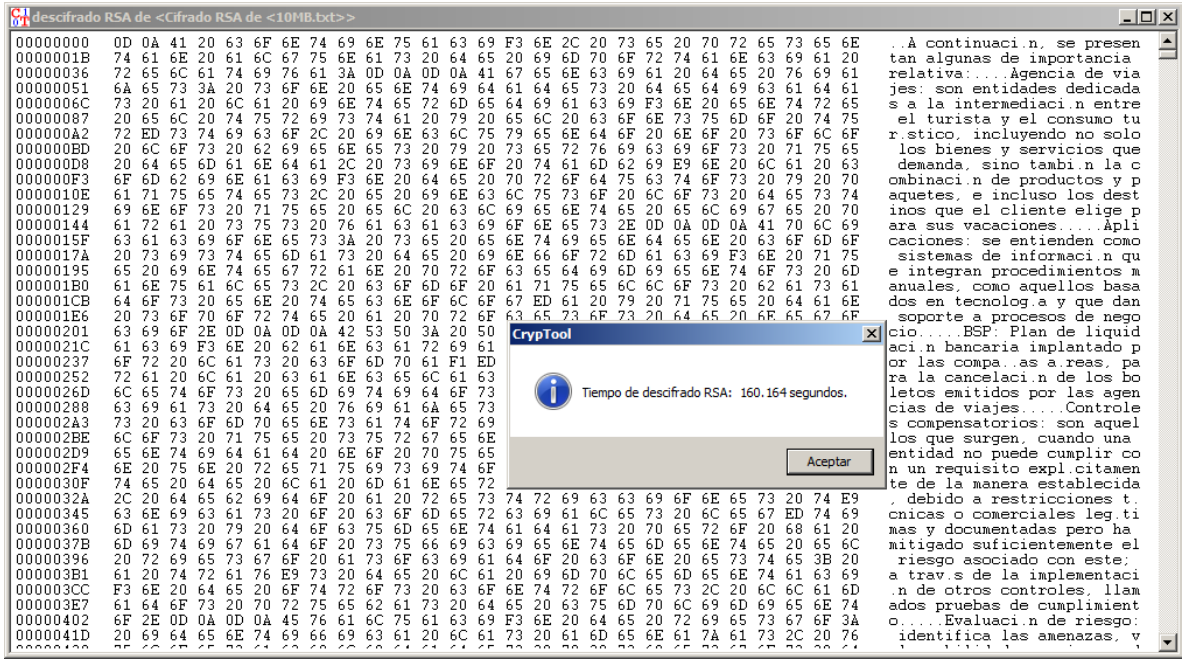
ANEXO O. CIFRADO Y DESCIFRADO RSA DE ARCHIVO DE 10240 KB

O1. Tiempo de cifrado



Fuente: autor, herramienta cryptool.

O2. Tiempo de descifrado



Fuente: autor, herramienta cryptool.

ANEXO P FORMATO RAE

Fecha de Realización: 20/05/2019

Título: Comparación de métodos criptográficos para la seguridad informática

Autor: SERRATO, Hernán.

Palabras Claves: Criptografía, Criptología, Cifrado, Firma digital. Claves, seguridad.

Descripción: Monografía realizada como opción de grado para optar por el título de especialista en seguridad informática.

FUENTES PRINCIPALES

ALCOCER y MARTINEZ, Mariano. (2006). Criptografía Española. Recuperado de http://www.cervantesvirtual.com/nd/ark:/59851/bmcqr5g8

AMIEVA, Eneko. (2015). Criptografía: simétrica, asimétrica e híbrida. Obtenido de https://enekoamieva.com/criptografia-simetrica-asimetrica-e-hibrida/

ANGEL ANGEL, José de Jesús. (2005). Advanced Encryption Standard. México. Recuperado de www.criptored.upm.es/guiateoria/gt_m117i.htm

ARRIAZU SANCHEZ, Jorge. (1999) Descripción del Algoritmo DES, disponible en: https://www.academia.edu/15633436/Descripción_del_algoritmo_DES_Data_Encryption_Standard

ALFONSO BELTRAN, Julián Ignacio. (2015). Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. Recuperado de https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1

CÁMARA DE COMERCIO DE BOGOTÁ. ¿Qué no es una firma digital? Disponible en línea: http://www.ccb.org.co/contenido/contenido.aspx?catID=107&conID=5087

CANTO NÚÑEZ, Emily. (Oct 28, 2016), ¿Qué es finalmente la criptografía y por qué es importante? Disponible en: https://iq.intel.la/que-es-finalmente-la-criptografia-y-por-que-es-importante/

ELDINERO (2016). Firma digital. Recuperado de https://www.eldinero.com.do/20543/camara-de-comercio-presenta-al-mercado-

certificado-de-firma-digital/
DALTABUIT, Enrique. (2015). Consideraciones sobre la Seguridad de la Información Digital. Obtenido de https://www.amazon.com/Consideraciones-Seguridad-Informaci%C3%B3n-Digital-Spanish-ebook/dp/B00VVQIUZO/ref=sr_1_5?qid=1569631498&refinements=p_27%3AEnrique+Daltabuit&s=digital-text&sr=1-5&text=Enrique+Daltabuit#reader_B00VVQIUZO

DÍAZ, Gabriel. MUR, Francisco. SAN CRISTÓBAL, Elio. (2004). Seguridad en las comunicaciones y en la información. Recuperado de: https://www.casadellibro.com/ebook-seguridad-en-las-comunicaciones-y-en-la-informacion-ebook/9788436247893/2004015

DUARTE, Eugenio. (2014). Mejores herramientas para cifrado de información de OpenSource. Recuperado de http://blog.capacityacademy.com/2014/10/20/ las-8-mejores- herramientas-de-cifrado-de-información/

LLANOS, Julia. MD5: vulnerabilidades y evoluciones (y II). Disponible en línea: http://blog.elevenpaths.com/2013/11/md5-vulnerabilidades-y-evoluciones-y-ii.html

ENCRIPTADOS, (Nov 18, 2011), La criptografía en la actualidad, disponible en: https://encriptados.wordpress.com/2011/11/18/la-criptografia-en-la-actualidad/

DIAZ DE SOLIZ, Juan. (2013) ESET Security Report, Cifrado de la información. Recuperado de http://www. eset-la.com/centro-amenazas/descarga/Latinoamérica- 2013/

FÚSTER SABATER, Amparo. MONTOYA VITINI, Faus. DE LA GUÍA MARTÍNEZ, Dolores. HERNANDEZ ENCINAS, Luis. (2004) Técnicas criptográficas de Protección de Datos. Editorial RA-MA, Madrid, España, disponible en: http://www.ra-ma.es/libros/TECNICAS-CRIPTOGRAFICAS-DE-PROTECCION-DE-DATOS-3-EDICION-ACTUALIZADA-INCLUYE-CD-ROM/124/978-84-7897-594-5

GÁLVEZ ZARAZAÚ, Javier. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles. México D.F. Obtenido de

http://148.204.210.201/tesis/1404316762511NPGMTesisAn.pdf.

GÓMEZ VIETES, Álvaro. (2007). Enciclopedia de la Seguridad Informática, Obtenido de https://books.google.com.pe/books/about/Enciclopedia_de_la_seguridad_inform%C3%A1tic.html?id=MQ_kOgAACAAJ &redir_esc=y

GUTIÉRREZ, Pedro. (2013). Tipos de criptografía. Recuperado de https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simétrica-asimétrica-e-hibrida

HERCIGONJA, Zoran. DRUGA, Gimnazija. (2016). Análisis Comparativo de Algoritmos Criptográficos. Revista Internacional de TECNOLOGÍA DIGITAL Y ECONOMÍA. Obtenido de https://hrcak.srce.hr/177886

HERRERA, Eduard. (2014). Principios fundamentales que se busca proteger con la seguridad informática - CIA. Recuperado de https://informaticaseguraupc.wordpress.Com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/

LITWAK, Noelia Desiree. ESCALANTE, Jaquelina Edith, (2004) Seguridad informática y criptografía, Recuperado de: http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf

LUCENA LOPEZ, Manuel José. (2014) Criptografía y Seguridad en Computadores. Recuperado de http://index-of.co.uk/INFOSEC/84.criptografia-y-seguridad-en-computadores.pdf

MARRERO TRAVIESO, Yran. (2003). La Criptografía como elemento de la seguridad informática. ACIMED, 11(6) Recuperado en 05 de marzo de 2019, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012&lng=es&tlng=es.

MORENO, Blanca. (2015). Tipos de Criptografía. Obtenido de https://plus.google. com/111785202907101039542
MORENO, Johnny. (2012). Criptografía. Recuperado de https://morenojhonny.wordpress.com/ 2012/06/14/unidad-4-criptografia.

MOZILLA DEVELOPER NETWORK – MDN. Contraseñas Inseguras. Disponible en línea: https://developer.mozilla.org/es/docs/Seguridad/Contrase%C3%B1asInseguras

MUÑOZ MUÑOZ, Alfonso. RAMIÓ AGUIRRE, Jorge. (2013). Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo RSA, disponible en: https://0xword.com/libros/36-libro-cifrado-comunicaciones-rsa.html

NFON, Advanced Encryption Standard, Recuperado de: https://www.nfon.com/es/acerca-de-nfon/recursos/glosario/advanced-encryption-standard/

OSAMA, Kashan. (2010). Implementing RC5 Encryption Algotrithm. Obtenido de https://www.amazon.co.uk/IMPLEMENTING-RC5-ENCRYPTION-ALGORIT HM-CONSULTATION/dp/3639243234

PACHECO, Federico. (2014). Criptografía. Recuperado de https://www.amazon.com/Criptograf%C3%ADa-Spanish-Pacheco-Federico-G/dp/9871949359

PADILLA HERNANDEZ, Javier Enrique. (Dic 9, 2014) Criptografía y Seguridad, Disponible en: http://ing.javierpadilla.over-blog.es/2014/12/criptografia-y-seguridad.html

PERAZA, Adarve. DIAZ, Levano. (2012). La Criptografía: "Una guerra de Piratas y Corsarios". Obtenido de https://egov.ufsc.br/portal/conteudo/la-criptograf%C3%ADa-una-guerra-de-piratas-y-corsarios

PEREZ, Simón. (2013). International Data Encryption Algorithm. Recuperado de https://sistemasumma.com/2010/09/14/algoritmo-de-encriptacion -idea/

PRIYADARSHINI, Patil. PARSHANT, Naranyakar., NARAYAN, DG. MEENA, SM. (2016). Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish. Publicada en http://www.sciencedirect.com/science/article/pii/S1877050916 001101

RAMIÓ AGUIRRE, Jorge. (2006). Seguridad Informática y Criptografía. Madrid, España: OxWord
Red Académica y de Investigación Española REDIRIS (2013). Cristología. Obtenido de http://www.rediris.es/ cert/doc/unixsec/node29.html

SANTANA OSORIO, Adriana. (2014). Formas de romper la seguridad. Obtenido de http://criptografias utp.blogspot.pe
Santana, A. (2012). Diseño de un algoritmo de cifrado de clave privada. (Tesis de Pregrado). Universidad Nacional Autónoma de México. México.

SAMANIEGO ZANABRIA, Ana Liz (2018) Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información, disponible en: http://repositorio.urp.edu.pe/bitstream/handle/URP/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

SÁNCHEZ ARRIAZU, Jorge. Descripción del Algoritmo DES. España, 1999. Disponible en: https://www.academia.edu/15633436/Descripci%C3%B3n_del_algoritmo_DES_Data_Encryption_Standard

SHIKATA, Junji. (2009). "Unconditional security". Obtenido de https://link.springer.com/chapter/10.1007/978-3-642-02002-5_7

TECNOLOGÍA & INFORMÁTICA, ¿Qué es la Criptografía? Disponible en: https://tecnologia-informatica.com/que-es-la-criptografia/

URAZAN BUENO, Rohwinzon. QUINTERO ECHEVERRY, José Manuel. Criptografía y Cifrado, disponible en: https://encriptados.files.wordpress.com/2011/11/criptografia.pdf

VILLEGAS GÓMEZ, Roberto. (2009). Comparativa de Seguridad de Algoritmos de cifrado Asimétrico.
México D.F. Recuperado de http://hdl.handle.net/12345 6789/8613.

WIKIPEDIA, (Julio 2018) Historia de la criptografía, recuperado de: https://es.wikipedia.org/wiki/Historia_de_la_criptograf%C3%ADa

XIFRÉ SOLANA, Patricia. (2009). Antecedentes y perspectivas de estudio en historia de la criptografía. Universidad Carlos III de Madrid. Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/6173/PFC_Patricia_Xifre_Solana.pdf?sequence=1&isAllowed=y

OBJETIVOS

OBJETIVO GENERAL

Realizar un análisis comparativo de métodos criptográficos utilizados actualmente en la seguridad informática que me permita identificar el nivel de seguridad y rendimiento para su implementación.

OBJETIVOS ESPECIFICOS

- Realizar la identificación de los diferentes algoritmos criptográficos utilizados actualmente en la seguridad informática.
- Realizar un estudio comparativo sobre los 3 algoritmos criptográficos utilizados en seguridad informática en la actualidad.
- Realizar una comparación sobre las ventajas y desventajas de los 3 algoritmos aplicados a seguridad informática.

CONTENIDO DEL DOCUMENTO:

La criptografía ha existido desde tiempos inmemorables y la humanidad sigue haciendo uso de ella casi sin percatarse; la criptografía nace de la necesidad del hombre por transmitir o enviar un mensaje y que en el camino no fuera interceptado y conocido por otro ajeno a su destinatario, ya que esto podría generar múltiples problemas dependiendo del grado de sensibilidad del mensaje. Esta necesidad motivó la creación o invención de los primeros métodos de cifrado que consistía en que solo el emisor y el receptor sabrían cómo interpretar el mensaje. Desde entonces se ha venido evolucionando en aras de hacer cada vez más segura la trasmisión de información.

En la actualidad se debe destacar la importancia de la criptografía como una rama fundamental de la seguridad informática la cual no solo proporciona protección, sino que también custodia la confidencialidad lo cual es un aspecto muy importante para todas las organizaciones de hoy en día. La criptografía es una herramienta primordial en la formación y continuidad de una organización debido a que en el tránsito de información o en su almacenamiento el riesgo está latente pueden suceder robos de información o violación de contraseñas y accesos no autorizados entre otros. Actualmente se cuentan con sofisticados algoritmos de cifrado cada uno con características particulares, pero todos con un fin en común; proteger la información.

Dicho lo anterior, se halla la necesidad de realizar esta monografía para comparar y conocer los métodos criptográficos utilizados en la seguridad informática para que sirva como documento de estudio a las organizaciones y profesionales de seguridad y garantice un conocimiento más amplio sobre la criptografía, así mismo se hace necesario que las organizaciones conozcan los riesgos a los que se exponen al no contar herramientas criptográficas que no permitan que los delincuentes informáticos puedan descifrar o desencriptar información confidencial y vulnerar la organización. Se estará creando campos de culturización en los entornos laborales, permitiendo una mejoría en el tratamiento de la información y ante todo creando una barrera a los atacantes informáticos.

La presente monografía se enfoca en los métodos criptográficos funcionales en seguridad informática, ya que se evalúan los algoritmos criptográficos identificando sus ventajas y desventajas y comparando su capacidad de cifrado y descifrado. Con el fin de brindar un punto de referencia al momento de seleccionar un método de cifrado para su posterior implementación en algún sistema informático.

Particularmente el desarrollo de esta monografía busca dar respuesta al siguiente interrogante: ¿Cuál de los métodos criptográficos comparados es el más eficaz y funcional en seguridad informática?

Para lograr el primer objetivo específico se realizó una consulta documental enfocada a la identificación de los diferentes algoritmos o métodos criptográficos que han existido y existen actualmente, de los cuales se plasmaron en este documento los que en la actualidad son considerados más funcionales en la seguridad. Resaltando de ellos sus características de seguridad.

Seguidamente para la realización del estudio comparativo se seleccionaron 3 métodos criptográficos resultantes de la consulta documental anterior de los cuales se eligieron 2 de la criptografía simétrica que son AES y DES. Y 1 de la criptografía asimétrica que es RSA. Para ello se definieron variables de comparación que permiten evidenciar las diferentes características con las que cuenta cada uno. Esas variables se enfocan principalmente en su simplicidad y funcionamiento, algunas variables son: Valor de longitud de clave, tipo de algoritmo, relación de cifrado, problemas de seguridad, velocidad de simulación, escalabilidad, clave utilizada, consumo de energía, implementación, funcionalidad. Esta información sobre estas variables es obtenida a través de la consulta documental.

Adicionalmente se realizan pruebas a cada uno de los algoritmos con la finalidad de determinar los tiempos utilizados para el cifrado y descifrado de archivos con diferentes tamaños, permitiendo evidenciar las diferencias existentes entre los mismos.

Por último se realiza una comparación de las ventajas y desventajas obtenidas a través de la consulta documental y recopilándolas en un cuadro comparativo donde se puede observar a grandes rasgos los pros y los contras de cada uno de los algoritmos criptográficos.

METODOLOGÍA

Se realizo una consulta documental de diversos autores cuyos estudios presentan similares objetivos al de la presente monografía, además de revistas y publicaciones científicas sobre los algoritmos criptográficos. Adicionalmente se utilizó la herramienta cryptool la cual permite poner a prueba diferentes métodos criptográficos incluidos los seleccionados en esta monografía DES, AES y RSA.

CONCLUSIONES

Como resultado Se lograron identificar los diferentes métodos criptográficos que existen encontrando gran variedad de estos cada uno con diferentes características, pero con un mismo fin, proteger la información.

Al realizar la comparación de estos tres métodos criptográficos se concluyó que el algoritmo AES consume menos tiempo de cifrado y descifrado y el uso del búfer en comparación con el algoritmo DES, RSA consume más tiempo en los procesos cifrado y descifrado y el uso de la memoria también es más alto en comparación a AES y DES.

Los algoritmos AES y DES son muy veloces en los procesos de cifrado y descifrado, sin embargo la corta longitud de la clave del algoritmo DES genera un poco de desconfianza. A partir del resultado de la simulación, sé pudo evidenciar que el algoritmo AES es mucho mejor que el algoritmo DES y RSA