UNIVERSIDAD RICARDO PALMA

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA INFORMÁTICA CON MENCIÓN EN INGENIERÍA DE SOFTWARE

Para optar el Grado Académico de Maestro en Ingeniería Informática con mención en Ingeniería de Software

"Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información"

Autora: Bach. Samaniego Zanabria, Ana Liz

Asesor: Mg. Pérez Godoy Ballón, Luis

LIMA – PERU

2018

DEDICATORIA

Dedicado a mi familia que es el motor de mi vida y la razón que me motiva a alcanzar mis metas.

AGRADECIMIENTO

La autora expresa su especial agradecimiento a todas las personas que apoyaron en el desarrollo de este trabajo de investigación: profesores de la Maestría Ingeniería Informática de la Universidad Ricardo Palma, amigos y colegas.

RESUMEN

Aunque el término criptografía nos suele hacer pensar en el mundo de los espías y en agencias como la NSA, actualmente está presente en el día a día. Por ejemplo: Cuando se usa los servicios de Gmail, se establece una comunicación segura porque está cifrada entre el ordenador (o nuestro dispositivo móvil) y los servidores de Google. También, cuando se realiza una llamada telefónica desde el terminal móvil, la secuencia de datos que se genera está cifrada, evitando que un tercero no autorizado pueda estar a la escucha e interceptar la comunicación.

En ese contexto, la criptografía se encarga de cifrar o codificar mensajes para evitar que su contenido pueda ser leído por un tercero no autorizado; la función principal de esta disciplina es la generación de códigos y algoritmos de cifrado que buscan proteger la información.

Por otro lado, las empresas están expuestas a las amenazas (como malware, phishing, entre otros) que vulneran los medios de comunicación y datos almacenados en servidores o repositorios, por lo que se recurre al uso de sistemas criptográficos, los cuales cuentan con algoritmos complejos a fin de proporcionar seguridad la información.

En la presente Investigación "Evaluación de algoritmos criptográficos para mejorar la seguridad en la comunicación y almacenamiento de la información", se sometió a pruebas, herramientas, enfoques y ataques a los algoritmos criptográficos globalmente conocidos (AES, IDEA y RC5) y al algoritmo propio ANN, con el propósito de obtener resultados del grado de seguridad, fortaleza de clave, diseño – modo de cifrado, rendimiento y resistencia de cada uno de ellos, con el objetivo de evidenciar cuál de ellos proporciona mayor seguridad en la comunicación y almacenamiento de la información, como solución al problema planteado en párrafos anteriores.

Palabras clave: Algoritmo, Criptografía, Criptoanálisis.

ÍNDICE

CAPITULO I: PLANTEAMIENTO DEL ESTUDIO

En este punto se realiza la introducción, se formula el problema y se justifica el estudio, asimismo se muestra los antecedentes relacionados con el tema, objetivos generales y específicos, y por último se describe la limitación del estudio.

1.1 Introducción

La aparición de la tecnología de información y el uso masivo de las comunicaciones digitales, han producido un número creciente de problemas de seguridad. El avance tecnológico trae consigo nuevas amenazas que vulneran a los medios de comunicación y datos almacenados en servidores o repositorios, las cuales se originaron a partir de las técnicas utilizadas por hackers, cibercriminales y ciberactivistas en los sistemas empleados en el tratamiento de la información.

Como consecuencia de estas capacidades y de las vulnerabilidades que se han ido evidenciando en los sistemas de información, los gobiernos han concientizado los efectos de los ciberataques y han elaborado estrategias de defensa para hacer frente a intrusiones potencialmente devastadoras, o ante cualquier tipo de vulnerabilidad de los sistemas de mando y control, no sólo de las redes militares de defensa, inteligencia o logística de las que se han dotado los estados, sino también de las redes de infraestructuras críticas: energía, servicios básicos, banca, etc., de las cuales los estados son absolutamente dependientes. Por ello, en las últimas décadas, la mayoría de las organizaciones optan por el uso, personalización y/o creación de algoritmos criptográficos específicos para garantizar la seguridad en la comunicación y almacenamiento de la información.

La investigación tiene como base a la tesis de pregrado “SISTEMA INTEGRAL DE SEGURIDAD CRIPTOGRAFICA Y DE COMUNICACIONES” desarrollada en coautoría por la suscrita, y se centra en la evaluación de los algoritmos criptográficos, con el propósito de medir y recoger información de manera independiente acerca de la seguridad que cada uno proporciona al proteger la información.

El objetivo general de la investigación es determinar si el algoritmo propio que utiliza una institución pública del estado peruano proporciona mayor seguridad en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

La hipótesis general de la investigación es la siguiente:

H_G: El algoritmo propio proporciona mayor seguridad en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

Las hipótesis Específicas son las siguientes:

1) H_1: El algoritmo propio presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.
2) H_2: El esquema del algoritmo propio contribuye a mejorar en mayor proporción a la seguridad de la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.
3) H_3: El algoritmo propio proporciona mayor rendimiento frente a los ataques informáticos en comparación con los algoritmos criptográficos globalmente conocidos.

El tipo y método de la investigación son los siguientes:

1) Es teórica por tratar temas de seguridad en los algoritmos, también se puede determinar que es experimental por el uso de herramientas lógicas, computacionales y matemáticas para analizar la seguridad de los sistemas criptográficos. Además, es de campo experimental ya que se utiliza variables independientes que se manipulan para determinar el efecto de esta manipulación sobre las variables dependientes.

2) Por las disciplinas incluidas y sus interrelaciones, la presente investigación es multidisciplinaria, puesto que en este nivel de investigación la aproximación al objeto de estudio se realiza desde diferentes aspectos como el uso de herramientas, la abstracción de procesos complejos para poder inspirar nuevos algoritmos, sistemas o soluciones y la capacidad de comprender nuevas formas de procesamiento de la información, los cuales son percibidos por enfoques basados en la teoría de la información, complejidad y basado en la práctica.

El objeto de estudio se basa en la investigación científica, puesto que se indica los procesos a seguir para realizar las pruebas con las herramientas y las técnicas que

precisan la manera correcta de realizarlo. Se distingue en cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación.

Cabe resaltar que la muestra es no probabilística y por conveniencia, ya que dentro del cifrado digital encontramos el uso de algoritmos globalmente conocidos (AES, IDEA y RC5) y el algoritmo propio ANN.

La presente investigación está respaldada por un marco teórico, siendo una investigación de tipo científica, con diseño de investigación experimental y se estructura de la siguiente forma: El Capítulo I describe el Planteamiento del estudio (Introducción, Formulación del problema y justificación del estudio), Antecedentes relacionados con el tema, Objetivos generales - específicos y Limitaciones del estudio. En el Capítulo II, se plantea el Marco Teórico, las Bases teóricas relacionadas, la definición de términos usados, Hipótesis y Variables que sustentan el estudio. En el Capítulo 3, se describe la Metodología de Investigación (Diseño de investigación, Población y muestra, Técnicas e instrumentos y Recolección de datos). En el Capítulo 4 se muestra los resultados y análisis para confrontar la investigación. En el Capítulo 5, se presentan resultados experimentales para respaldar tal situación, se realiza un análisis de los resultados obtenidos de los cuatro algoritmos criptográficos que fueron sometidos a prueba.

1.2 Formulación del Problema y Justificación del Estudio

Formulación del problema

La información sensible, es el tipo de información generada al interno de una institución, la cual no puede divulgarse, es considerada como parte fundamental para tener un alto nivel de competitividad y posibilidades de desarrollo, es así que los Gerentes y/o Directores han optado por la implantación de sistemas automatizados (integración de los ordenadores y los sistemas de información como estrategia empresarial) capaces de facilitar tareas mecánicas y rutinarias. De esta manera, surge la necesidad de proteger la información.

La Red de Defensa de los Derechos Digitales (2017) ha revelado que:

> Las empresas de software Hacking Team, NSO Group y FinFisher, las cuales son compañías mundiales de ciberespionaje han vendido sus programas a, al menos, 12 gobiernos estatales de México. La primera de ellas, es el caso más claro de espionaje, ya que en 2015 se filtraron miles de correos y documentos en los cuales se destacaba que México invertía cerca de seis millones de euros en estos programas, coronándole como el principal comprador mundial. (p.1)

GReAT (2015) sostiene que:

> La existencia de una campaña de ataques a entidades financieras, que aún continúa, y que se bautizó como Carbanak. Cuyo objetivo es que el atacante no busca información, sino dinero, hablamos propiamente de ciberdelincuencia. La víctima es directamente la institución financiera, a través de transferencias por la red SWIFT (lo que ubica este ataque en el contexto de este proyecto), utilizando múltiples recursos para conseguir el robo de cantidades al parecer prefijadas. Una vez conseguido el objetivo, la víctima es abandonada y se eliminan los rastros. (p.71)

Accenture y HfS Research (2016) afirma que:

> El robo interno de datos y los ataques de malware encabezan la lista de problemas más relevantes para los ejecutivos de seguridad. Una de las principales conclusiones del estudio "The State of Cybersecurity and Digital Trust 2016" es que el 69% ha experimentado un robo o intento de robo de datos por parte de sus empleados en los últimos 12 meses, siendo los sectores de medios de comunicación y las TIC los más afectados por este hecho, con un 77%. La investigación demuestra, además, cómo la falta de presupuesto para la contratación de talento experto en ciberseguridad y empleados bien formados está dificultando la habilidad de las organizaciones para defenderse de estos ataques. (pp.1-2)

El problema que abarca la presente investigación, se centra en el sector defensa y en el campo de la seguridad, ya que se evalúa a los algoritmos criptográficos, los cuales proporcionan seguridad en la comunicación y almacenamiento de información, los mismos que se gestan en una institución pública del estado peruano; en cuyos establecimientos se usan algoritmos criptográficos globalmente conocidos, pero cabe resaltar que en los últimos años se ha optado por el uso de algoritmos propios con el fin de proporcionar mayor seguridad a la información y suplir sus necesidades.

El problema general que responde el estudio es la siguiente:

¿Qué algoritmo criptográfico proporciona mayor seguridad en la comunicación y almacenamiento de la información?

Los problemas específicos son las siguientes:

a) ¿Qué algoritmo criptográfico presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información?
b) ¿Qué algoritmo criptográfico cuenta con el mejor esquema para proporcionar mayor seguridad en la comunicación y almacenamiento de la información?
c) ¿Qué algoritmo criptográfico proporciona mayor rendimiento frente a los ataques informáticos?

Justificación del estudio

Las instituciones y sus sistemas de información se encuentran expuestas a riesgos e inseguridades procedentes de una amplia variedad de fuentes.

Hewlett (2014) precisa que:

> El 80% de los dispositivos disponen de procedimientos de autenticación muy débiles. El 70% de los dispositivos no encriptan la información al transmitirla por internet. El 60% de los interfaces con las webs accedidas son inseguras, disponen de un sistema de credenciales muy débil y son vulnerables a ataques. Todo el firmware y el software implementado en los dispositivos son extremadamente sencillos e inseguros. Por último, el 90% de los dispositivos recolecta algún tipo de información personal, a través del propio dispositivo, la conexión a internet o la aplicación en el móvil. (p.53)

Julián Alfonso (2015) detalla que:

> El FBI detectó una variante que encriptaba el sistema de archivos generando un par de claves RSA de 2048 bits prácticamente imposibles de descifrar, denominada CryptoLocker. El rescate, equivalente a 1 bitcoin, debía realizarse en el plazo de 3 días, o en caso contrario se incrementaba el costo. Esto generó pérdidas de cientos de millones de dólares y afectó a más de un millón de sistemas en todo el mundo. Se calcula que 235.000 víctimas realizaron el pago del rescate, la mitad de ellos en EE.UU., directamente a cuentas de Bogachev, generando una

recaudación de más de 30 millones de dólares entre septiembre y diciembre de 2013. (p.82)

ESET Security Report (2013), informa lo siguiente:

- Solo el 20% de las empresas de Latinoamérica utilizan cifrado para proteger su información. (p.16)
- El caso PRISM y los programas de espionaje de agencias gubernamentales han puesto el tema de la privacidad en Internet en el centro del debate, popularizando el cifrado de datos como una alternativa para la protección de los correos electrónicos y demás comunicaciones. (p.18)
- En julio de 2012, Yahoo! sufrió un ataque donde se robaron alrededor de 500 mil contraseñas de sus usuarios. Las mismas no se almacenaban cifradas, lo cual permitió el acceso directo a las cuentas comprometidas. (p.21)

Eugenio Duarte (2014), determinó que: "Las 8 mejores herramientas para cifrado de información de OpenSource (DiskCryptor, VeraCrypt, OpenTego, GNUGPG, OpenSSH, Open SSL y TOR) incluyen algoritmos de cifrado tales como AES, IDEA DES, MARS y RC5" (p.3).

En la presente investigación se busca conocer la efectividad de los algoritmos criptográficos que se usan constantemente en la institución pública del estado peruano, por lo que se ha elegido a tres (03) algoritmos criptográficos globalmente conocidos y a un (01) algoritmo propio en específico, para ser sometidos a pruebas, análisis y ataques, con el fin de poder calibrar la seguridad que aportan en función de sus mecanismos de seguridad, y de esta forma conocer que tan "fuertes" son, es decir, que se podrá determinar si la seguridad que brindan a la información es de forma incondicional o bajo qué condiciones son vulnerados.

Asimismo, proporciona un conocimiento para que los profesionales de seguridad tengan un criterio en la elección entre un algoritmo criptográfico globalmente conocido u otro, sin descartar la posibilidad diseñar e implantar uno propio. Esto obliga a los ingenieros de sistemas a cuidar con detalle no sólo el diseño de los sistemas, sino su especificación y la posibilidad de razonamiento en aspectos como el uso de herramientas lógicas, computacionales y matemáticas, la abstracción de procesos complejos para poder inspirar nuevos algoritmos, sistemas o soluciones y la capacidad de comprender nuevas formas de procesamiento de la información y/o conocimiento.

Es necesario definir criterios para medir su rendimiento o comportamiento. Estos criterios se centran principalmente en su simplicidad y en el uso eficiente de los recursos. Respecto al uso eficiente de los recursos, éste suele medirse en función de dos parámetros: el espacio, es decir, memoria que utiliza, y el tiempo, lo que tarda en ejecutarse. Ambos representan los costos que supone encontrar la solución al problema planteado mediante un algoritmo. Dichos parámetros van a servir además para comparar algoritmos entre sí, permitiendo determinar el más adecuado de entre varios que solucionan un mismo problema.

1.3 Antecedentes relacionados con el tema

Existen variadas experiencias, investigaciones y documentos relacionados a temas de seguridad de los algoritmos criptográficos. A continuación, haremos una revisión integral respecto de los antecedentes relacionados con el estudio:

Comparativa de Seguridad de Algoritmos de cifrado Asimétrico.

Villegas Gómez Roberto (2009), en la ciudad de México D.F, realizó una investigación en la que propone que los sistemas de cifrado de la Información han logrado evoluciones importantes, al grado de poder unir las fortalezas de diferentes técnicas de cifrado para ofrecer criptosistemas híbridos que conjugan la seguridad ofrecida por cifrado simétrico con las que ofrece el cifrado asimétrico. Es necesario conocer las necesidades particulares de la organización para poder ofrecer la solución óptima utilizando las herramientas que existen acopladas a las necesidades que se pretenden cubrir.

Los fundamentos matemáticos y algoritmos de uso de esta tesis, se tomaron en cuenta en la realización de simulaciones, a fin de conocer la fortaleza del algoritmo criptográfico.

Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish.

Priyadarshini, P., Parshant, N., Narayan, D., Meena, S. (2016), publicaron en Procedia Computer Science, la implementación y análisis de las fortalezas, debilidades, costo y rendimiento de los algoritmos criptográficos utilizados popularmente (DES, 3DES, AES, RSA y Blowfish) para mostrar el rendimiento y poder elegir un algoritmo que mejor se ajusta a los requisitos del usuario.

Cada una de las técnicas de cifrado tiene sus propios puntos fuertes y débiles, las cuales se tomaron en consideración para analizar a cada uno de los algoritmos criptográficos.

Análisis Comparativo de Algoritmos Criptográficos.

Zoran Hercigonia (2016), publicó en la Revista Internacional de Tecnología digital y Economía, las limitaciones de implementación de algoritmos criptográficos existentes como DES, 3DES, CAST-128, BLOWFISH, IDEA, AES y RC6 de técnicas simétricas y RSA de técnicas asimétricas. Asimismo, analizó parámetros como el intercambio de claves, la flexibilidad y los problemas de seguridad de los algoritmos que determinan la eficacia del sistema criptográfico.

Aspectos mencionados en párrafo anterior que sirvieron para calificar al algoritmo que proporciona mayor precisión, eficiencia y seguridad.

Estudio de casos orientados por el Esquema Nacional de Seguridad.

Julián Alfonso Beltrán (2015), en la ciudad de Valencia, realizó un estudio, en el cual recopiló casos de ataques y analizó las técnicas empleadas por los estados en la lucha contra otros estados (guerra electrónica y ciberguerra, y ciberespionaje), y viceversa (hacktivismo y ciberterrorismo).

Se tomó en cuenta los escenarios y técnicas que se han ido implementando para contrarrestar los ataques, con la finalidad de favorecer la comunicación e implantar un propio esquema de seguridad.

1.4 Objetivo general y específicos

A continuación, se detalla el objetivo general y los objetivos específicos de la presente investigación.

Objetivo General

El objetivo general que se identificó en la investigación:

Determinar qué algoritmo criptográfico proporciona mayor seguridad en la comunicación y almacenamiento de la información.

Objetivos Específicos

Para llevar a cabo el cumplimiento del objetivo general, se identificó los siguientes objetivos específicos:

a) Valorar a los cuatro algoritmos criptográficos para precisar cuál de ellos presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información.
b) Evaluar con los principales enfoques a los esquemas de los cuatro algoritmos criptográficos para determinar cuál de ellos proporciona mayor seguridad en la comunicación y almacenamiento de la información.
c) Comparar a los cuatro algoritmos criptográficos con la finalidad de identificar cuál de estos proporciona mayor rendimiento frente los ataques informáticos.

1.5 Limitación del estudio.

La presente investigación consta del estudio, análisis y evaluación de las representaciones de algoritmos criptográficos (AES, IDEA, RC5 y el algoritmo propio ANN) que son empleados para dar seguridad a la comunicación y almacenamiento de la información en una institución pública del estado peruano. El periodo de tiempo de recolección de la información comprende de cinco (05) meses o veinte (20) semanas.

CAPITULO II: MARCO TEÓRICO

En el presente capítulo se detalla el contenido teórico, el cual comprende las bases teóricas, términos usados, hipótesis, variables y matriz de consistencia de la presente investigación.

2.1 Bases teóricas relacionadas con el tema.

En las siguientes líneas se detallan las bases teóricas que se utilizaron en la investigación:

Norma ISO 27001.

La ISO/IEC 27001 (2013), plantea un enfoque completo a la seguridad de la información y define que: "Los activos que necesitan protección van de la información digital, documentos en papel y activos físicos (computadoras y redes) a conocimientos de los empleados. Las cuestiones que se tienen que tratar van del desarrollo de competencias del personal a la protección técnica contra los fraudes informáticos" (p.14).

Comunicación Segura.

Los aspectos que hay que manejar en el proceso de transferencia de un documento electrónico y que definen una comunicación segura, son los siguientes:

Figura 1. Esquema de Comunicación Segura. Se muestra las partes que intervienen para establecer una comunicación segura. Fuente: Tecnología avanzada en medidas y contramedidas electrónicas. TAMCE, 2016.

- *Autenticidad*

Lucena (2004), sostiene que: "La autenticidad es identificar al generador de la información; es decir, consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser". (Citado por Chaves, 2008, p.27).

- *Confidencialidad*

Peraza Adarve y Díaz Lévano (2012), indican que:

> Se trata de la seguridad de que los datos que contiene el documento permanecen ocultos a los ojos de terceras personas durante su trayecto desde A hacia B. Y aquí no entra en juego sólo el papel que realiza la criptografía ocultando los datos, si no también qué se hace con dichos datos una vez han llegado al destinatario de los mismos. Ataques posibles a la Confidencialidad pueden ser entonces la captura del documento en su viaje de A hacia B y el uso indebido de los datos del documento o la mala gestión y almacenamiento de estos datos por parte de B. La confidencialidad se consigue generalmente mediante métodos criptográficos. (p.10)

- *Integridad*

Peraza Adarve y Diaz Levano (2012), afirman que:

> Consiste en la seguridad de que los datos del documento no sufren modificación a lo largo de su transmisión. Un posible ataque en este punto podría ser que una tercera persona capturara el documento en el camino. La comprobación de la integridad se suele realizar mediante firmas electrónicas, generalmente basadas en funciones Hash. La Autenticidad es condición suficiente para la Integridad, por lo que si un documento es auténtico es integro, pero no al revés. (p.10)

- *No Repudio*

Lucena (2004), sostiene que:

> El no repudio de **origen**, es cuando el emisor no puede negar que envió alguna información porque el destinatario recibe una prueba infalsificable del origen del envío. En este caso, la prueba la crea el propio emisor y la recibe el destinatario.
>
> El no repudio de **destino**, es cuando el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona

> al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor. (p.256)

Al respecto, Jhonny Moreno (2012) afirma que: "Proporciona protección frente a que alguna de las entidades implicadas en la comunicación, pueda negar haber participado en toda o parte de la comunicación. Para conseguirlo puede usar por ejemplo firma digital" (p.6).

Seguridad de la Información

Para una correcta gestión en la seguridad de la información se necesita que se tome en consideración a los siguientes principios básicos:

- *Confidencialidad*

Edward Herrera (2014), define que: "Se conoce la confidencialidad como la forma de prevenir la divulgación de la información a personas o sistemas no autorizados" (p.3).

Según la ISO/IEC 17799:2000, "La confidencialidad es el aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso" (p.5).

- *Integridad*

Edward Herrera (2014), sostiene que: "Al hablar de la integridad, es conocer cómo los datos se mantienen intactos, libres de modificaciones o alteraciones por terceros (Personas no autorizadas)" (p.3).

Según la ISO/IEC 17799:2000, "La integridad es la garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento" (p.5).

- *Disponibilidad*

Edward Herrera (2014), define que: "Debe estar disponible cuando el usuario o un sistema necesite consultar la información" (p.4).

Según la ISO/IEC 17799:2000, "La disponibilidad es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados" (p.6).

La Criptografía.

Eneko Amieva (2015), sostiene que:

> La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto. (p.10)

Las principales ramas de la criptografía son:

- *Criptografía Simétrica*

Pedro Gutiérrez (2013), detalla que: "Utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad" (p.4).

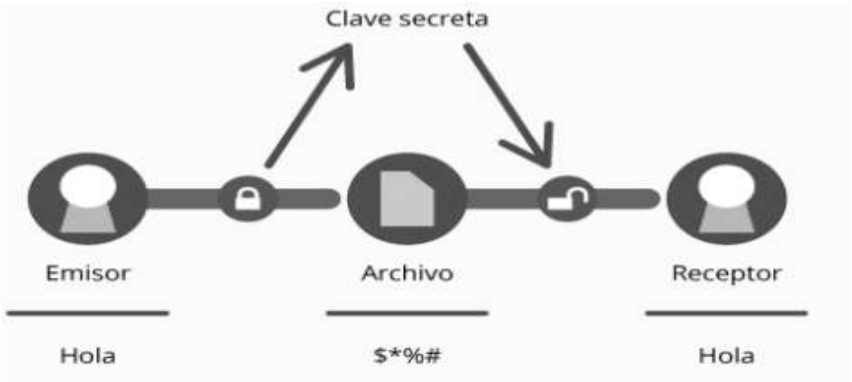


Figura 2. Criptografía Simétrica. Se muestra el proceso de la comunicación, en donde la información es cifrada con una clave compartida entre emisor y receptor.
Fuente: Genbeta (2013)

- *Criptografía Asimétrica*

Pedro Gutiérrez (2013), afirma que: "Se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca)" (p.4).

Las claves públicas y privadas se generan al mismo tiempo y están ligadas entre sí. Esta relación debe ser muy compleja para que resulte difícil que se obtenga una a partir de la otra.

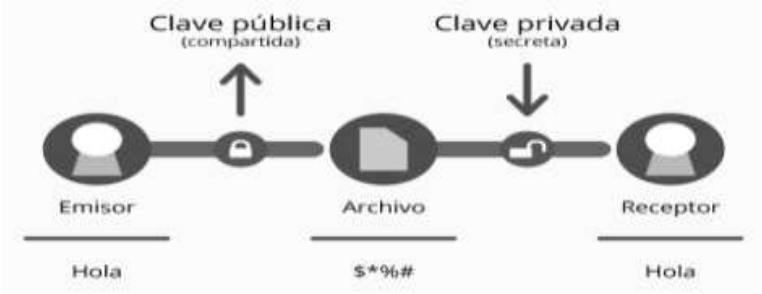


Figura 3. Criptografía Asimétrica. Se muestra el proceso de la comunicación, en donde la información es cifrada con clave compartida y para descifrar es necesario una clave privada.
Fuente: Genbeta (2013)

- *Criptografía Hibrida*

Pedro Gutiérrez (2013), sostiene que: "Es la mezcla o unión de las dos anteriores" (p.4).

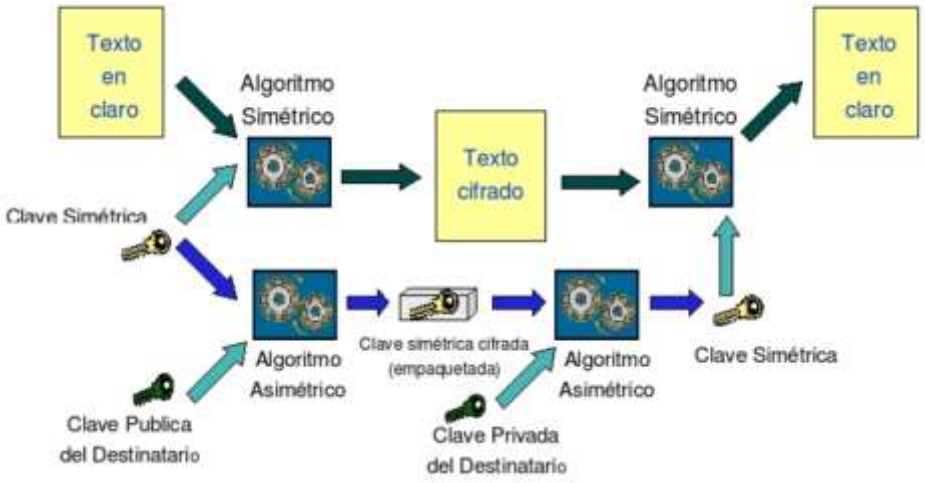


Figura 4. Criptografía Hibrida. Unión de Criptografía Simétrica con la Criptografía Asimétrica.
Fuente: Blanca Moreno (2015)

- *Algoritmo propio*

Shoghi Communications Ltd. (2008), sostiene que: "La mayoría de las organizaciones e instituciones definen su propio algoritmo de cifrado personalizado para garantizar 100% la seguridad en lugar de utilizar algoritmos globalmente conocidos o que no confían en algoritmos específico del vendedor" (p.11).

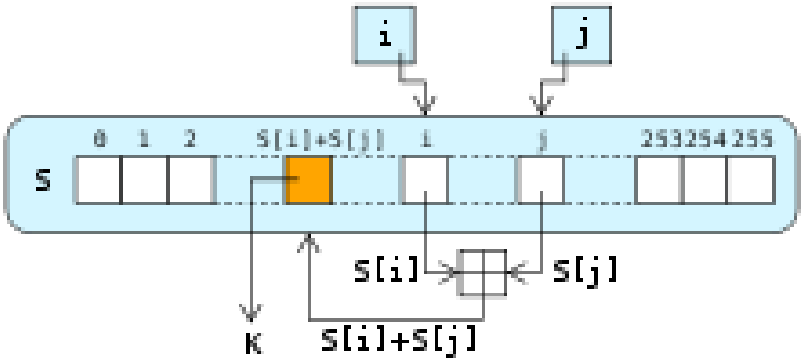


Figura 5. Algoritmo Propio. Aplicaciones de seguridad de la comunicación con función exclusiva (algoritmo de cifrado personalizado).
Fuente: Blanca Moreno (2015)

Firmas Digitales.

Según Jorge Ramió Aguirre (2006), "la firma digital es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje" (p.16).

Figura 6. Proceso de Firma Digital. La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático.
Fuente: Cámara de Comercio y Producción - CCPSD

Ataques informáticos.

Jorge Mieres (2009), define que: "Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización" (p.4).

Figura 7. Ataque Informático. Un ataque no es más que la realización de una amenaza.
Fuente: Jorge Mieres (2009)

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- *Interrupción*

Se considera un ataque a la **disponibilidad**, es decir cuando un recurso del sistema es destruido o deja de estar disponible.

José García (2011), sostiene que: "Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque es la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros" (p.13).

- *Intercepción*

Jaime Rodríguez (2011), afirma que:

> Una entidad no autorizada consigue acceso a un recurso. Éste es un ataque contra la **confidencialidad**. Ejemplos de este ataque son la obtención de datos mediante el empleo de programas troyanos o la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes de datos para develar la identidad de uno o más de los usuarios mediante el Spoofing o engaño implicados en la comunicación intervenida (intercepción de identidad). (p.3)

- *Modificación*

José García (2011), define que: "Una entidad no autorizada que no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la **integridad**. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red" (p.13).

- *Fabricación*

Jaime Rodríguez (2011), define que: "Una entidad no autorizada inserta objetos falsificados en el sistema. Éste es un ataque contra la **autenticidad**. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir datos a un archivo. Asimismo, estos ataques se pueden clasificar en términos de ataques pasivos y ataques activos" (p.3).

Estado del arte.

En este punto se menciona a otros estudios que tienen temas similares a la presente investigación:

- *Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre matriz de puertas programables (del inglés Field-Programmable Gate Array).*

Msc. Alejandro Cabrera y Dr. Alejandro Cabrera (2013), La Habana-Cuba, en su trabajo integran implementaciones hardware de algoritmos criptográficos a la biblioteca OpenSSL, la cual es utilizada para establecer comunicaciones seguras sobre el sistema operativo Linux con la finalidad de asegurar redes TCP/IP. Los algoritmos implementados son el AES (*Advanced Encryption Standard*) y las funciones resumen

SHA-1 y SHA-256. Estos algoritmos son implementados como coprocesadores del procesador MicroBlaze utilizando interfaces FSL para el intercambio de datos entre ellos. Estos coprocesadores son integrados dentro de la biblioteca OpenSSL considerando la naturaleza multitarea del sistema operativo Linux, por lo que se selecciona un mecanismo de sincronización para controlar el acceso a estos dispositivos. Además son presentados los resultados de velocidad alcanzados por los coprocesadores integrados en la biblioteca utilizando la herramienta speed de la misma. Finalmente es presentado el impacto de estos coprocesadores en la velocidad de transmisión a través de una red privada virtual utilizando la herramienta OpenVPN. (http://scielo.sld.cu/scielo.php?script=sci_ arttext &pid=S1815-59282013000300005).

Un aspecto muy importante a tener en cuenta en la implementación de algoritmos criptográficos es la cantidad de recursos de cómputo, ya que fue necesario para realizar las pruebas y la ejecución de ataques, los cuales requieren equipos de última generación.

- *Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles.*

Gálvez Meza Nancy (2014), en la ciudad de México D.F, en su investigación enmarca el estudio y desarrollo de algoritmos criptográficos para dispositivos móviles. Concretamente, se enfocó en el desarrollo de una mejora en la implementación del algoritmo AES en un dispositivo móvil (teléfono celular) con arquitectura ARM de 32 bits. Realizó un análisis de los Algoritmos más utilizados con respecto a su desempeño (en tiempo y seguridad) y tras elegir el algoritmo más idóneo (AES) se han aplicado diversas técnicas para mejorar su implementación de manera que se ahorren al máximo los recursos limitados que un dispositivo móvil posee.(http://148.204.210.201/tesis/1404316762511NPGMTesis An.pdf).

Los retos afrontados en la presente tesis, sirvió para descubrir los procesos algorítmicos que cada vez son más eficaces y poseen mayor rendimiento.

- *Estudio de factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001.*

Javier Seclén Arana (2016), en la ciudad de Lima, realizó la investigación que tiene por finalidad analizar y evaluar todos aquellos aspectos que afectan el desarrollo del proceso de implementación del Sistema de Gestión de Seguridad de la Información en las entidades del sector público, así como también investigar las estrategias y metodologías que permitieron alcanzar beneficios en las instituciones. (http://cybertesis.unmsm.edu.pe/handle/cybertesis/4884).

Se tomó como referencia a las variables encontradas, para ser utilizadas como información de apoyo a la mejora de las políticas de seguridad de información.

2.2 Definición de términos usados

En las siguientes líneas se detallará los diferentes términos usados en la presente investigación:

Criptografía (Cifrado de datos).

Se ocupa de transposicionar u ocultar el mensaje enviado por el emisor hasta que llega a su destino y es descifrado por el receptor. "Según el Diccionario de la Real Academia, la palabra criptografía proviene de la unión de los términos (oculto) y (escritura), y su definición es: Arte de escribir con clave secreta o de un modo enigmático" (Manuel Lucena, 2014, p.29).

Criptoanálisis.

Basado en el conocimiento de los algoritmos de cifrado y de las características generales de los mensajes. "Consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación" (Manuel Lucena, 2014, p.32).

Terminología criptográfica.

La terminología criptográfica se refiere al conjunto de términos y de siglas utilizados en el dominio de la criptografía.

- *Alfabeto:* Conjunto de letras o caracteres que representan los sonidos humanos.
- *Alfabeto Criptográfico:* Alfabeto utilizado en procedimientos Criptográficos, integrado por 26 o 27 letras o signos. Se excluye las letras dobles (CH, LL, RR).
- *Ambiente:* Información conocida sobre un texto cifrado de una determinada fuerza enemiga. (Fecha, promotor destinatario, acontecimientos, procedimientos de cifra, términos de cortesía, comienzos de texto, separaciones, letras muertas, final de texto, artificios, etc.)
- *Cadena Fraseológica:* Es la parte de un código, representado por letras, sílabas, palabras, números, frases, etc. que determinan el claro y se encuentran ubicadas en paralelo a la cadena criptográfica.
- *Cadena Criptográfica:* Es la parte de un código, representado por grupos de letras o números en forma eslabonada, que determinan el cripto y obedecen a convenios preestablecidos.
- *Cámara Negra:* División o departamento integrado por equipos de criptoanálistas, dedicados exclusivamente a la descriptación de todo tipo de mensajes.
- *Cifrar:* Operación que consiste en transformar un texto claro en texto cifrado, utilizando un procedimiento de cifra convenido.

Texto claro (CL) + procedimiento de cifra (K) = cripto (XP)

- *Decalaje:* Acción de desarrollar un alfabeto ordenado en forma vertical, tomando como base las letras de un criptograma.
- *Descifrar:* Operación que consiste en transformar un texto cifrado en texto claro, utilizando un procedimiento convenido.

Texto cripto (XP) + procedimiento de cifra (K) = claro (CL)

- *Descriptar:* También conocido como "romper". Es el resultado del criptoanálisis, permite penetrar definitivamente en el secreto que contiene determinado criptograma, así como el acto mismo de reconstruir el sistema o método que se empleó para cifrarlo.
- *Frecuencia:* Número de veces que se repite una letra, una sílaba, un polígrama, una palabra o números en determinado mensaje.

- *Método Criptográfico:* Procedimiento especial de cifrado que se deriva de un sistema de cifra, con instrucciones convencionales para transformar en enigmático un texto claro.
- *Palabra Probable:* Posible palabra utilizada para descriptar (estará relacionada siempre al ambiente).
- *Perturbación:* Es la alteración del orden normal de un alfabeto, en base a palabras claves o numéricas.
- *Recifrar:* Operación de cifrar por segunda vez un texto cifrado.
- *Rejilla:* Plancha o plancheta de cartón, cartulina u otro material, generalmente cuadrangular, con perforaciones en forma de casillas o ventanas.
- *Regleta:* Elemento de cifra conformado por un Alfabeto Primario y uno o más alfabetos secundarios (cuerpo de claves) fijos o móviles.
- *Secuencia:* Veces que una letra le sigue a otra, tanto en texto llano como en cifrado. En el idioma castellano, a la letra "A" le sigue con gran frecuencia la letra "R" (AR), lo mismo sucede con la letra "E" que frecuentemente es seguida por la letra "S" (ES). Así mismo existe una "secuencia obligada", a la letra "Q" le sigue la letra "U" (QU).
- *Sustitución:* Reemplazar la letra de un texto por otras letras o guarismos.
- *Tablero o cuadro:* Papel cuadriculado, especialmente preparado para "vaciar" las letras del mensaje, al ser transpuestas en base a una llave.
- *Transposición:* Alteración o mezcla del orden normal de las letras de un texto.

En conclusión esta investigación está respaldada por un Marco teórico.

2.3 Hipótesis de la investigación

Hipótesis General

H_G: El algoritmo propio proporciona mayor seguridad en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

Hipótesis Específicas

a) H_1: El algoritmo propio presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

b) H_2: El esquema del algoritmo propio contribuye a mejorar en mayor proporción a la seguridad de la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

c) H_3: El algoritmo propio proporciona mayor rendimiento frente a los ataques informáticos en comparación con los algoritmos criptográficos globalmente conocidos.

2.4 Variables de la investigación

Variable Independiente.

- *Algoritmo criptográfico*

Definición Conceptual: Es un algoritmo que modifica los datos de un documento con el objetivo de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.

a. AES: "Método para cifrar información también conocido como Rijndael, es un esquema de cifrado por bloques, es uno de los algoritmos más populares usados en criptografía simétrica". (Jesús Ángel, 2005, p.37).

b. IDEA: "Cifrador por bloques que es utilizado para cifrar textos con un tamaño de bloque de 64 bits, utilizando una llave K de 128 bits". (Sergio Perez, 2013, p.36).

c. RC5: Es una unidad de cifrado por bloques notable por su simplicidad. también contiene algunas unidades de sumas modulares y de Puertas O-exclusivo (XOR). La

estructura general del algoritmo es una red tipo Feistel. Las rutinas de cifrado y descifrado pueden ser especificadas en pocas líneas de código, pero la programación de claves es más complicada. (Osama Khashan, 2010, p.4)

d. ANN: Algoritmo propio.

Definición operacional:

a. Grado de Seguridad

En este aspecto se considera la capacidad de almacenamiento y fortaleza de clave que posee un algoritmo criptográfico, según el detalle siguiente:

- Capacidad de almacenamiento del algoritmo (unidad de medida en Kilobytes).
  Los ponderados asignados a la capacidad de almacenamiento se pueden observar en la tabla 1.

Tabla 1. Capacidad de almacenamiento

	CONSIDERACION	PESO
Fuerte	Algoritmo con mayor capacidad	3
Débil	Algoritmo con menor capacidad	1

Fuente: Elaboración Propia

- Fortaleza de clave: Número de combinaciones del algoritmo criptográfico (Cálculo matemático 2^n, n es el número de bits).
  Los ponderados asignados a la fortaleza de clave se pueden observar en la tabla 2.

Tabla 2. Fortaleza de clave

	CONSIDERACION	PESO
Fuerte	Algoritmo que posee más de 64 bits	3
Débil	Algoritmo que posee menos de 64 bits.	1

Fuente: Elaboración Propia

b. Esquema del Algoritmo

En este aspecto se considera el diseño de un algoritmo criptográfico.

- Diseño - Modo de cifrado: Número de etapas o pasos que tiene un algoritmo para cifrar.

Los ponderados asignados al diseño del algoritmo criptográfico se pueden observar en la tabla 3.

Tabla 3. Diseño del algoritmo

	CONSIDERACION	PESO
Alto	Algoritmo que tiene más de 16 etapas.	3
Medio	Algoritmo que tiene de 7 a 16 etapas.	2
Bajo	Algoritmo que tiene hasta 6 etapas.	1

Fuente: Elaboración Propia

c. Rendimiento frente ataques informáticos

En este aspecto se considera al rendimiento y resistencia que posee un algoritmo criptográfico, según el detalle siguiente:

- Rendimiento: Velocidad que posee el algoritmo criptográfico para realizar una tarea, es necesario tener el tiempo que demora en cifrar o descifrar.

  Re: Rendimiento.

  D: Tiempo de velocidad del descifrado en segundos.

  E: Tiempo de velocidad del cifrado en segundos.

$$\mathrm{Re} = \frac{\mathrm{D}}{\mathrm{E}}$$

Los ponderados asignados al rendimiento se pueden observar en la siguiente tabla:

Tabla 4. Rendimiento del algoritmo

	CONSIDERACION	PESO
Positivo	Velocidad del cifrado es menor que la velocidad del descifrado.	3
Negativo	Velocidad del cifrado es mayor o igual que la velocidad del descifrado.	1

Fuente: Elaboración Propia

- Resistencia: Número de ataques que soporta en forma individual e independiente durante 5 meses de pruebas.

  En la tabla 5 se muestran las consideraciones y ponderados que obtendrán los algoritmos criptográficos para determinar la resistencia que cada uno posee.

Tabla 5. Resistencia del algoritmo

	CONSIDERACION	PESO
Fuerte	Soporta 3 o más de 3 ataques.	3
Débil	Soporta 1 o 2 ataques.	1

Fuente: Elaboración Propia

Variable Dependiente

Definición conceptual:

a. Seguridad de las comunicaciones: Para Díaz, Mur, San Cristóbal (2004), es conocida por las siglas **COMSEC**, es la disciplina que se encarga de prevenir que alguna entidad no autorizada que intercepte la comunicación pueda acceder de forma inteligible a información.

b. Seguridad de la información: Para Gómez Vieites, Álvaro (2007), es un conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Definición operacional:

a. Grado de seguridad
   Se evaluó la disponibilidad e integridad que posee cada algoritmo criptográfico.

- Disponibilidad: Capacidad que tiene el algoritmo para recuperar la operatividad ante un posible fallo.
  R: Disponibilidad.
  MTBF: Tiempo medio entre fallas en segundos.
  MTTR: Tiempo medio para reparación en segundos.

Fórmula para obtener la disponibilidad de un algoritmo:

$$R = \frac{MTBF}{MTBF + MTTR} * 100$$

En la tabla 6 se muestran las consideraciones y ponderados que obtendrán los algoritmos criptográficos para determinar el porcentaje de disponibilidad que cada uno posee.

Tabla 6. Disponibilidad del algoritmo

	CONSIDERACION	PESO
Alto	Algoritmo que tiene más de un 70%.	3
Medio	Algoritmo que tiene entre 45% y 70%.	2
Bajo	Algoritmo que tiene menos de 45%.	1

Fuente: Elaboración Propia

- Integridad: Comprobar que el mensaje no fue modificado.

  En la tabla 7 se muestran las consideraciones y ponderados que obtendrán los algoritmos criptográficos para determinar la integridad que cada uno posee.

Tabla 7. Integridad del algoritmo

	CONSIDERACION	PESO
Fuerte	El código del cripto es igual al que recibe el receptor.	3
Débil	El código del cripto es diferente al que recibe el receptor.	1

Fuente: Elaboración Propia

Matriz de Consistencia

Se detallan los siguientes aspectos del estudio: Planteamiento del problema, objetivos, hipótesis, variables e indicadores.

Tabla 8. Matriz de Consistencia

PLANTEAMIENTO DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
Pregunta General	**Objetivo General**	**Hipótesis General**	**VARIABLE INDEPENDIENTE**

¿Qué algoritmo criptográfico proporciona mayor seguridad en la comunicación y almacenamiento de la información?	Determinar cuál de los cuatro algoritmos criptográficos proporciona mayor seguridad en la comunicación y almacenamiento de la información.	**H_G:** El algoritmo propio proporciona mayor seguridad en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.	Algoritmos criptográficos globalmente conocidos (AES, IDEA y RC5) y el algoritmo propio ANN. **Indicador** ***Grado de Seguridad*** • Capacidad de almacenamiento. • Fortaleza de clave ***Esquema*** • Diseño y Modo de cifrado
Preguntas específicas	**Objetivos específicos**	**Hipótesis especificas**	***Rendimiento frente ataques*** • Rendimiento • Resistencia **VARIABLE DEPENDIENTE** Seguridad en la comunicación y almacenamiento de la información. **Indicador** ***Grado de Seguridad*** • % Disponibilidad • Integridad
a) ¿Qué algoritmo criptográfico presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información?	a) Valorar a los cuatro algoritmos criptográficos para precisar cuál de ellos presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información.	**H_1:** El algoritmo propio presenta mayor grado de seguridad en forma incondicional en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.	
b) ¿Qué algoritmo criptográfico cuenta con el mejor esquema para proporcionar mayor seguridad en la comunicación y almacenamiento de la información?	b) Evaluar con los principales enfoques a los esquemas de los cuatro algoritmos criptográficos para determinar cuál de ellos proporciona mayor seguridad en la comunicación y almacenamiento de la información.	**H_2:** El esquema del algoritmo propio contribuye a mejorar en mayor proporción a la seguridad de la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.	
c) ¿Qué algoritmo criptográfico proporciona mayor rendimiento frente a los ataques informáticos?	c) Comparar a los cuatro algoritmos criptográficos con la finalidad de identificar cuál d estos proporciona mayor rendimiento frente los ataques informáticos.	**H_3:** El algoritmo propio proporciona mayor rendimiento frente a los ataques informáticos en comparación con los algoritmos criptográficos globalmente conocidos.	

Fuente: Elaboración Propia

CAPÍTULO III: METODOLOGÍA DE INVESTIGACIÓN

En este capítulo se presenta la metodología de la investigación, la cual está basada en el diseño, población - muestra, técnicas - instrumentos y recolección de datos.

3.1 Diseño de investigación.

Clasificación de la investigación

La presente investigación según su clasificación tiene las siguientes características:

- Según la clasificación "Por el propósito o finalidad perseguida":

Marín (2008), define que: "La investigación es teórica porque busca la aplicación y/o utilización de los conocimientos adquiridos" (p.2).

Según esta tipificación, la presente investigación es teórica puesto que proporcionará conocimientos para mejorar la seguridad de la comunicación y almacenamiento de la información.

- Según la clasificación "Por el enfoque utilizado":

Alvira (2002), sostiene que: "Una investigación es cuantitativa usando un diseño cuasi experimental. La investigación cuantitativa es aquella que permite examinar los datos de manera numérica, además de existir claridad en los elementos de investigación, es objetiva por lo que se utiliza la medición absoluta y controlada" (p.4).

Según el punto anterior, la presente investigación plantea consideraciones para cada uno de los aspectos a evaluar y cada uno con sus respectivos ponderados, permitiendo que los resultados sean numéricos y se puedan apreciar de forma gráfica.

- Según la clasificación "Por el alcance o nivel de conocimiento que se adquieren":

Para Hernández, Fernández y Baptista (1997), "la investigación es correlacional, porque busca especificar propiedades, características y rasgos importantes" (p.81).

En la presente investigación se evalúa a los algoritmos criptográficos, a fin de medir o recoger información de manera independiente acerca de la seguridad que cada uno proporciona al proteger la información.

- Según la clasificación "Por la clase de medios utilizados para obtener los datos":

Es una investigación de campo experimental ya que consiste en la manipulación de una (o más) variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o porqué causa se produce una situación o acontecimiento particular. El experimento provocado por el investigador, le permite introducir determinadas variables de estudio manipuladas por él, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas. (Alfaro, 2012, p.17).

En la presente investigación, se ha considerado como variable independiente a los algoritmos criptográficos (AES, RC5, IDEA y ANN) con la finalidad de evaluar y comparar respecto a la seguridad que proporciona a la variable dependiente.

- Según la clasificación "Por las disciplinas incluidas y sus interrelaciones":

La investigación interdisciplinaria es un tipo de investigación realizada por equipos de individuos por la cual se integra información, datos, técnica, herramientas, perspectivas, conceptos, y/o teorías de dos o más disciplinas o cuerpo especializados de conocimiento orientados a avanzar una compresión fundamental o resolver problemas cuyas soluciones yacen, más allá del ámbito de una disciplina área práctica investigatoria. (National Academy of Sciences, 2005, p.27).

En la presente investigación se ha tomado en consideración herramientas lógicas, computacionales y matemáticas, las cuales están acorde con el desarrollo de nuevas tecnologías y del crecimiento en el poder computacional.

- Según la clasificación "Dependiendo del campo de conocimientos":

Torres (2007), sostiene que: “La investigación científica es el proceso general qué conjuga la teoría y la práctica; es decir, es una actividad relacionante entre la gnosis y la práctica, que viene a ser la relación existente entre la investigación científica básica y aplicada” (p.4).

En la presente investigación, se busca incrementar el conocimiento en áreas de criptografía y seguridad, ya que ambas son necesarias para contrarrestar las amenazas de la informática y agentes ajenos al sistema.

Metodología de Gestión y/o Desarrollo

Para la obtención de información se empleará el método de observación y el uso de herramientas lógicas, computacionales y matemáticas.

La presente investigación es científica, su razonamiento es la inferencia que hace uso de la noción de "fuerza inductiva", con la cual se obtiene conclusiones generales a partir de premisas particulares. Se distingue en cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación. (Karl R. Popper, 2013, p.17)

3.2 Población y muestra.

Población

La población de estudio para la presente investigación estará compuesta por los algoritmos criptográficos y como unidad de análisis a los algoritmos criptográficos globalmente conocidos de código abierto.

Muestra

La muestra ha sido elegida por conveniencia. Los cuatro algoritmos criptográficos (AES, RC5, IDEA y ANN) son utilizados en una institución pública del estado peruano para cifrar sus informaciones.

Relación entre variables

La presente investigación permitirá conocer la relación entre variables:

a. Variables independientes:

Algoritmos criptográficos (AES, RC5, IDEA y ANN).

b. Variables dependientes:

Seguridad en la comunicación y almacenamiento de la información.

En la tabla 9 se muestra la relación entre variables, según el detalle siguiente:

Tabla 9. Relación entre variables

VARIABLE	INDICADORES	SUB INDICADORES
Algoritmos criptográficos	Grado de Seguridad	Capacidad de almacenamiento.
		Fortaleza de clave.
	Esquema	Diseño y modo de cifrado.
	Rendimiento	Tiempo de velocidad en cifrado y descifrado.
		Resistencia.
Seguridad en la comunicación y almacenamiento de la información.	Grado de Seguridad	Disponibilidad. Integridad.

Fuente: Elaboración Propia.

3.3 Técnicas e instrumentos.

Se usaron las herramientas lógicas, computacionales y matemáticas para la evaluación de los algoritmos criptográficos antes mencionados.

Asimismo, la abstracción de procesos complejos ayudó a comprender las formas de procesamiento de la información, gracias a los enfoques basados en la teoría de la información, complejidad y en la práctica.

3.4 Recolección de datos

Se aplicó la técnica de análisis documental a los resultados, que permitió seleccionar los datos relevantes a fin de expresar su contenido.

Se registraron los datos de acuerdo al detalle siguiente:

- Ficha técnica del algoritmo criptográfico.
- Matrices de comparación entre algoritmos criptográficos.
  - Matriz basada en el Principio de KERCKHOFFS.
  - Matriz de Seguridad por oscuridad.
  - Matriz basada en la Ingeniería Inversa.
  - Matriz del Ataque de la Fuerza Bruta.
  - Matriz de Fortaleza.
- Matriz de Resultados.

Técnicas de procesamiento y análisis de datos

Concluida la recolección de datos, se procesaron los datos y se elaboraron cuadros comparativos entre los algoritmos criptográficos globalmente conocidos (AES, RC5, IDEA) y el algoritmo propio (ANN), para ello se usó los programas informáticos de tratamientos de datos como Excel y/o el programa Statistical Product and Service Solutions conocido como SPSS.

El análisis y estudio de los algoritmos, en algunas ocasiones es completamente abstracto, sin embargo, es necesario para calibrar la seguridad que aporta cada algoritmo en función de si éste es seguro de forma incondicional o si es seguro sólo si se cumplen ciertas condiciones.

CAPÍTULO IV: RESULTADOS Y ANÁLISIS DE RESULTADOS

En este capítulo, se realiza el desarrollo de la evaluación de los algoritmos criptográficos, se muestra los resultados derivados del proceso de desarrollo y el respectivo análisis de estos resultados.

4.1 Desarrollo de la evaluación

A continuación, se muestra la descripción y análisis de cada uno de los algoritmos criptográficos.

Descripción de algoritmos criptográficos.

a. AES:

- Se utilizan cuatro fases diferentes para cifrar, una de permutación y tres de sustitución:
  - Sustitución de bytes: Se usa una tabla, denominada caja S4, para realizar una sustitución byte a byte del bloque.
  - Desplazamiento de filas: Una simple permutación realizada fila por fila.
  - Mezcla de columnas: una sustitución que altera cada byte de una columna en función de todos los bytes de la columna.
  - Suma de la clave de etapa: Una simple operación XOR bit a bit del bloque actual con una porción de la clave expandida.
- Proceso de generación de las subclaves.

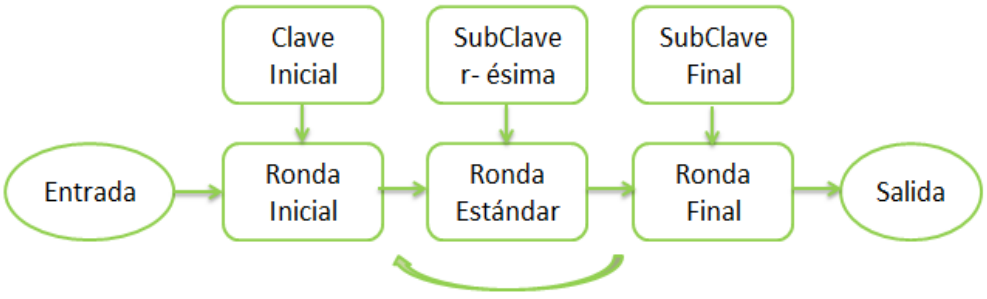


Figura 8. Proceso de generación de subclaves. Se muestra las 3 rondas que tiene el proceso y que de estas se genera las subclaves.
Fuente: Patricia Xifré (2009)

- Proceso de cifrado

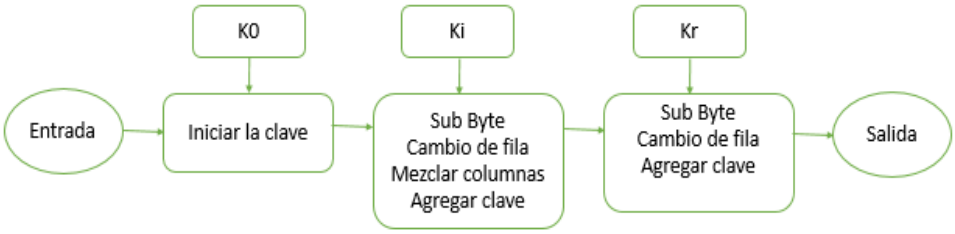


Figura 9. Proceso de cifrado. Se muestra el proceso de cifrado del algoritmo AES.
Fuente: Patricia Xifré (2009)

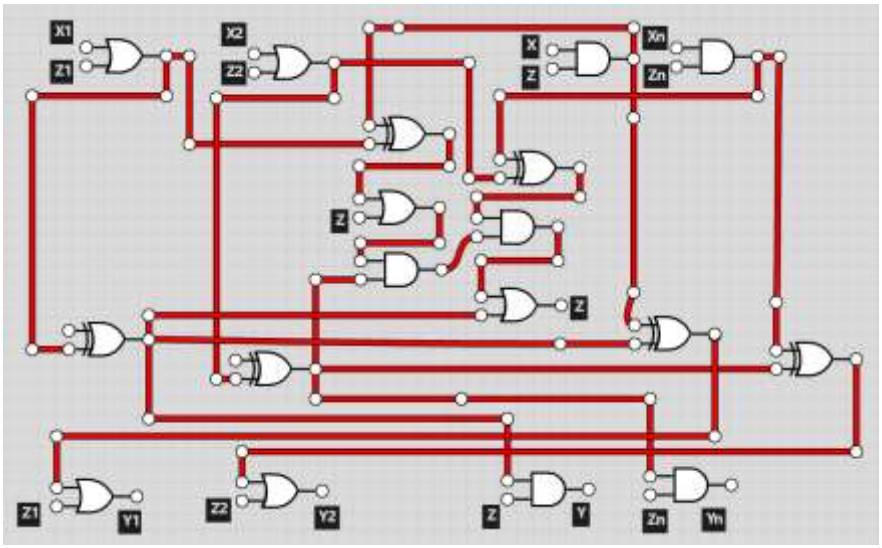


Figura 10. Circuito del Proceso de cifrado. Se muestra el proceso de cifrado del algoritmo AES.
Fuente: Patricia Xifré (2009) / Software logic.ly

b. IDEA:

- El algoritmo de generación de subclaves se basa solamente en el uso de desplazamientos circulares pero ejecutados de manera compleja para generar un total de seis subclaves para cada una de las ocho etapas del IDEA.
- Proceso de cifrado.

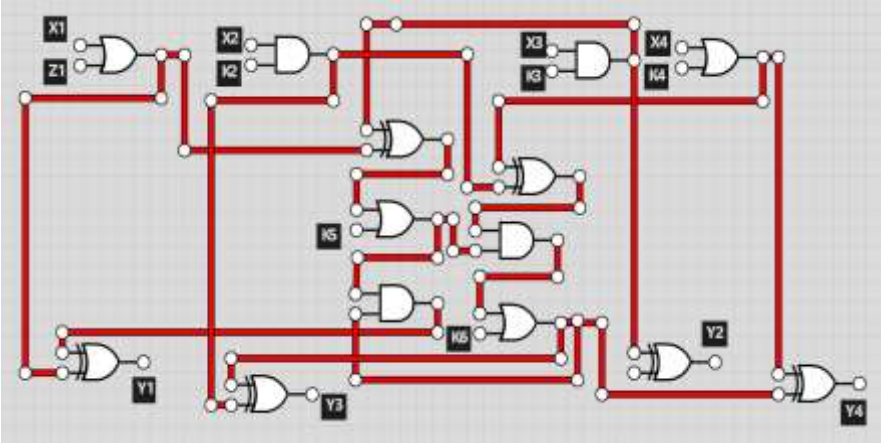


Figura 11. Proceso de cifrado. Se muestra el diagrama general del proceso de cifrado del Algoritmo IDEA.
Fuente: Sergio Pérez (2013) / Software logic.ly

c. RC5:

- Es un algoritmo simple y orientado a palabras. Las operaciones básicas procesan palabras enteras de datos cada vez.
- Rotaciones dependientes de los datos: incorpora rotaciones (desplazamientos circulares de bits) cuya cantidad depende de los datos.
- Proceso de cifrado.

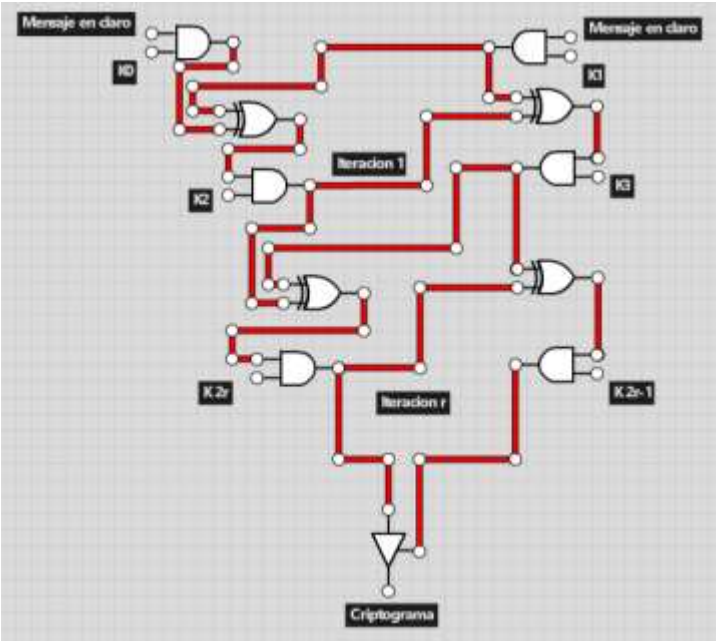


Figura 12. Proceso de cifrado. Se muestra el diagrama del proceso de cifrado del Algoritmo RC5.
Fuente: Osama Khashan (2010) / Software logic.ly

d. ANN:

- Cifra todo tipo de archivos digitales.
- Las claves son generadas de forma aleatoria
- Las llaves de cifrado nunca se repiten.
- Emplea tres bloques de cifrado binario.
- Proceso de cifrado.

Figura 13. Proceso de cifrado. Se muestra el diagrama del proceso de cifrado del Algoritmo ANN.
Fuente: Elaboración propia.

Las figuras que se muestran a continuación corresponden a los registros del algoritmo propio:

	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	0	1	1	0	0	1
1	0	0	1	0	0	0	1	0	1	0	0	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	0	1	1	0
2	0	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	1	0	0	1	0	1	0	0	0	0	0	1	1	1	0
3	0	1	0	1	0	1	1	0	1	1	0	1	0	0	1	1	1	0	0	1	0	0	1	0	1	0	1	0	1	0	0
4	1	0	1	1	0	1	1	1	1	0	0	0	0	0	0	1	0	0	1	0	1	1	0	0	1	0	1	0	1	1	0
5	0	1	1	0	0	1	1	1	0	1	1	0	0	0	1	0	0	1	1	1	0	0	0	0	1	1	1	0	0	0	0
6	0	1	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0
7	0	1	1	1	1	0	1	0	1	0	1	0	0	1	0	1	0	0	1	0	1	1	1	1	1	1	0	1	1	1	1

Figura 14. REG 1. Se muestra el primer registro que posee el Algoritmo ANN.
Fuente: Institución pública del estado peruano.

3	2	1	0
1	1	0	1
1	0	0	0
1	1	1	1
0	1	0	1
0	1	0	1
1	0	1	0
0	1	1	0
1	0	0	0

Figura 15. REG 2. Se muestra el segundo registro que posee el Algoritmo ANN.

		17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
13	0	0	1	0	0	1	1	1	1	1	1	0	0	0	1	1	0	1	1
8	1	0	1	1	1	0	0	0	0	0	1	0	1	0	1	1	0	0	0
15	2	1	1	1	0	1	1	0	0	0	1	1	0	0	1	1	1	1	1
5	3	0	0	1	1	0	0	0	1	1	1	1	0	1	1	1	1	1	0
5	4	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	0	1	0
10	5	0	0	1	1	1	0	0	1	1	1	1	1	0	1	1	0	0	1
6	6	1	1	1	0	1	1	0	1	1	0	0	1	0	1	0	1	0	1
8	7	1	1	1	0	1	1	1	0	0	1	1	1	1	1	0	1	1	0

Figura 16. REG 3. Se muestra el tercer registro que posee el Algoritmo ANN.
Fuente: Institución pública del estado peruano.

30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	1	1	0	0	0	1	1	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	1	0	0	0	0	1	1	1
1	1	1	1	0	0	0	0	0	1	0	0	1	1	0	0	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0
1	1	1	1	0	0	0	1	0	0	0	0	1	0	0	1	0	1	1	0	1	0	1	1	1	1	0	0	0	1	1
0	1	0	1	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	1	0
0	0	1	1	0	0	1	1	0	1	0	1	0	0	0	1	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1
1	0	0	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	0	1	0	0
0	0	1	0	1	0	0	0	0	0	1	1	0	0	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	0	0
1	1	1	0	1	0	0	1	1	1	0	0	1	0	0	1	1	1	0	1	1	1	0	1	1	1	1	1	0	1	0

Figura 17. REG 4. Se muestra al tercer registro que posee el Algoritmo ANN.
Fuente: Institución pública del estado peruano.

1	0
1	1
1	2
1	3
0	4
1	5
1	6
1	7

Figura 18. Clave cifrante. Se muestra el resultado de todos los pasos del Algoritmo ANN.
Fuente: Institución pública del estado peruano.

Análisis de algoritmos criptográficos.

Las características más destacadas a evaluar de los algoritmos criptográficos (AES, RC5, IDEA y ANN) son las siguientes:

- Longitud de claves: Una medida del número de claves posibles que pueden usarse en un cifrador.
- Tamaño de bloque: Es una unidad de cifrado de clave simétrica que opera en grupos de bits de longitud fija.
- Número de rondas: Realiza siempre las mismas operaciones un número determinado de veces.
- Operaciones que realiza: Ciencia matemática utilizada para poder realizar un buen diseño de un algoritmo es conveniente basarse en: la teoría de la información, teoría de números, estadística. (Adriana Santana, 2012, p.13).

- Uso de la caja S: En criptografía, una caja-S es un componente básico de los algoritmos de cifrado simétrico. En los algoritmos por bloques son usadas a menudo para oscurecer la relación existente entre texto claro y texto cifrado. En muchos casos las cajas-S son elegidas cuidadosamente para ser resistentes al criptoanálisis. (Adriana Santana, 2012, p.75).

En la tabla 10 se muestran las principales características de los algoritmos criptográficos, según el detalle siguiente:

Tabla N° 10: Principales características de los algoritmos criptográficos

CARACTERÍSTICA	AES	IDEA	RC5	ANN
Tipo	Algoritmo simétrico	Algoritmo simétrico	Algoritmo simétrico	Algoritmo mixto
Longitud de clave (bits)	128, 192 o 256 bits	128 bits	128, 192 y 256 bits	512 bits
Tamaño de bloque	128 bits	64 bits	32, 64 o 128 bits	256 bits
Numero de Rondas	10, 12 o 14	8	12	24
Operaciones	⊕, Desplazamiento, Transposición	⊙, ⊕,⊞	⊕,⊞	
Basado	Sustituciones, permutaciones y transformaciones lineales	Transformaciones idénticas	Rotaciones dependientes	Las llaves de cifrado nunca se repiten
Caja S	Si	No	Si	No
Aplicaciones	Destinados a sustituir DES y 3DES	PGP	Varios paquetes de software	Sistema de Seguridad

Fuente: Elaboración propia, se ha tomado como referencia a la Tesis de Diseño de un algoritmo de cifrado, 2012.

4.2 Resultados de la evaluación

Para una mejor apreciación de los resultados, se ha formulado fichas técnicas por cada algoritmo criptográfico de acuerdo al detalle siguiente:

Ficha técnica del algoritmo criptográfico

a. AES

Tabla N° 11: Ficha técnica del algoritmo AES

CARACTERÍSTICAS	ESPECIFICACIONES BÁSICAS
Aplicación	Cifrador iterado, relativamente sencillo, que emplea funciones invertibles y opera con bloques enteros y bytes en vez de bits.
Modalidad de operación	El resultado obtenido en cada paso del algoritmo, es un conjunto de tantos bits como la longitud del bloque. Los bits adyacentes se agrupan de ocho en ocho, formando bytes, y éstos en una tabla cuadrada de cuatro filas y columnas (cuatro para el caso particular de este estándar).
Seguridad de información de llaves	Diseñado teniendo en cuenta tres criterios: un máximo de resistencia frente a ataques conocidos, sencillez en el diseño y que su implementación pueda realizarse de manera compacta teniendo en cuenta a la vez características de velocidad y adaptabilidad a diferentes plataformas.
Mecanismo de protección	Se implementa entonces una única ronda mediante lógica combinacional suplementada con registros, memorias y multiplexores, debido fundamentalmente al hecho de tener que distinguir entre rondas con diferentes secuencias de operaciones.
Parámetros Criptográficos	
Tipo de algoritmo	Simétrico.
Algoritmo personalizable por el usuario	No cuenta con este parámetro.
Capacidad de generación de llaves	Consiste en dos partes, la primera en el proceso de cifrado y la segunda en el proceso de generación de las subclaves.
Seguridad	Resistente al análisis lineal y el análisis diferencial.
Borrado de emergencia	No cuenta con este parámetro.
Capacidad	Para 80 bits de seguridad AES, es equivalente a 1024 bits de RSA, y 163 de ECDSA.

Fuente: Elaboración propia

b. IDEA:

Tabla N° 12: Ficha técnica del algoritmo IDEA

CARACTERÍSTICAS	ESPECIFICACIONES BÁSICAS
Aplicación	Cifrador por bloques, consiste de ocho transformaciones idénticas (cada una llamada ronda) y una transformación de salida, llamada media ronda.
Modalidad de operación	El proceso para cifrar y para descifrar es el mismo, solo cambian las llaves de ronda, en total 52 de 16 bits cada una.
Seguridad de información de llaves	Gran parte de la seguridad se deriva del intercalado de operaciones de distintos grupos adición y multiplicación modular y O-exclusivo (XOR) bit a bit.
Parámetros Criptográficos	
Tipo de algoritmo	Simétrico.
Algoritmo personalizable por el usuario	No cuenta con este parámetro.
Capacidad de generación de llaves	Se divide la llave original en 8 partes de 16 bits cada una. Las primeras 6 partes son las llaves k1 a k6 de izquierda a derecha respectivamente, utilizadas en la primer ronda de IDEA. Las últimas dos partes serán las llaves K7 y K8. Las otras 44 llaves son generadas de realizar un corrimiento circular a la izquierda de 25 bits sobre la llave original, se extraen las llaves siguientes y se hace el corrimiento nuevamente, hasta completar las 52 llaves en 6 pasos.
Borrado de emergencia	No cuenta con este parámetro.
Capacidad	Para cifrar mensajes de mayor tamaño se utilizan los modos de operación, el cual permite cifrar archivos de cualquier tamaño utilizando un cifrador determinado y una sola llave.

Fuente: Elaboración propia

c. RC5:

Tabla N° 13: Ficha técnica del algoritmo RC5

CARACTERÍSTICAS	ESPECIFICACIONES BÁSICAS
Aplicación	Algoritmo que opera por bloques.
Modalidad de operación	Hace uso de rotaciones dependientes. En su estructura contiene algunas operaciones como sumas modulares y operaciones XOR.
Seguridad de información de llaves	Utiliza la clave secreta del usuario para expandir un arreglo S de claves, que contiene 2(r + 1) palabras aleatorias determinada por la clave original.
Mecanismo de protección	Proporciona alta seguridad.
Parámetros Criptográficos	
Tipo de algoritmo	Simétrico.
Algoritmo personalizable por el usuario	No cuenta con este parámetro.
Capacidad de generación de llaves	Tamaño variable de bloques (32, 64 o 128 bits), con tamaño de clave (entre 0 y 2040 bits) y número de vueltas (entre 0 y 255). La combinación sugerida originalmente era: bloques de 64 bits, claves de 128 bits y 12 vueltas.
Seguridad	Permite negociar o acordar entre la velocidad y alta seguridad. Se incorporan rotaciones circulares de bits las cuales dependen de los datos introducidos, esto hace que RC5 sea más robusto aún, por consiguiente, que sea prácticamente irrompible para cualquier criptoanalista.
Borrado de emergencia	No cuenta con este parámetro.
Capacidad	Su estructura permite que sea fácilmente implementado y de igual manera da la oportunidad de evaluar y determinar la con facilidad la robustez del algoritmo.

Fuente: Elaboración propia

d. ANN:

Tabla N° 14: Ficha técnica del algoritmo ANN

CARACTERÍSTICAS	ESPECIFICACIONES BÁSICAS
Aplicación	Sistema de Seguridad
Modalidad de operación	Algoritmo de cifrado robusto y no comercial. (Diseñado según necesidades). Emplea tres bloques de cifrado binario.
Mecanismo de protección	Emplea dos llaves de cifrado de 512 bit, generadas de forma aleatoria cada una.
Parámetros Criptográficos	
Tipo de algoritmo	Algoritmo mixto.
Algoritmo personalizable por el usuario	Permite escalabilidad. Sin embargo la fuente es confidencial.
Capacidad de generación de llaves	Las claves son generadas de forma aleatoria.
Seguridad	Las llaves de cifrado nunca se repiten.
Borrado de emergencia	No cuenta con este parámetro.
Capacidad	Cifra todo tipo de archivos digitales.

Fuente: Elaboración propia

Pruebas de Seguridad.

a. Niveles de Seguridad.

- Se mide en referencia al tamaño de claves que cada algoritmo criptográfico emplea. Asimismo se muestran los tiempos obtenidos como resultado de la ejecución al cifrar con cada uno de ellos.

  La tabla 15 muestra los tiempos obtenidos para las diferentes claves, con su nivel de seguridad correspondiente.

Tabla N° 15: Nivel de Seguridad Criptográfica

Ítem	AES	IDEA	RC5	ANN
Longitud de clave	256 bits	128 bits	256 bits	512 bits
Tiempo de ejecución	1539.7 Mb/s	4174 b/s	3450 b/s	376 b/s

Fuente: Elaboración propia.

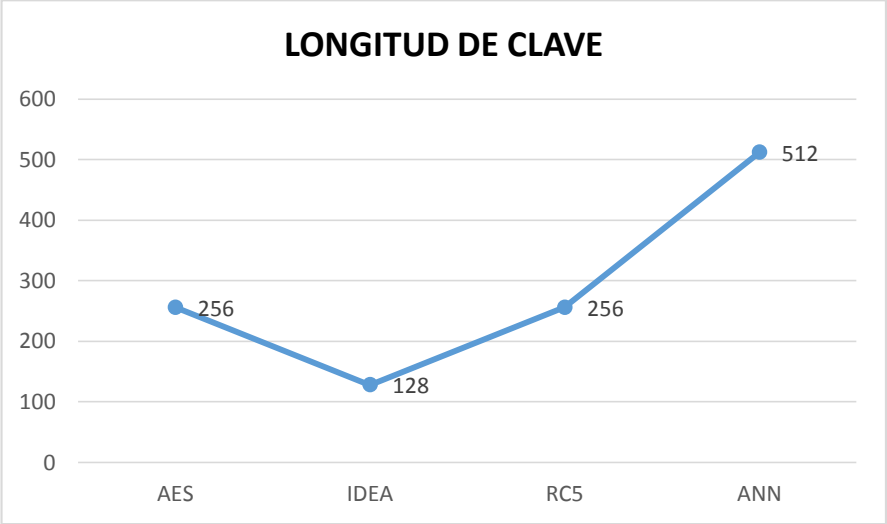


Figura 19. Longitud de clave. Se muestra el histograma de la longitud de clave de cada algoritmo criptográfico.
Fuente: Fuente propia.

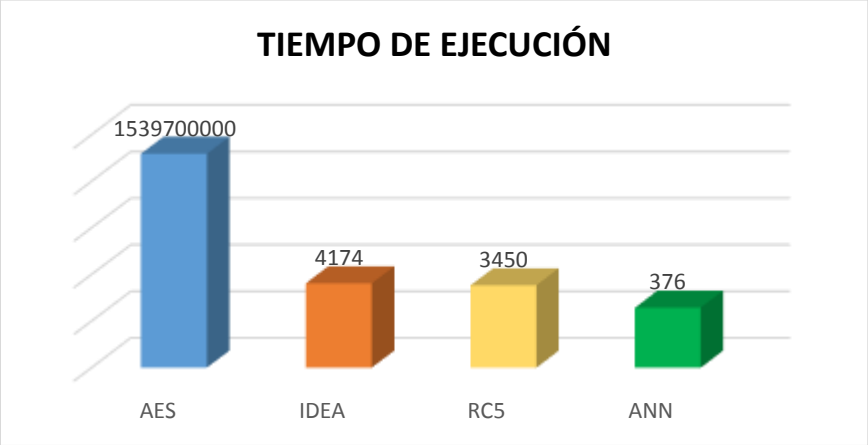


Figura 20. Tiempo de ejecución. Se muestra el gráfico comparativo de los tiempos de ejecución al cifrar el mismo mensaje con cada algoritmo criptográfico.
Fuente: Fuente propia.

- Se mide el tiempo que emplea cada algoritmo criptográfico en descifrar un mensaje.

Tabla N° 16: Tiempo de Descifrado de los Algoritmos

ALGORITMO	TIEMPO DE DESCIFRADO
AES	1519.9 Mb/s
IDEA	6452 bits por segundo
RC5	5665 bits por segundo
ANN	447 bits por segundo

Fuente: Elaboración propia.

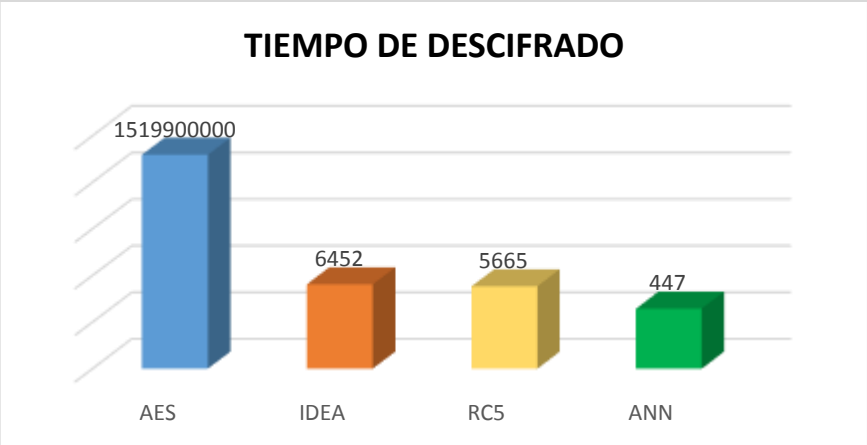


Figura 21 Tiempo de descifrado. Se muestra el gráfico comparativo de los tiempos de cada algoritmo criptográfico en descifrar el mismo mensaje.
Fuente: Fuente propia.

Pruebas de Criptoanálisis.

Para las pruebas realizadas, se tomaron en cuenta la definición de Jorge Mieres, quien indica que el criptoanálisis consiste en realizar diferentes técnicas para descubrir la clave y/o contraseña, como ataques por fuerza bruta, por diccionarios o híbridos en un tiempo no definido.

Sin embargo, es importante tener en cuenta que para un ataque de búsqueda de clave no basta con probar todas las posibles claves.

Para este estudio, es conveniente conocer los siguientes ataques posibles:

- Ataque con texto cifrado. Sólo se conoce el criptograma.

- Ataque con texto original conocido. Se conoce un texto inicial y texto cifrado.
- Ataque con texto cifrado escogido. Se conoce al texto original y a su respectivo cripto.

Tabla N° 17: Tiempo empleado en descifrar texto cifrado escogido.

ALGORITMO	TIEMPO EMPLEADO
AES	634 segundos
IDEA	399 segundos
RC5	538 segundos
ANN	1872 segundos

Fuente: Elaboración propia.

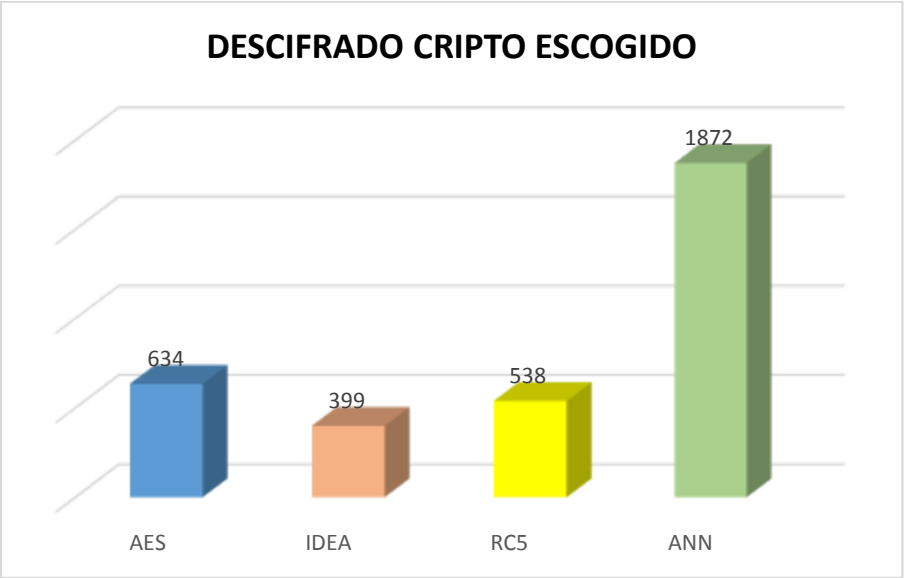


Figura 22. Descifrado de cripto escogido. Se muestra el gráfico comparativo de los tiempos empleado por cada algoritmo criptográfico en descifrar el texto cifrado escogido.
Fuente: Elaboración propia.

Presentación de los datos.

Se formuló cinco matrices para la presentación de los datos, en las cuales se especifican los ítems elegidos en la evaluación de cada uno de los algoritmos criptográficos.

- Matriz basada en el principio de KERCKHOFFS

  Los principios de KERCKHOFFS aplicados a la criptografía son:

  a. El sistema debe ser computacionalmente seguro (indescifrable).
  b. La seguridad del sistema debe recaer sólo en la clave.
  c. El sistema debe ser portable y su uso no deberá requerir la intervención de varias personas.
  d. El sistema debe ser fácil de usar, no requerirá conocimientos especiales ni tendrá una larga serie de reglas.

Tabla N° 18: Matriz de KERCKHOFFS

ITEM	ALGORITMOS CRIPTOGRAFICOS			
	AES	IDEA	RC5	ANN
Sistema irrompible	X	X	X	X
Efectividad del sistema radica en su clave	X			X
Los criptogramas son alfanuméricos	X	X	X	X

Tabla 18. Matriz de KERCKHOFFS. El (X) representa que el algoritmo criptográfico cumple con los Ítems elegidos para evaluar la seguridad de un sistema cifrado.
Fuente: Fuente propia.

- Matriz de seguridad por oscuridad

  La seguridad por oscuridad también conocida como la seguridad por ocultación, comúnmente utilizada en criptografía y seguridad informática, es un controvertido principio de ingeniería de la seguridad, que intenta utilizar el secreto para garantizar la seguridad.

Tabla N° 19: Matriz de Seguridad por oscuridad

ITEM	ALGORITMOS CRIPTOGRAFICOS			
	AES	IDEA	RC5	ANN
Mantener el secreto el código fuente del software				X
Mantener el secreto de algoritmos y protocolos utilizados				X
Adopción de políticas de no revelación pública de la información sobre vulnerabilidades				X
Cambiar puerto de acceso				X

Tabla 19. Matriz de Seguridad por oscuridad. El (X) representa que el algoritmo criptográfico cumple con los Ítems elegidos para evaluar la seguridad por oscuridad.
Fuente: Fuente propia.

- Matriz basada en la ingeniería inversa

  La ingeniería inversa consiste en realizar análisis del algoritmo criptográfico, supone profundizar en el estudio de su funcionamiento y principios tecnológicos, hasta el punto de que podamos llegar a entender, modificar y vulnerar dicho modo de funcionamiento, mediante el razonamiento abductivo.

Tabla N° 20: Matriz de Ingeniería inversa

ITEM	ALGORITMO CRIPTOGRAFICO			
	AES	IDEA	RC5	ANN
Reducir la complejidad del sistema		X	X	
Recuperar y/o actualizar la información perdida				X
Detectar efectos laterales				X
Facilitar la reutilización	X	X	X	X

Tabla 20. Matriz de Ingeniería Inversa. El (X) representa que el algoritmo criptográfico cumple con los Ítems elegidos para evitar la ingeniería inversa.
Fuente: Fuente propia.

- Matriz del ataque de Fuerza Bruta

  Es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Tabla N° 21: Matriz de ataque de Fuerza bruta

ITEM	ALGORITMO CRIPTOGRAFICO			
	AES	IDEA	RC5	ANN
Longitud de la clave	X		X	X
Complejidad de clave	X			X

Tabla 21. Matriz de Ataque de fuerza bruta. El (X) representa que el algoritmo criptográfico cumple con los Ítems que evitan el ataque de fuerza bruta.
Fuente: Fuente propia.

- Matriz de Fortaleza

  Se basa en la complejidad que se tendría para descubrir la clave que emplea el algoritmo criptográfico.

Tabla N° 22: Matriz de Fortaleza

ITEM	ALGORITMO CRIPTOGRAFICO			
	AES	IDEA	RC5	ANN
Seguridad de la clave				X
Dificultad de adivinar la clave				X
Dificultad de invertir el algoritmo cifrado	X			X

Tabla 22. Matriz de Fortaleza. El (X) representa que el algoritmo criptográfico cumple con los Ítems elegidos para evaluar la fortaleza.

Fuente: Fuente propia.

Análisis de Resultados

- **Matriz de Resultados**

  Se muestran los resultados obtenidos por cada algoritmo criptográfico. El ponderado nos indica el valor que obtuvo cada algoritmo, a mayor ponderación el algoritmo proporciona mayor seguridad a la comunicación y almacenamiento de la información. Como resultado, el algoritmo propio ANN proporciona mayor seguridad y el IDEA proporciona menor seguridad en comparación con el AES, RC5 y ANN.

Tabla N° 23: Matriz de Resultados

VARIABLE	INDICADOR	ITEM	ALGORITMO CRIPTOGRAFICO			
			AES	IDEA	RC5	ANN
Independiente	Grado de Seguridad	Capacidad de almacenamiento	1	1	1	3
		Fortaleza de clave	3	1	1	3
	Esquema	Diseño - Modo de cifrado	2	1	2	3
	Rendimiento frente ataques	Rendimiento	1	3	3	3
		Resistencia	3	1	1	3
Dependiente	Grado de seguridad	Disponibilidad	2	1	2	3
		Integridad	3	1	1	3
TOTAL DE PONDERADOS			15	9	11	21

Fuente: Elaboración Propia

En la figura 23 “Matriz de resultados” se observa que el algoritmo propio, denominado ANN, tiene el mayor ponderado en todos los ítems al ser comparado con los otros algoritmos criptográficos globalmente conocidos.

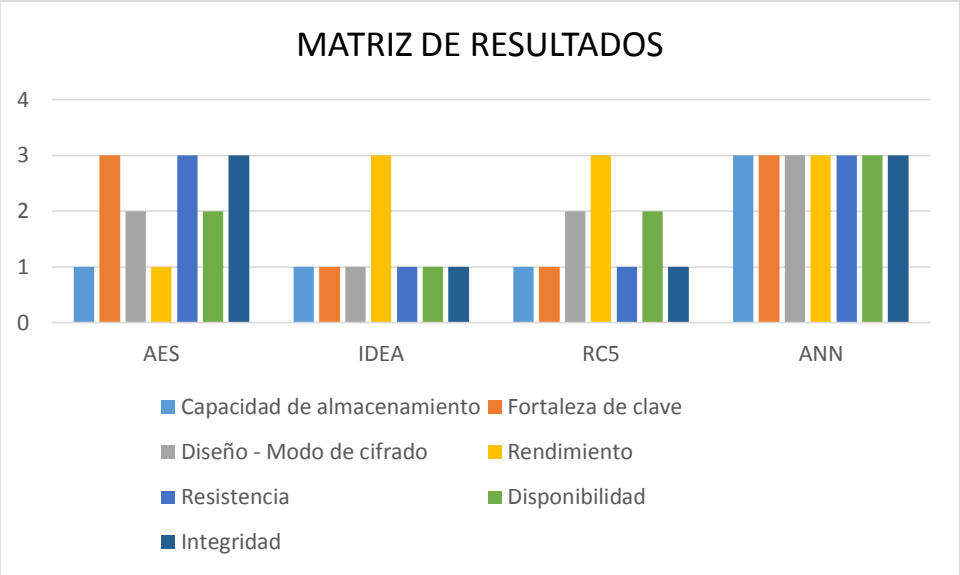


Figura 23. Matriz de resultados. Se muestra el diagrama de ponderación por ítems de cada algoritmo criptográfico.
Fuente: Elaboración propia.

En la figura 24 “Resultado por indicadores” se observan los siguientes aspectos:

a. El algoritmo propio ANN posee mayor capacidad de almacenamiento en comparación con los algoritmos criptográficos globalmente conocidos.
b. El algoritmo AES y ANN tienen ponderado 3 respecto al Ítem de la fortaleza de clave, es decir poseen mayor número de combinaciones en comparación con algoritmos IDEA y RC5.
c. El algoritmo ANN posee mayor número de etapas de proceso; por ende, su diseño (método de cifrado) es más complejo que los algoritmos criptográficos globalmente conocidos.
d. El algoritmo IDEA, RC5 y ANN poseen el mismo ponderado en rendimiento y son superiores al algoritmo AES.
e. El algoritmo AES y ANN poseen el mismo ponderado respecto a la resistencia, siendo los más resistentes frente a los ataques sometidos.
f. El algoritmo ANN posee mayor ponderado en disponibilidad e integridad.

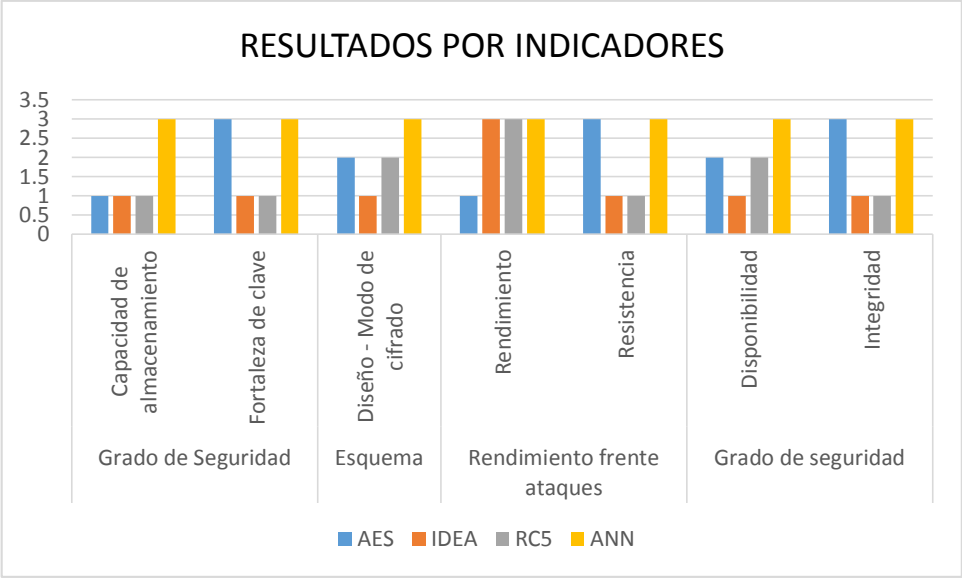


Figura 24. Matriz de resultados por Indicadores. Se muestra el diagrama de ponderación por indicadores de cada algoritmo criptográfico.
Fuente: Elaboración propia.

En la figura 25 "Resultado de la comparación" se observa evidentemente que el algoritmo propio ANN proporciona mayor seguridad en comparación con los algoritmos criptográficos globalmente conocidos.

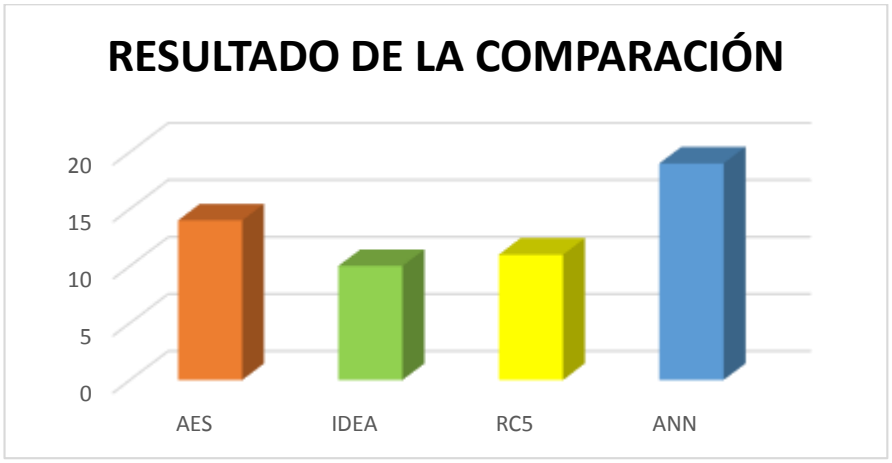


Figura 25. Resultado de la comparación de algoritmos criptográficos. Se muestra el diagrama de ponderación por ítems de cada algoritmo criptográfico.
Fuente: Elaboración propia.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

A continuación se enuncian las conclusiones y recomendaciones derivadas de la presente investigación:

Conclusiones

a) El algoritmo propio ANN presenta mayor grado de seguridad en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos, los ítems que sustentan este resultado son la resistencia y capacidad de almacenamiento.

b) El esquema del algoritmo propio ANN posee el mayor número de combinaciones para generar las claves y su diseño tiene mayor número de etapas en el proceso de cifrado, es decir que contribuye a mejorar en mayor proporción a la seguridad de la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

c) El algoritmo propio proporciona mayor rendimiento frente a los ataques informáticos en comparación con los algoritmos criptográficos globalmente conocidos.

d) Se puede apreciar en la Tabla N° 23 “Matriz de Resultados”, que el algoritmo propio resulta ser el que mayor puntaje obtiene al sumar los ponderados de los ítems, seguido por el algoritmo AES, RC5 y en último lugar el algoritmo IDEA. En consecuencia, se concluye que el algoritmo propio ANN proporciona mayor seguridad a la comunicación y almacenamiento de la información.

Recomendaciones

a) Se recomienda usar claves más largas y que sea una combinación de letras (mayúsculas y minúsculas), números y caracteres para prolongar el tiempo empleado en el ataque de fuerza bruta a un algoritmo criptográfico.

b) Se recomienda capacitar al personal idóneo en criptología de acuerdo al avance tecnológico, pues serán los encargados de desarrollar algoritmos criptográficos enfocándose en el grado de seguridad, diseño y resistencia frente a nuevos ataques.

c) Tener presente que ante un entorno seguro, las personas ya sea por desconocimiento, negligencia o coacción podrían vulnerar las reglas establecidas en las políticas de seguridad de la información, por ende es necesario afianzar la ética, tener un enfoque proactivo y establecer mecanismos que contrarresten esa acción.

d) Para consolidar los resultados y dando continuidad a la línea de investigación, se debe realizar pruebas con el simulador del protocolo cuántico.

REFERENCIA BIBLIOGRÁFIA

Accenture and HfS Research (2016). *The State of Cybersecurity and Digital Trust.* Recuperado de https://www.accenture.com/t20160704T014005Z_w_/us-en/_can media/PDF-23/Accenture-State-Cybersecurity- and- Digital- Trust- 2016-Report-June.pdf#zoom=50.

Alcocer, M. (2006). *Criptografía Española*. Recuperado de http://www. cervantesvirtual.com/obra/criptografia-espanola/

Alfaro, C. (2012). *Metodología de investigación científica aplicado a la ingeniería.* (Proyecto de investigación). Universidad Nacional del Callao, Lima, Perú.

Alvira, M. (2002). *Perspectiva cualitativa / perspectiva cuantitativa en la metodología sociológica*. México. México: Mc Graw Hill.

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

Angel, J. (2005). *Advanced Encryption Standard*. México. Recuperado de www.criptored.upm.es/guiateoria/gt_m117i.htm

Belran, J. (2015).*Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad*. Recuperado de https://riunet. upv.es/ bitstream/handle/025/5602/Memoria.pdf?sequence=1

Cámara de Comercio y Producción CCPSD (2016). *Firma digital*. Recuperado de https://www.eldinero.com.do/20543/camara-de-comercio-presenta-al-mercado-certificado-de-firma-digital/

Daltabuit, E. (2015). *Consideraciones sobre la Seguridad de la Información Digital*. Obtenido de https://ccns.jimdo.com/ encriptaci%C3%B3n-de-datos/

Díaz, G., Mur, F., San Cristóbal, E. (2004). *Seguridad en las comunicaciones y en la información*. Recuperado de https://books.google.com.pe/

Duarte, E. (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-informacion/

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

Gálvez, N. (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.

García, J. (2011). *Tipos de Ataques informáticos*. Recuperado de http://www.delitosinformaticos.com/seguridad/clasificacion.shtml.

Genbeta (2013). *Tipos de Criptografía*. Recuperado de https://www. genbeta.com/

Gómez, A. (2007). *Enciclopedia de la Seguridad Informática*. Bogotá, Colombia: Alfaomega. Obtenido de https://books.google.com.pe/books/about/ Enciclopedia_de_la_seguridad_inform%C3%A1tic.html?id=MQ_kOgAACAAJ &redir_esc=y

GReAT, Kaspersky Lab's Global Research & Analysis Team (2015). *"El gran robo de banco: el APT Carbanak". VirusList*. Recuperado de http://www.viruslist.com/ sp/weblog?weblogid=208189052

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

Hercigonja, Z. (2016). *Análisis Comparativo de Algoritmos Criptográficos*. Revista Internacional de TECNOLOGÍA DIGITAL Y ECONOMÍA. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved =0ahUKEwiRtvzH_4vXAhXJ4SYKHeGICh4QFghgMAk&url=https%3A%2% 2Fhrcak.srce.hr%2Ffile%2F262162&usg=AOVa w1y3gBx0a6SNPlaufNDZF5n

Hernández, R., Fernández, C. y Baptista, P. (1997). *Metodología de la Investigación.* México, México: McGraw Hill Interamericana.

Herrera, E. (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/

ISO/IEC 17799:2000. Código de Buenas Prácticas para la Gestión de la Seguridad de los Sistemas de Información. Obtenido de http://www.belt.es/expertos/experto. asp?id=2245

ISO/IEC 27001 (2013). *Seguridad de la Información*. Recuperado de http://www.dnvba.com/cl/certificacion/sistemas-de-gestion.aspx

Kirk, R. (1995). *Experimental design: procedures for the behavioral sciences* (3ªEd.).

California, Estados Unidos: Brooks/Ciole Publishing.

Lucena, M. (2014) *Criptografía y Seguridad en Computadores*. Recuperado de http://sertel.upc.edu/tdatos/ Libros/Lucena.pdf.

Marín, A. (2008). *Clasificación de la investigación*. Recuperado de https://metinvestigacion.wordpress.com/

Mieres, J. (2009). *Ataques Informáticos (Debilidades de seguridad comúnmente explotadas).* Obtenido de https://www.evilfingers.com/publications/ white_AR/01_Ataques_informaticos.pdf.

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

Moreno, A. (2015). *Tipos de Criptografía*. Obtenido de https://plus.google. com/111785202907101039542

Muñoz, A., Ramió, J. (2013). *Cifrado de las comunicaciones digitales de la cifra clásica al algoritmo RSA*. Madrid.

National Academy of Sciences, NAS (2005). *Facilitat inginter disciplinary Research*. Washington, Estados Unidos: The National Academies Press

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

Pacheco, F. (2014). *Criptografía*. Recuperado de https://ccns.jimdo.com/ encriptaci%C3%B3n-de-datos/

Peraza, A., Diaz L. (2012). *La Criptografía: "Una guerra de Piratas y Corsarios"*. Obtenido de http://www.egov.ufsc.br/portal/conteudo/la-criptograf %C3%ADa-una-guerra-de-piratas-y-corsarios.

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

Popper, K. (2013). *Revisión de su legado*. Recuperado de http://www. academia.edu/27295692/Karl_R._Popper_Revisi%C3%B3n_de_su_legado

Priyadarshini, P., Parshant, N., Narayan, D., Meena, S. (2016). *Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish.*. Publicada en http://www.sciencedirect.com/science/article/pii/S1877050916 001101

Ramió, J. (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, J. (2011). *Tipos de violación a la seguridad informática*. Obtenido de http://wwwcomputacion95.blogspot.pe/2011/04/tipos-de-violacion-la-seguridad. Html

Sánchez, C. (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.

Seclén, J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*. LIMA. Recuperado de http://cybertesis.unmsm.edu.pe/ handle/cybertesis/4884

Shikata, J. (2009). *"Unconditional security"*. Obtenido de http://seglogica ycriptografia.blogspot.pe/2015/12/la-criptografia-criptografia-griego. Html

Shoghi Communications Ltd. (2008) *Seguridad de Comunicaciones*. Obtenido de http://www.shoghicom.com/Spanish/algorithms-customization.html.

TAMCE. (2016). Tecnología avanzada en medidas y contramedidas electrónicas. *Comunicación Segura.* Recuperado de http://tamce.net/categorias/20/ comunicaciones_cifradas.

Torres, C. (2007). *Orientaciones Básicas de Metodología de la Investigación Científica* (9ª Ed.). Lima, Lima: Libros y publicaciones.

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

Xifré, P. (2009). *Antecedentes y perspectivas de estudio en historia de la criptografía*. Universidad Carlos III de Madrid. Obtenido de http://e-archivo.uc3m.es.

ANEXOS

ANEXO 1: Fases comunes de un ataque informático

(Reconocimiento). Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.

(Exploración). En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

(Obtener acceso). En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración.

(Mantener el acceso). Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet.

Borrar huellas: Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red.

ANEXO 2: Matemáticas y seguridad

Matemáticas y seguridad: de la criptografía a la lucha contra el terrorismo

Ángel Martín del Rey
Departamento de Matemática Aplicada
Universidad de Salamanca
delrey@usal.es

Introducción

- El gran desarrollo de las TIC en los últimos años ha dado lugar a una sociedad totalmente dependiente de ellas.
- Caminamos de manera inexorable hacia el pleno establecimiento de la Internet de las Cosas.



Introducción

- Hoy en día los Sistemas Informáticos controlan el buen funcionamiento de multitud de procesos y tareas.
- Cobra especial relevancia la protección de las Infraestructuras Críticas.





Introducción

- Peligros ya existentes se han adaptado al nuevo escenario y otros han aparecido:

Amenazas contra la información

- Espionaje
- Robo y publicación de información clasificada
- Robo y publicación de datos personales
- Robo de la identidad digital
- Fraude


España sufre un récord de asaltos cibernéticos desde Rusia y China

Amenazas contra los sistemas

- Amenazas Persistentes Avanzadas
- Ataques contra infraestructuras críticas
- Ataque contra las redes y sistemas de control
- Infecciones por malware.

Introducción

- Las Matemáticas ofrecen herramientas que permiten analizar, evaluar y gestionar dichas amenazas con el objetivo de minimizar su impacto:
  - Algoritmos criptográficos para proteger la información (confidencialidad, integridad, autenticidad, etc.)
  - Modelos matemáticos para detectar, evaluar y gestionar potenciales amenazas en la red.
  - Etc.

Introducción

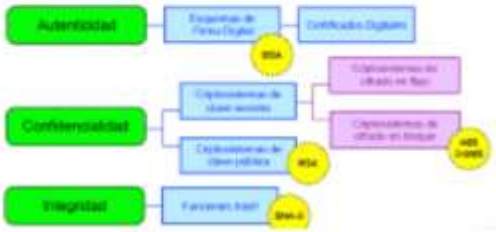
¿Cuál es el organismo, agencia o empresa que más matemáticos contrata y en el que más matemáticos trabajan?

Criptografía: diseño de algoritmos matemáticos para proteger la Información

7

Algoritmo criptográficos: Introducción

- A lo largo de la historia se han utilizado diferentes técnicas para proteger la información.
- El uso de algoritmos matemáticos surge fundamentalmente en el siglo XX en paralelo al desarrollo de los ordenadores.



Algoritmos criptográficos: El DNI electrónico

- En marzo de 2006 comienza la expedición del DNIe.

dni

- En septiembre de 2015 se empieza a expedir la versión 3.0 del DNI electrónico.

Algoritmos criptográficos: El DNI electrónico

- Los algoritmos que tiene implementados la versión 3.0 son los siguientes:
  - Esquema de firma digital RSA (claves de 1024 ó 2048 bits).
  - Función resumen SHA-256.
  - Cifrado de clave secreta:
    - 3-DES CBC (claves de 192 bits)
    - AES (claves de 128 bits)

Algoritmos criptográficos: El DNI electrónico

¿Qué Matemáticas se utilizan en el protocolo de cifrado RSA?

- Cálculo de potencias: m^e
- Cálculo del m.c.d.: m.c.d.(e,φ)
- Cálculo de congruencias: $c = m^e \pmod{n}$

(c es el resto de dividir m^e entre n)

- n es el producto de dos números primos de 2.048 bits (617 cifras decimales).
- La seguridad del RSA reside en la enorme dificultad que supone factorizar el número n.

Algoritmos criptográficos: El DNI electrónico

¿Qué Matemáticas se utilizan en el 3-DES?

- Permutaciones.
- Sustituciones: S-boxes.
- Suma XOR: $0 \oplus 0 = 0 \quad 1 \oplus 0 = 1$ $0 \oplus 1 = 1 \quad 1 \oplus 1 = 0$

Algoritmos criptográficos: El DNI electrónico

¿En qué se basan las función resumen SHA-256?

- La función resumen SHA-256 asigna a una cadena de bits de longitud arbitraria (Gb, Mb,…) una secuencia de 256 bits (resumen) de manera que:
  - Es muy sencillo calcular la secuencia de 256 bits.
  - Es computacionalmente muy difícil encontrar dos mensajes que tengan el mismo resumen.

Algoritmos criptográficos: El DNI electrónico

Algoritmos criptográficos: Seguridad

Ataques al algoritmo

- "Romper" un criptosistema de clave pública conlleva resolver un problema matemático muy difícil (seguridad computacional):
  - factorización de números enteros (RSA)
    - ➡ se ha conseguido factorizar un RSA-768
- Un ordenador cuántico sería capaz de romper el RSA y, en menor medida ECC (criptosistemas de curvas elípticas: *el plan B*).
  - El algoritmo cuántico de Shor consigue factorizar números muy grandes en tiempo polinómico.

Algoritmos criptográficos: Seguridad

Ataques por canal lateral

- Aprovechan las debilidades de las implementaciones de los algoritmos matemáticos.
- En 2013, Genkin, Shamir y Tromer consiguieron romper una clave RSA-4096 en 1 hora gracias al análisis del sonido emitido por el portátil mientras descifraba algunos mensajes.

Algoritmos criptográficos: Otras aplicaciones

- Identificación amigo/enemigo.
- Póquer *on-line*.
- Venta o intercambio de secretos.
- Reparto de secretos.
- Votación electrónica.
- Descubrimiento mínimo o nulo.

Algoritmos criptográficos: Los servicios secretos

- Inventores *públicos* de la "Criptografía de Clave Pública"

- Ralph Merkle.
- Martin Edward Hellman. 1976
- Bailey Whitfield Diffie.

- Inventores *reales* de la "Criptografía de Clave Pública"

- Clifford Christopher Cocks.
- Malcolm John Williamson. 1973
- James Henry Ellis

Algoritmos criptográficos: Los servicios secretos

- El GCHQ es el homólogo británico a la NSA americana

Government Communications Headquarters
(Reino Unido)

11

Algoritmos criptográficos: Los servicios secretos

- No solo Estados Unidos y el Reino Unido poseen una agencia de este tipo...

Special Communications Service
(Rusia)

Agence Nationale de la sécurité des systèmes d'information
(Francia)

Centro Criptológico Nacional
(España)

2

Algoritmos criptográficos: Usos maliciosos

- Los terroristas también usan estas tecnologías...

Aplicación *Amn Al-Mujahed* (AES, RSA-4096)

2

Algoritmos criptográficos: ¡Últimas noticias!

- A mediados de agosto de 2015, la NSA (National Security Agency) presenta nuevas directivas en las que recomienda...
  - No migrar los sistemas funcionando bajo RSA a ECC.
  - Diseñar nuevos estándares resistentes a los algoritmos cuánticos (*criptografía post-cuántica*).
- Muchas elucubraciones en la comunidad científica...
  - ¿Han roto el RSA?
  - ¿Han construido un ordenador cuántico?
  - ¿Han roto la ECC?
  - ...

21

ANEXO 3: Manual de Usuario del Sistema de Seguridad integrado con el algoritmo propio ANN

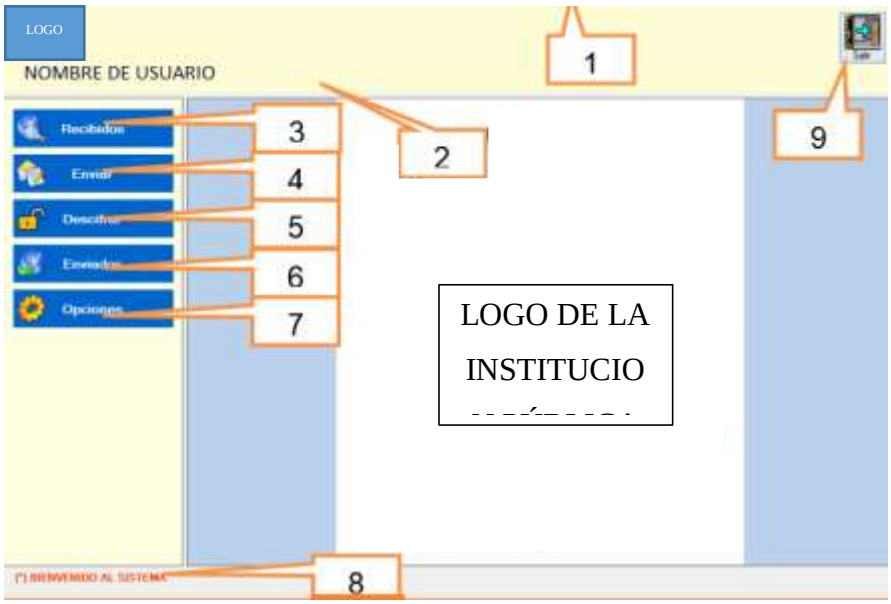
Modo en Línea

a. Ingreso al sistema

Para ingresar al sistema, el usuario deberá realizar los siguientes pasos:

- ✓ Ingresar el USUARIO (Ver imagen opción 1)
- ✓ Ingresar la CONTRASEÑA (Ver imagen opción 2)
- ✓ Hacer Clic en el botón CONECTAR (Ver imagen opción 3)

b. Menú del sistema



El sistema tiene las siguientes partes:

- ✓ **Nombre del usuario (1):** Muestra el usuario que ha ingresado al sistema.
- ✓ **Nombre de la unidad (2):** Muestra la unidad al cual pertenece el usuario que ha ingresado al sistema.

- ✓ **Opción Recibidos (3):** Opción donde se muestra los mensajes recibidos por el usuario. Muestra un máximo de 150 mensajes.

- ✓ **Opción Enviar (4):** Opción donde el usuario puede enviar información a los usuarios del sistema.

- ✓ **Opción Descifrar (5):** Opción donde el usuario puede DESCIFRAR información.

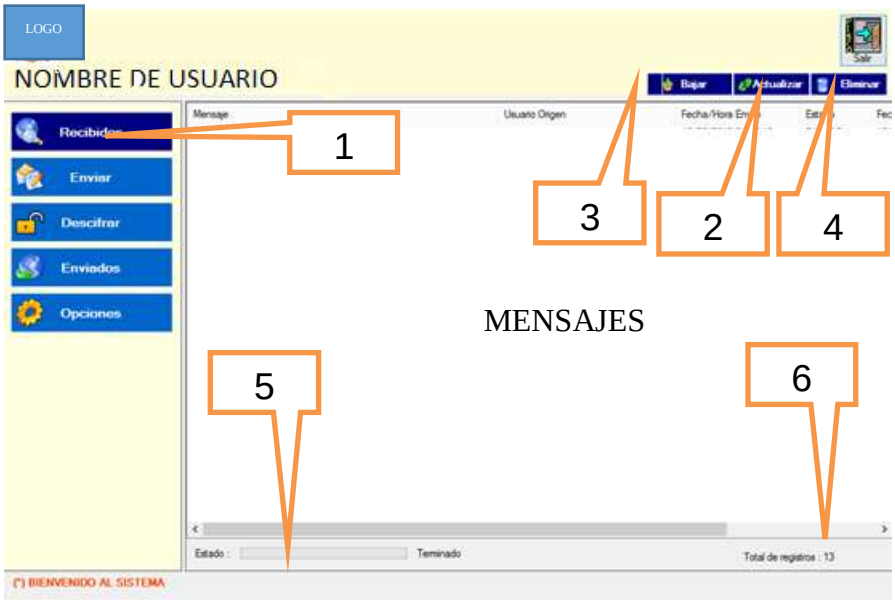
- ✓ **Opción Enviados (6):** Opción donde el usuario puede ver el estado de sus mensajes enviados. Muestra un máximo de 300 mensajes.

- ✓ **Opciones (7):** Opción donde el usuario puede cambiar algunos parámetros básicos para el funcionamiento del sistema.

- ✓ **Mensaje del Administrador (8):** El administrador va a enviar mensajes a todos los usuarios del sistema, como por ejemplo en caso de corte de fluido eléctrico u otro que crea conveniente.

- ✓ **Salir del sistema:** Para salir del sistema, hacer Clic en el botón **Salir (9).**

c. <u>Ver archivos recibidos</u>



Para ver la información recibida, el usuario debe de hacer Clic en la opción de **Recibidos (1)**.

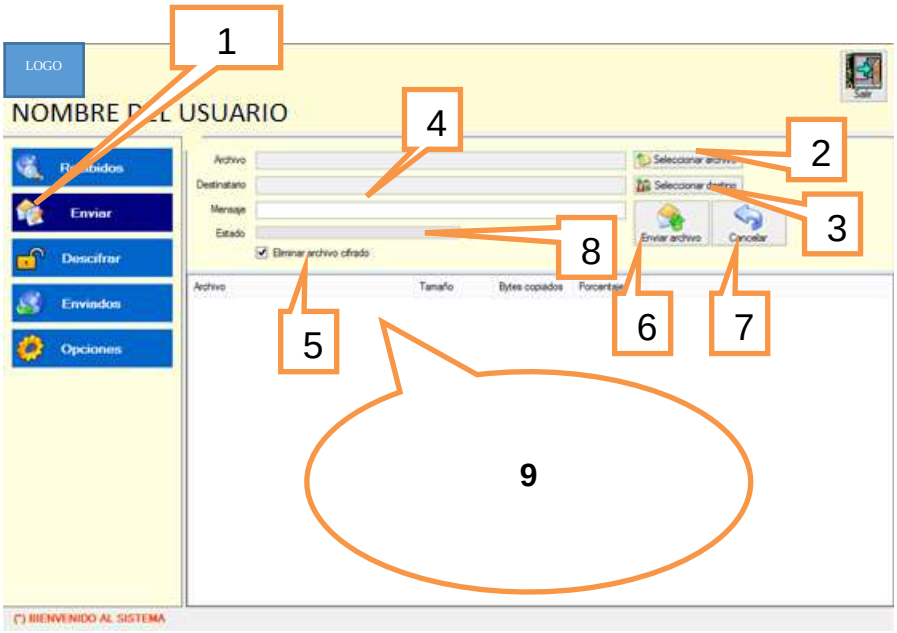
En esta opción podemos hacer tres (03) procesos:

- ✓ **Proceso de Actualizar:** Para ver la información recibida, el usuario debe de hacer un Clic en el botón **Actualizar (2)**. Se muestra el total de registros **(6)**.

- ✓ **Proceso de Bajar:** Para bajar información, el usuario debe de hacer Clic en el botón de **Bajar (3)**. El usuario debe observar que la barra de progreso **(5)** termine.

- ✓ **Proceso de Eliminar:** El usuario debe seleccionar el mensaje que desea eliminar y luego hacer Clic en el botón **Eliminar (4)**. Aparecerá un mensaje donde advierte que va a eliminar el mensaje. Si realmente se va a eliminar el usuario debe aceptar el mensaje.

d. <u>Enviar archivo</u>



Para enviar información, el usuario debe de hacer Clic en la opción de **Enviar (1)**.

Los pasos son los siguientes:

- ✓ **Seleccionar archivo (2)**: El usuario debe hacer Clic en esta opción para seleccionar la información que va a enviar.

- ✓ **Seleccionar destino (3)**: El usuario debe hacer Clic en esta opción para seleccionar los destinatarios. Aparecerá una ventana donde se muestra los usuarios disponibles.

- ✓ **Mensaje (4)**: Para enviar la información a los usuarios, se debe ingresar obligatoriamente un mensaje.

- ✓ **Opción de Eliminar archivo cifrado (5)**: Esta opción permite mantener el archivo cifrado luego de ser enviado. El archivo cifrado quedará almacenado en la ruta **"….."**. La opción por defecto es Eliminar archivo cifrado.

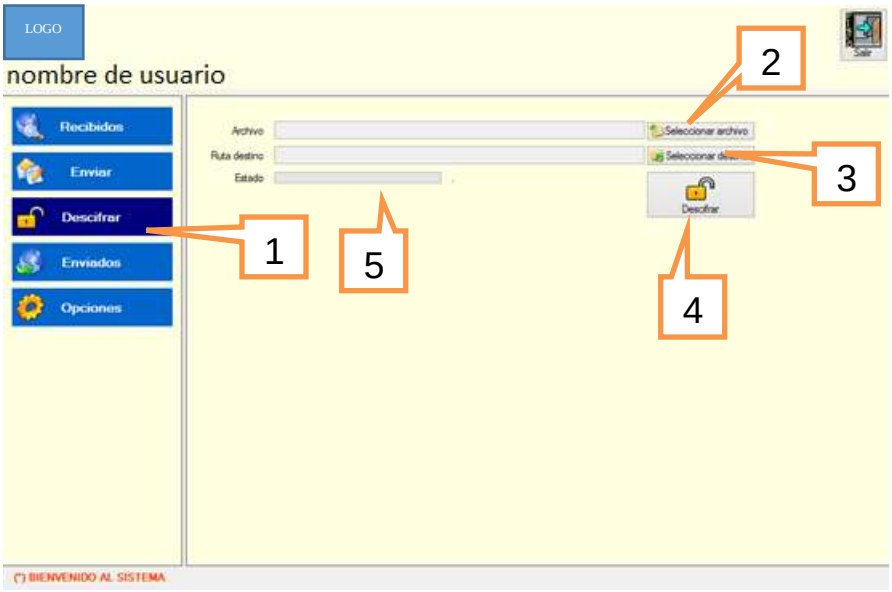
- ✓ **Enviar archivo (6)**: Hacer Clic en este botón para enviar la información.

- ✓ **Enviar archivo (7)**: Hacer Clic en este botón para cancelar la operación.

- ✓ **Estado del Archivo (8)**: En esta área se muestra el estado del archivo.

- ✓ **Área de archivos enviados (9)**: En esta área se muestra temporalmente todos los archivos enviados antes de cerrar el sistema.

e. Descifrar información



Para Descifrar una archivo, el usuario debe de hacer Clic en la opción de **Descifrar (1)**.

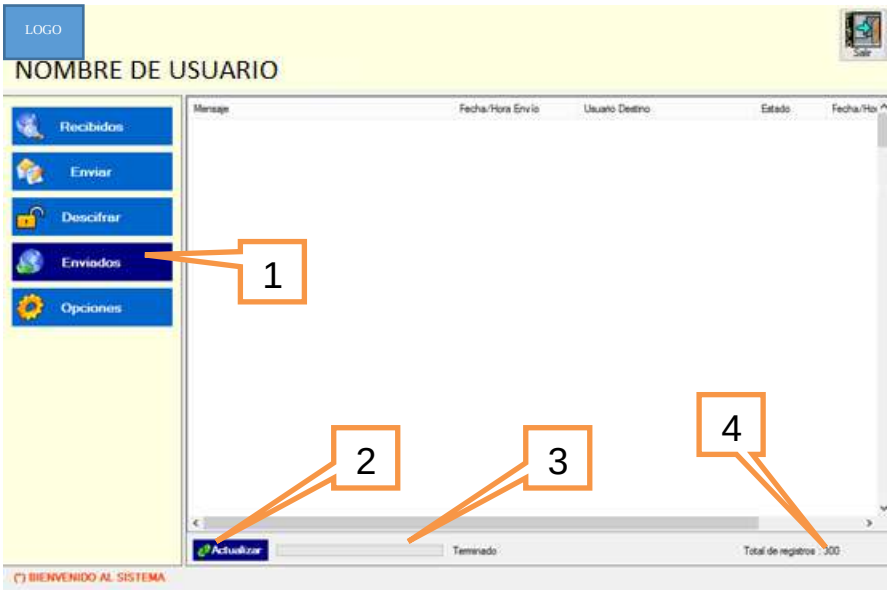
Los pasos son los siguientes:

- ✓ **Seleccionar archivo (2)**: En esta opción, el usuario deberá hacer Clic para seleccionar el archivo que va a descifrar.

- ✓ **Seleccionar destino (3)**: En esta opción, el usuario debe seleccionar donde va a ser almacenado el archivo descifrado.

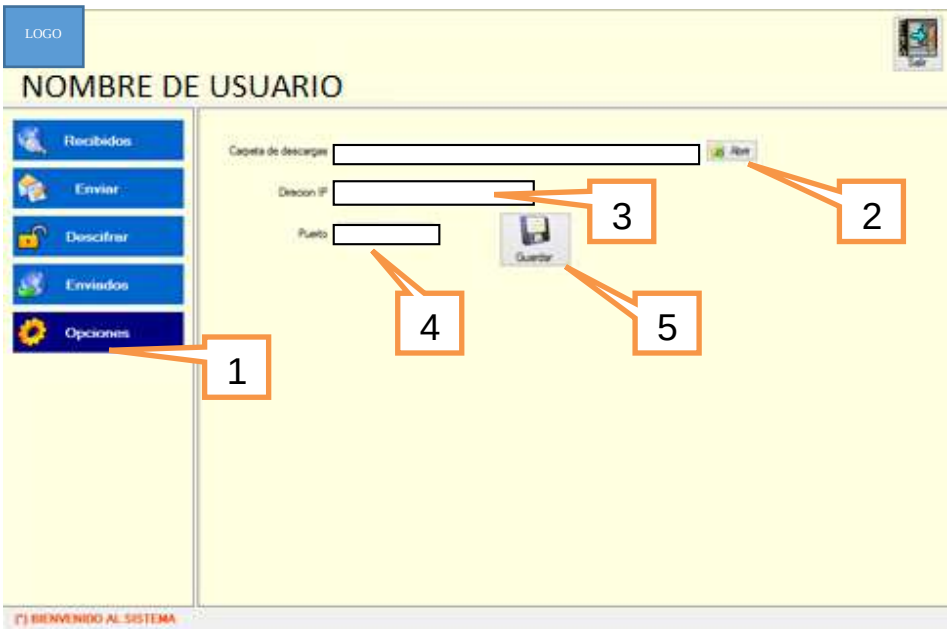
- ✓ **Descifrar (4)**: Hacer Clic en este botón para descifrar el archivo. Observar la **barra de progreso (5)**, donde se muestra el avance de descifrado.

f. Ver archivos enviados



Para ver el estado de los archivos enviados, el usuario debe de hacer Clic en la opción de **Enviados (1)**, luego hacer Clic en el botón **Actualizar (2)**. Es muy probable que tarde debido al ancho de banda del internet, para ello ver la **barra de progreso (3)**. Al final se observara el **total de registros (4)**.

g. <u>Opciones del sistema</u>



Para cambiar algunos parámetros para el funcionamiento del sistema, el usuario debe de hacer Clic en **Opciones (1)**.

Las opciones disponibles son:

- ✓ **Carpeta de descargas**: Representa la ubicación donde se va a descargar los archivos.

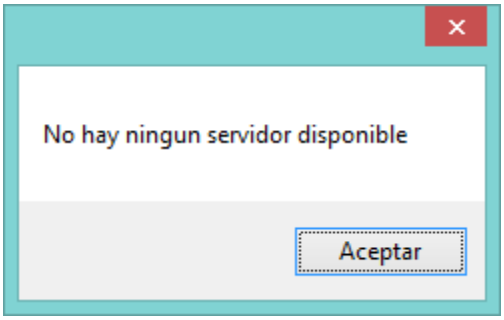
- ✓ **Dirección IP**: Representa la dirección del servidor. **No cambiar a menos que el Administrador del sistema lo disponga.**

- ✓ **Puerto**: Representa el puerto del servidor. **No cambiar a menos que el Administrador del sistema lo disponga.**

Modo Fuera de Línea

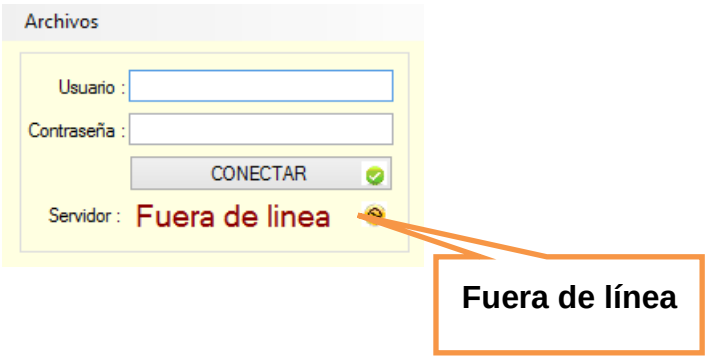
Cuando el usuario quiera ingresar al sistema y aparece el siguiente mensaje, se puede deber a los siguientes casos:

- ✓ El servidor no está disponible.
- ✓ No se ha ingresado a la red VPN.
- ✓ Los parámetros de dirección IP y Puerto no son los correctos.



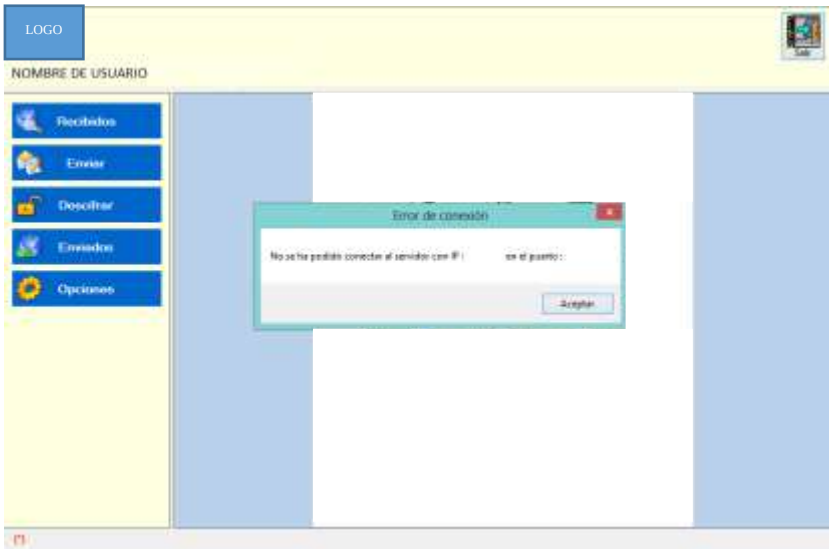
Al hacer Clic en el botón Aceptar, aparece la ventana para ingresar las credenciales mostrando el mensaje de **Fuera de línea**.

a. Ingreso al sistema

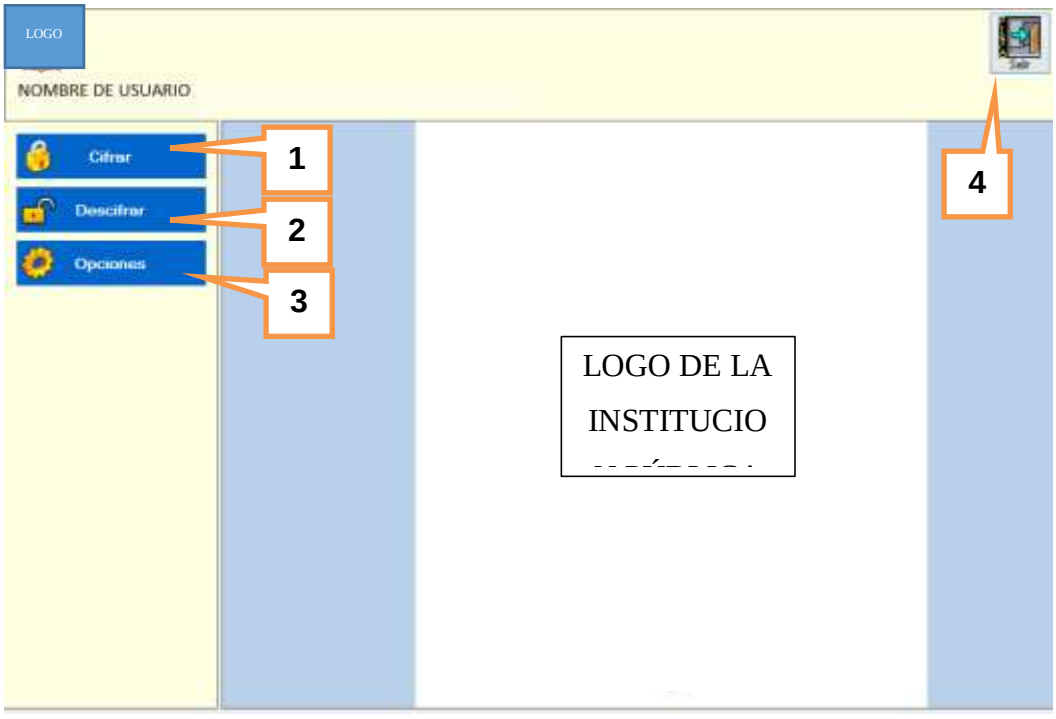


Al ingresar las credenciales y hacer Clic en CONECTAR, es muy probable que ingrese en **modo en línea** siempre y cuando se haya solucionado el problema de red (VPN), de

lo contrario se mostrará un mensaje advirtiendo que no se ha podido ingresar con los datos existentes (dirección IP y Puerto).



b. <u>Menú del sistema</u>



El sistema tiene las siguientes partes:

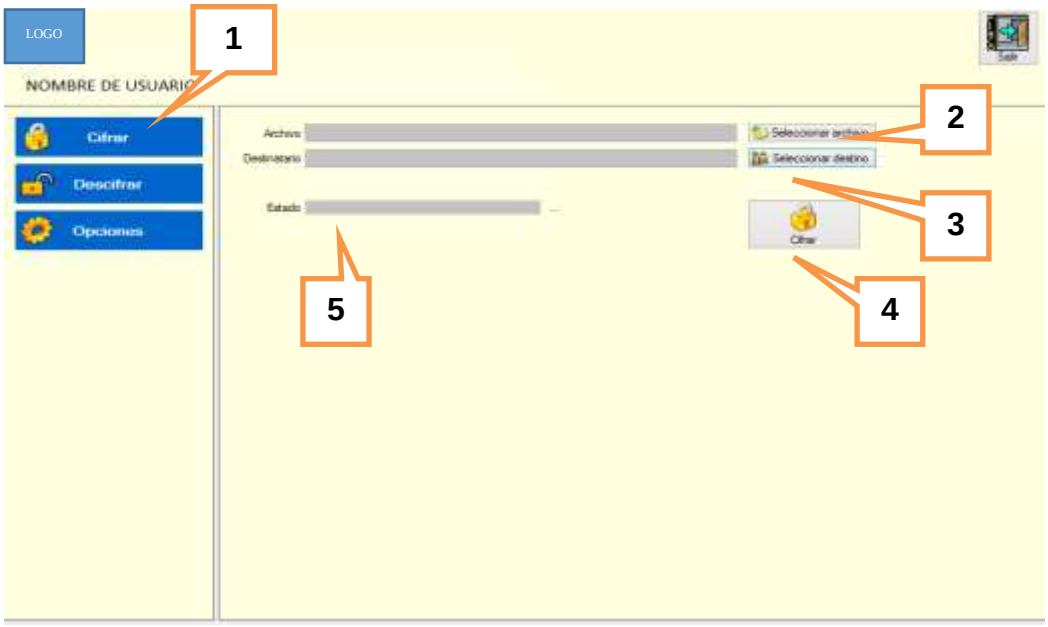
✓ **Opción Cifrar (1):** Opción donde el usuario puede CIFRAR información.

✓ **Opción Descifrar (2):** Opción donde el usuario puede DESCIFRAR información.

✓ **Opciones (3):** Similar a Modo en línea.

✓ **Salir (4)**: Botón para salir del sistema.

c. Cifrar información



Para cifrar un archivo, el usuario debe de hacer Clic en la opción de **Cifrar (1)**.

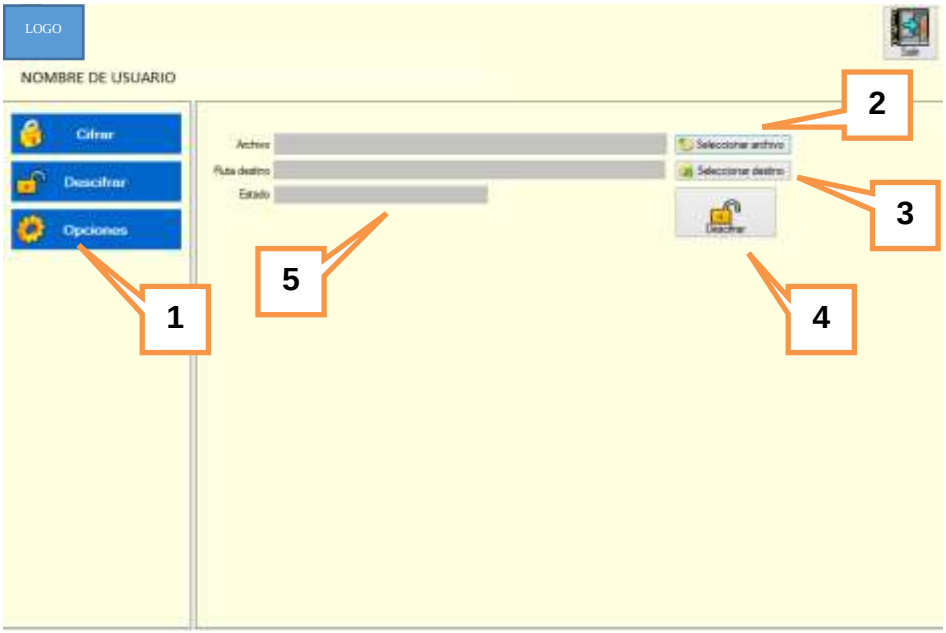
Los pasos son los siguientes:

✓ **Seleccionar archivo (2)**: El usuario debe hacer Clic en esta opción para seleccionar la información que va a enviar.

✓ **Seleccionar destino (3)**: El usuario debe hacer Clic en esta opción para seleccionar los destinatarios. Aparecerá una ventana donde se muestra los usuarios disponibles.

✓ **Cifrar (4)**: Hacer Clic en este botón para cifrar el archivo. Ver al avance del proceso de cifrado en la **barra de progreso (5)**.

d. Descifrar información



Para Descifrar una archivo, el usuario debe de hacer Clic en la opción de **Descifrar (1)**.

Los pasos son los siguientes:

- ✓ **Seleccionar archivo (2)**: En esta opción, el usuario deberá hacer Clic para seleccionar el archivo que va a descifrar.

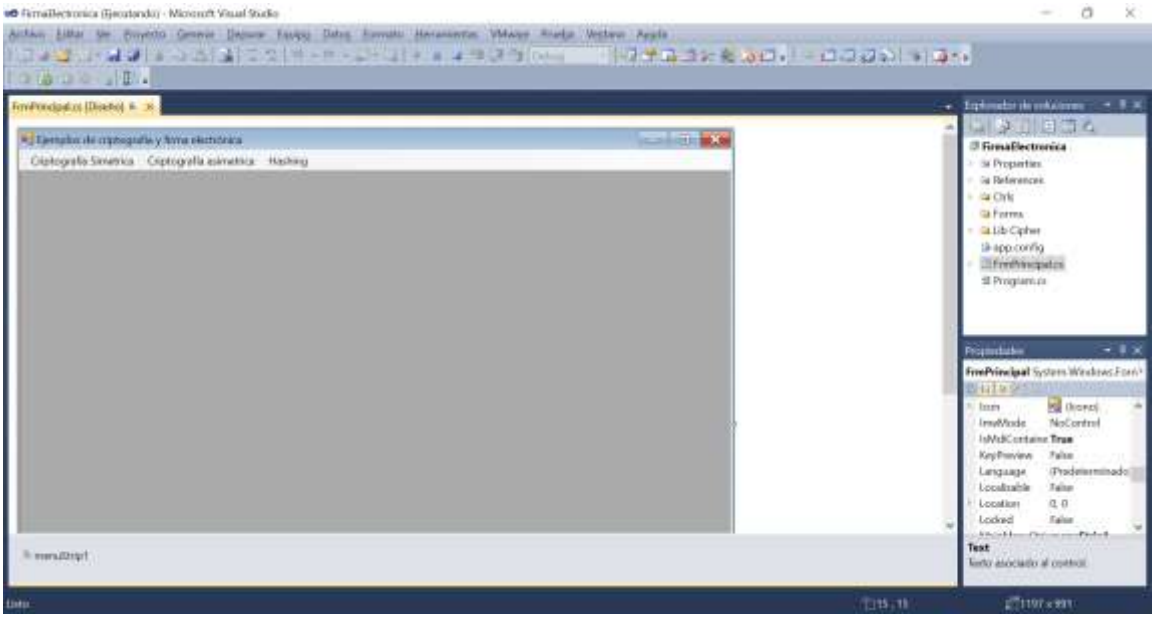
- ✓ **Seleccionar destino (3)**: En esta opción, el usuario debe seleccionar donde va a ser almacenado el archivo descifrado.

- ✓ **Descifrar (4)**: Hacer Clic en este botón para descifrar el archivo. Observar la **barra de progreso (5)**, donde se muestra el avance de descifrado.

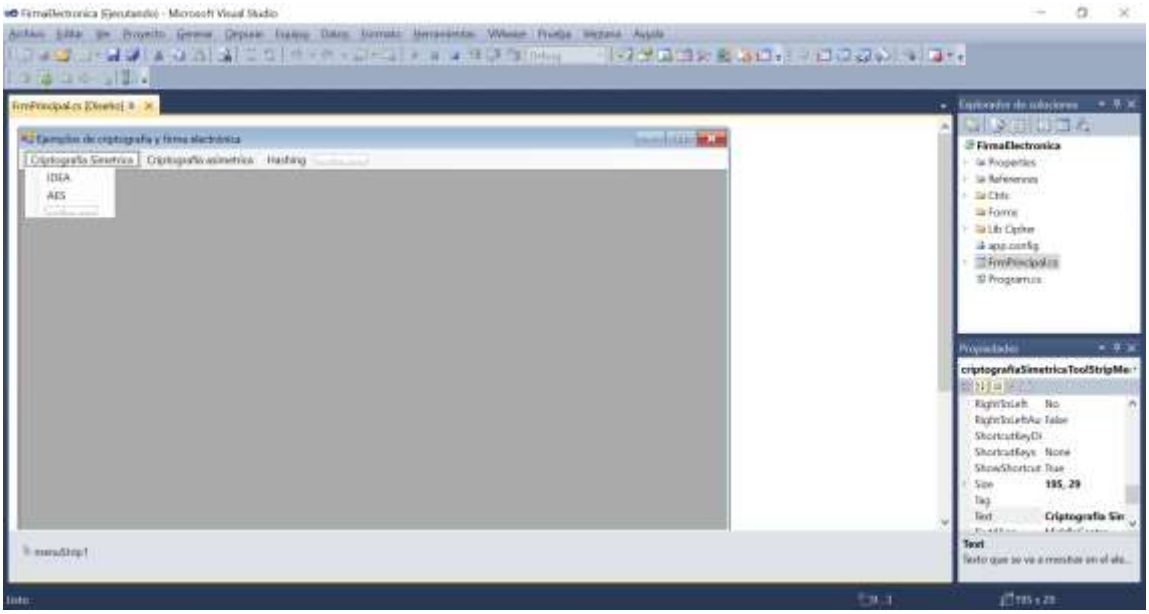
ANEXO 4: Sistema de cifrado

El sistema tiene la funcionalidad de trabajar con los algoritmos criptográficos globalmente conocidos y elegidos por conveniencia.

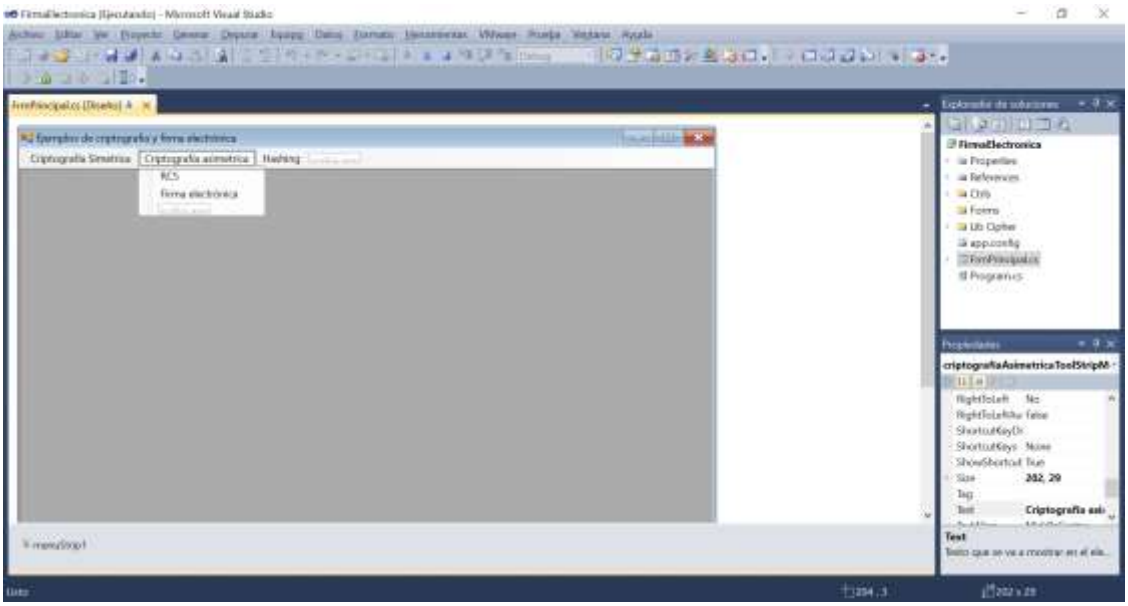
En la pantalla principal se muestran las opciones de tipos de criptografía a utilizar: Criptografía simétrica y criptografía asimétrica.



En la pestaña de Criptografía Simétrica, se encuentra el algoritmo IDEA y AES.



En la pestaña de Criptografía Asimétrica, se encuentra el algoritmo RC5.



Mensaje en claro

El siguiente mensaje fue utilizado para ser cifrado con cada uno de los algoritmos criptográficos con la finalidad de conseguir los criptos que se evaluaron y fueron sometidos a pruebas.

Aquí la solución para el peligroso malware 'Wanna Cry'

La clave es actualizar el sistema operativo Windows y activar varios servicios de seguridad en tu PC incluyendo tu antivirus

La propagación en todo el mundo del "malware" "Wanna Cry" sigue imparable y afecta a varias computadoras en el Perú así como en otros 99 países. Ante ello diversas compañías de **seguridad informática y entidades** buscan soluciones inmediatas para superar este problema, no obstante la solución pasa por una actualización clave de Windows.

Si usted tiene una versión pirata del sistema operativo **Windows** y ya fue contaminado por el peligroso malware será poco probable que pueda salir de este percance. Lo cierto es que el peligroso "**Wanna Cry**" no solo extrae información de las computadoras sino que estas se convierten en una suerte de rehenes exclusivos.

Lo peor es que usted al siguiente se dará cuenta de la actuación de este **malware** pues sus sistemas cifrados para extraer **información bancaria, clave de email** y otros elementos que pueden estar guardados en tu PC.

Pero, **¿qué debe hacer usted para solucionare este problema?** Pues no se trata solo de actualizar el antivirus original que usted posee sino que es vital actualizar Windows (sistema operativo de la PC) según Kaspersky Lab.

- **Instale el parche oficial de Microsoft que cierra la vulnerabilidad** utilizada en el ataque. (Buscar actualizaciones en Windows)
- Asegúrese de que **las soluciones de seguridad estén habilitadas** en todos los nodos de la red. (Windows defender, Firewall, etc)
- Si utiliza la solución de **Kaspersky Lab, asegúrese de que incluya el System Watcher,** un componente de detección proactivo de comportamiento y que esté habilitado
- Ejecute el **Scan de Área Crítica en la solución de Kaspersky Lab** para detectar una posible infección. Si antes posible (de lo contrario, se detectará automáticamente dentro de 24 horas, si no se deshabilita).
- Reinicie el sistema **después de detectar MEM: Trojan.Win64.EquationDrug.gen**
- Utilice los servicios de Terminal de Inteligencia de Amenazas específicos para clientes de su antivirus

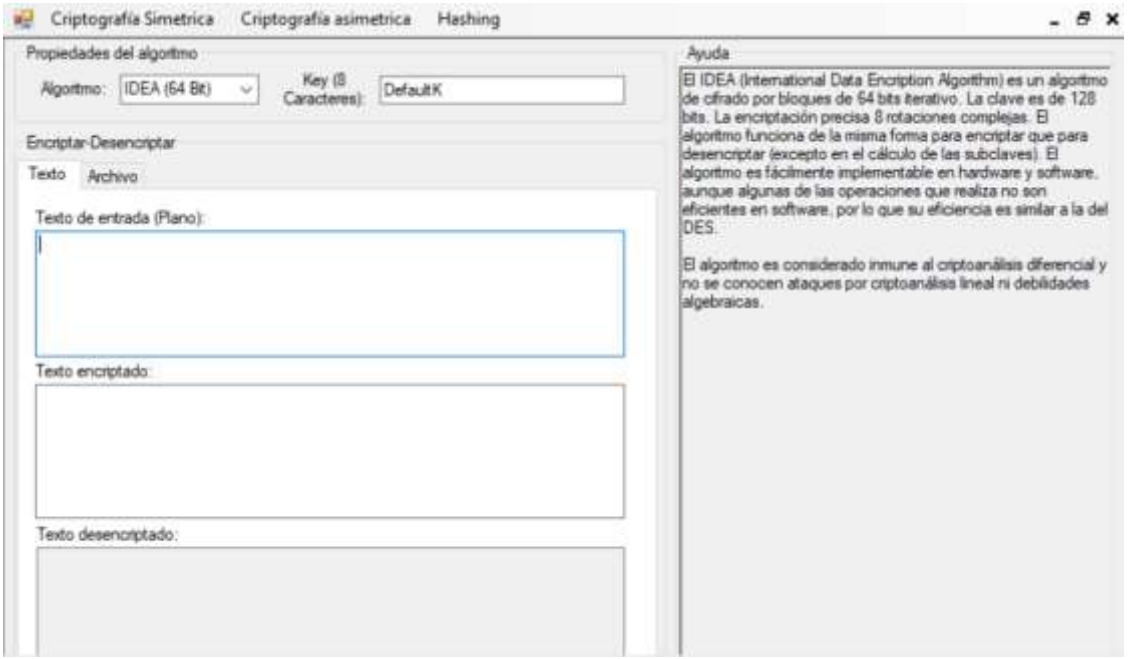
Mapa del avance del "**malware**" "**Wanna Cry**" en el mundo

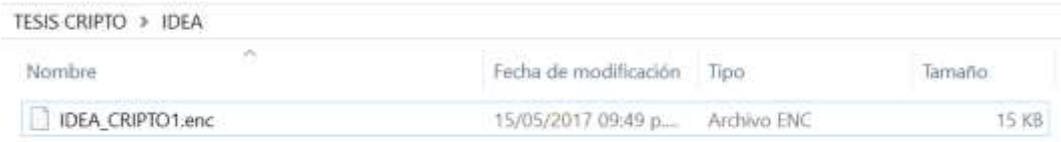
Los expertos de **Kaspersky Lab** están actualmente tratando de determinar si es posible descifrar los datos bloqueados en este ataque con el objetivo de desarrollar una herramienta de descifrado tan pronto como sea posible. Las soluciones de seguridad de Kaspersky Lab detectan el malware utilizado en este ataque por los siguientes nombres de detección:

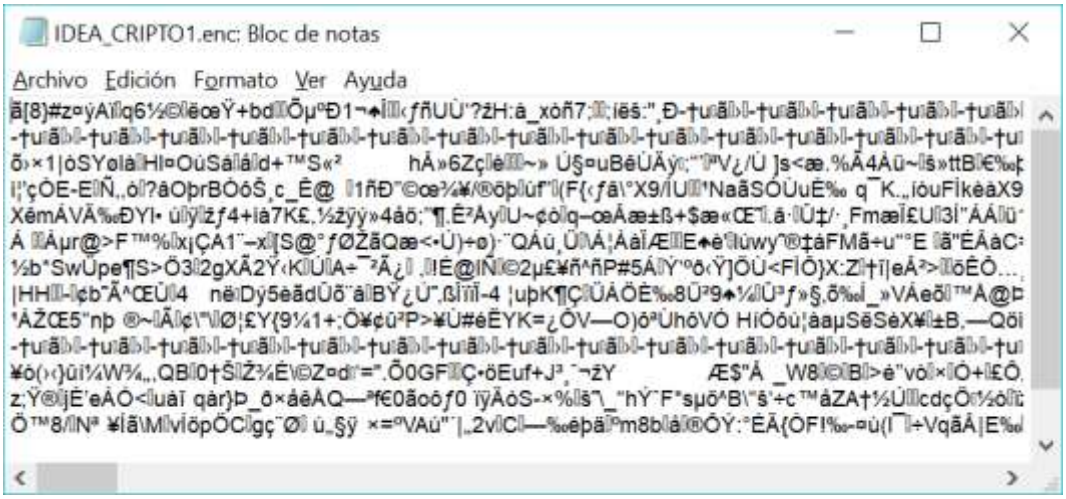
- Trojan-Ransom.Win32.Scatter.af
- Trojan-Ransom.Win32.Scatter.ln
- Trojan-Ransom.Win32.Fury.fl
- Trojan-Ransom.Win32.Gen.tjkl
- Trojan-Ransom.Win32.Wanna.b
- Trojan-Ransom.Win32.Wanna.c
- Trojan-Ransom.Win32.Wanna.d
- Trojan-Ransom.Win32.Wanna.f
- Trojan-Ransom.Win32.Zapchast.i
- Trojan.Win64.EquationDrug.gen
- Trojan.Win32.Generic (el componente System Watcher del sistema debe estar habilitado)

Algoritmos globalmente conocidos

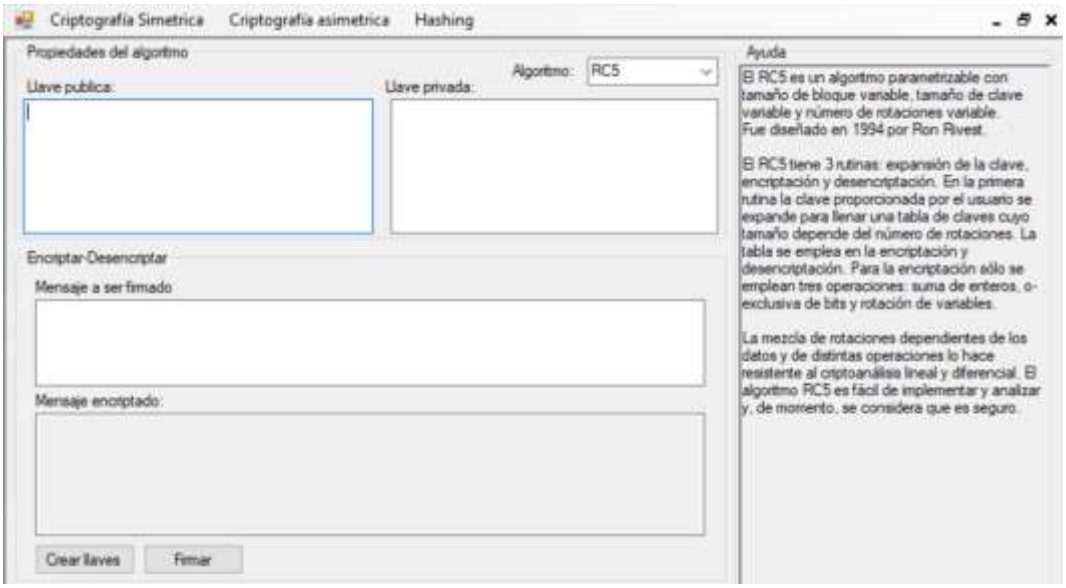
1. Algoritmo IDEA

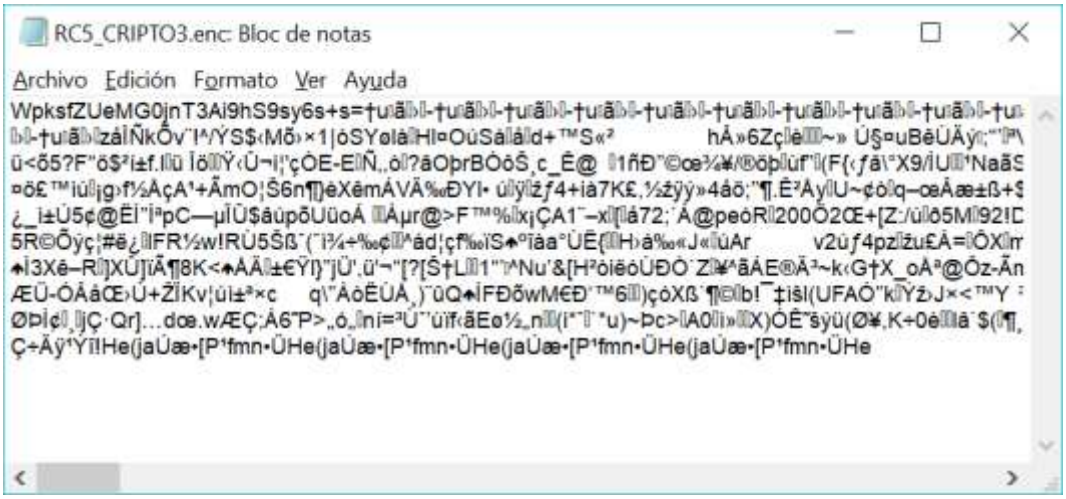




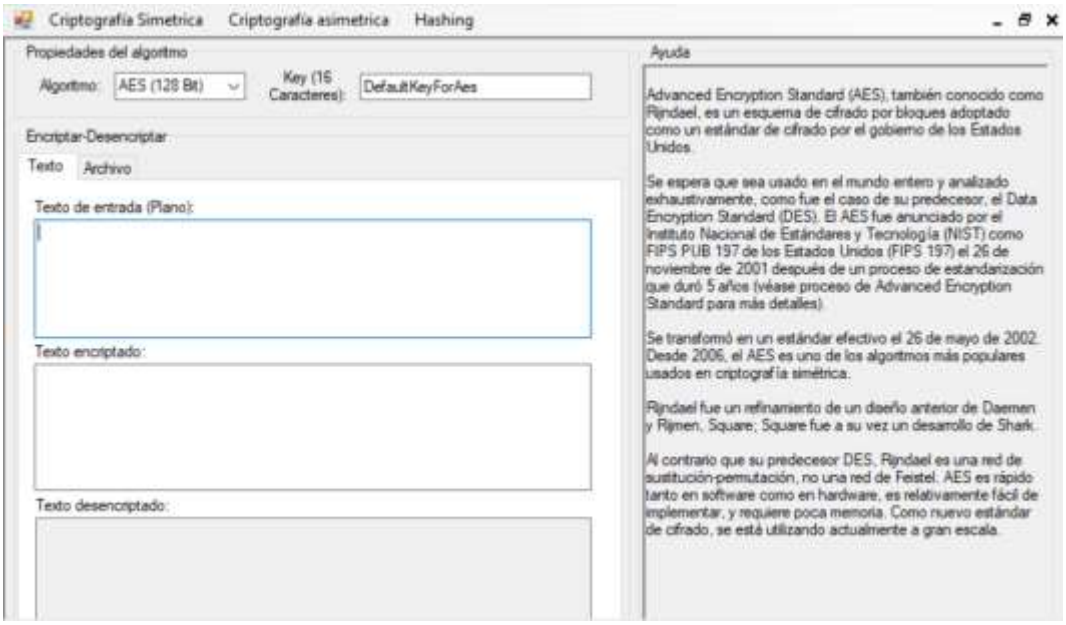


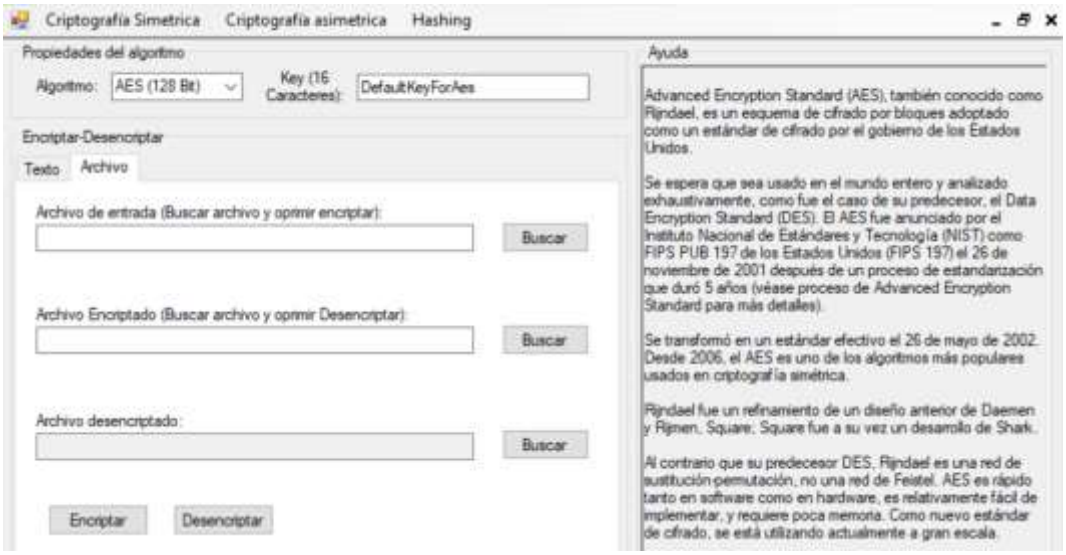
2. **Algoritmo RC5**



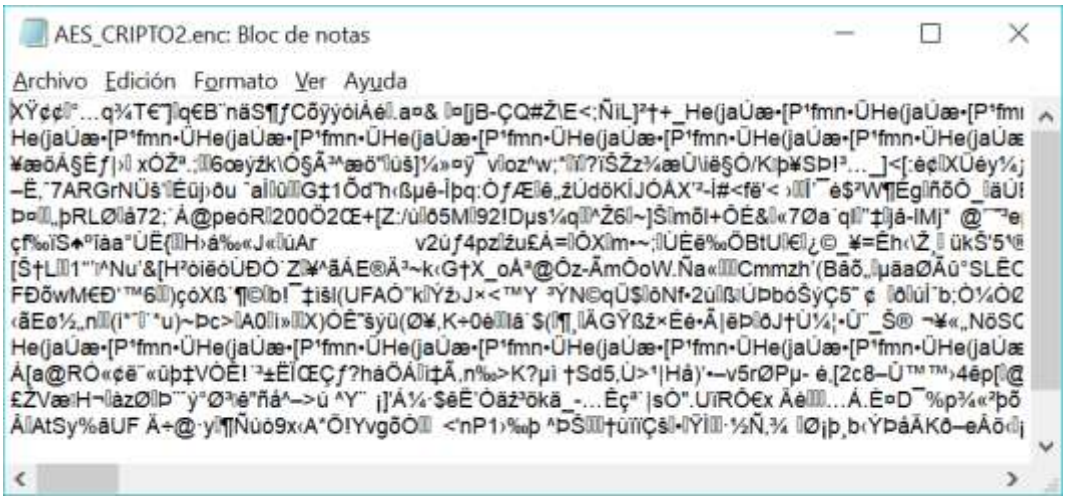


3. **Algoritmo AES**




Criptografía Simetrica
Criptografía asimetrica
Hashing
Propiedades del algoritmo
Algoritmo:
AES (128 Bit)
Key (16 Caracteres):
DefaultKeyForAes
Encriptar-Desencriptar
Texto
Archivo
Archivo de entrada (Buscar archivo y oprimir encriptar):
Buscar
Archivo Encriptado (Buscar archivo y oprimir Desencriptar):
Buscar
Archivo desencriptado:
Buscar
Encriptar
Desencriptar
Ayuda
Advanced Encryption Standard (AES), también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.
Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el Data Encryption Standard (DES). El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años (véase proceso de Advanced Encryption Standard para más detalles).
Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.
Rijndael fue un refinamiento de un diseño anterior de Daemen y Rijmen, Square; Square fue a su vez un desarrollo de Shark.
Al contrario que su predecesor DES, Rijndael es una red de sustitución-permutación, no una red de Feistel. AES es rápido tanto en software como en hardware, es relativamente fácil de implementar, y requiere poca memoria. Como nuevo estándar de cifrado, se está utilizando actualmente a gran escala.


TESIS CRIPTO › AES
Nombre
Fecha de modificación
Tipo
Tamaño
AES_CRIPTO2.enc
15/05/2017 09:51 p...
Archivo ENC
15 KB


AES_CRIPTO2.enc: Bloc de notas
Archivo Edición Formato Ver Ayuda

4. **Algoritmo propio ANN**

Se utilizó en su propio sistema de cifrado, pero para la evaluación y las pruebas se usó el mensaje claro elegido.