ESTUDIO DE EFICIENCIA Y EFICACIA DE LOS ALGORITMOS CRIPTOGRÁFICOS RSA, AES, IDEA y RC4 EN LA SEGURIDAD INFORMÁTICA

EDISSON ESTEBAN ALVARADO PRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO, COLOMBIA
2020

ESTUDIO DE EFICIENCIA Y EFICACIA DE LOS ALGORITMOS CRIPTOGRÁFICOS RSA, AES, IDEA, RC4 EN LA SEGURIDAD INFORMÁTICA

ESP. EDISSON ESTEBAN ALVARADO PRADO

MONOGRAFÍA

Proyecto de grado para optar al título de:
Especialista en seguridad informática

Director del proyecto:
Ing. Edgar Roberto Dulce

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO, COLOMBIA
2020

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Pasto, julio de 2020

Dedicatoria

El presente trabajo es dedicado a mis padres, quienes siempre me apoyaron y me alentaron a continuar constantemente. A Milena y nuestra hija, quienes son la principal motivación para alcanzar nuevos logros cada día. A Dios, por brindarme paciencia, esperanza, sabiduría y la fuerza para superar cada dificultad en mi vida.

RESUMEN

Hoy en día la información se transmite de un lugar a otro y medios como Internet hacen que dicha información no se mantenga segura, pues en cualquier momento los atacantes informáticos intentarán acceder a ella con el fin de causar daños, modificarla y alterarla para beneficios mal intencionados. Es por ello, que en esta monografía se propone un estudio de algunos métodos y algoritmos criptográficos como Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Ron's Code número 4 (RC4) y Rivest, Shamir y Adleman (RSA), como sistema de seguridad informática para asegurar la información. De estos algoritmos, se determina características principales, su eficiencia y beneficios frente a las amenazas informáticas.

Palabras clave: algoritmo criptográfico, AES, IDEA, RC4, RSA, seguridad informática, seguridad de la información, amenazas informáticas.

ABSTRACT

Currently, information is transmitted from one place to another and media such as the Internet do not keep this information secure, because at any time the computer attackers will try to access it in order to cause damage, modify it and alter it for ill-intentioned benefits. That is why, in this monograph we propose a study of some cryptographic methods and algorithms such as Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Ron's Code number 4 (RC4) and Rivest, Shamir and Adleman (RSA), as a computer security system to secure information. From these algorithms, the main characteristics, their efficiency and benefits against computer threats are determined.

Keywords: cryptographic algorithm, AES, IDEA, RC4, RSA, computer security, information security, computer threats.

CONTENIDO

Pág.

INTRODUCCIÓN 13
1. EL PROBLEMA DE INVESTIGACIÓN 14
1.1. DESCRIPCIÓN 14
1.2. FORMULACIÓN 14
1.3. OBJETIVOS 14
1.3.1. Objetivo general. 14
1.3.2. Objetivos específicos. 14
1.4. JUSTIFICACIÓN 15
1.5. DELIMITACIÓN 15
2. MARCO DE REFERENCIA 16
2.1. ANTECEDENTES 16
2.2. MARCO TEORICO 18
2.3. MARCO CONCEPTUAL 19
2.3.1. Criptografía. 19
2.3.2. Pilares de la Seguridad Informática. 19
2.3.3. Seguridad Informática. 20
2.3.4. Seguridad de la información. 20
2.3.5. Aritmética modular. 20
2.3.6. Algoritmo criptográfico. 21
2.3.7. Inverso multiplicativo modular. 22
2.3.8. Números primos. 22
2.3.9. Operadores Bits a Bits. 22
2.3.10. Amenaza a la información. 23
2.3.11. Algoritmo de Fermat. 23
2.3.12. Criptografía simétrica. 24
2.3.13. Cifrado asimetrico. 24
2.3.14. Eficiencia de un algoritmo criptográfico. 25
2.3.15. Eficacia de un algoritmo criptográfico. 25

2.3.16. Promedio. 26
2.3.17. Rendimiento de un algoritmo. 26
2.4. MARCO LEGAL 26
2.4.1. Ley 1273 de 2009. 26
2.4.2. Ley 1581 de 2012. 27
2.4.3. Ley 1928 de 2018. 27
2.4.4. Ley 527 de 1999. 28
3. RESULTADOS 28
3.1. CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA 28
3.2. DESCRIPCIÓN DE LOS ALGORITMOS DE CIFRADO 31
3.2.1. RSA (Rivest, Shamir, Adleman). 31
3.2.2. AES (Advanced Encryption Standard). 32
3.2.3. IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM) 41
3.2.4. RC4 (RIVEST CIPHER 4) 43
3.3. CARACTERÍSTICAS DE LOS ALGORITMOS 44
3.4. EFICIENCIA DE LOS ALGORITMOS RSA, AES, IDEA Y RC4 45
3.4.1. Eficiencia RSA. 45
3.4.2. Eficiencia AES. 47
3.4.3. Eficiencia IDEA. 49
3.4.4. Eficiencia RC4. 50
3.5. COMPARACIÓN DE RENDIMIENTO DE LOS ALGORITMOS 52
3.6. ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS FRENTE A AMENAZAS INFORMÁTICAS 53
3.7. SEGURIDAD DE LOS ALGORITMOS CRIPTOGRÁFICOS 54
3.7.1. Seguridad de RSA. 54
3.7.2. Seguridad de AES. 54
3.7.3. Seguridad de IDEA. 55
3.7.4. Seguridad de RC4. 55
3.8. ATAQUES A LOS ALGORITMOS CRIPTOGRAFICOS 56
3.8.1. Ataques a RSA. 56
3.8.2. Ataques a AES. 57

3.8.3. Ataques a IDEA. 59
3.8.4. Ataques A RC4. 60
3.9. SÍNTESIS DEL ESTUDIO 61
4. CONCLUSIONES 62
RECOMENDACIONES 63
BIBLIOGRAFÍA 64
ANEXOS 75

LISTA DE TABLAS

Pág.

Tabla 1. Operador NOT 22
Tabla 2. Operador AND 22
Tabla 3. Operador OR 23
Tabla 4. Operador XOR 23
Tabla 5. Cifrado y descifrado de subclaves 42
Tabla 6. Características de los algoritmos RSA, IDEA, AES, RC4 45
Tabla 7. Tiempo de cifrado y descifrado RSA 46
Tabla 8. Tiempo de cifrado y descifrado AES 48
Tabla 9. Tiempo de cifrado y descifrado IDEA 49
Tabla 10. Evolución tiempo de cifrado RC4 51
Tabla 11. Evolución tiempo de descifrado RC4 51
Tabla 12. Rendimiento RC4 52
Tabla 13. Rendimiento descifrado RC4 52
Tabla 14. Combinaciones posibles de "UNAD" 58
Tabla 15. Resumen seguridad algoritmos criptográficos 61

LISTA DE FIGURAS

Pág.

Figura 2. Cifrado simétrico 24
Figura 3. Cifrado asimétrico 25
Figura 4. Funcionamiento algoritmo AES 28
Figura 5. Matriz de estado 28
Figura 6. Clave de 128 bits 28
Figura 7. Subclaves a calcular 28
Figura 8. Operación Rotword 28
Figura 9. Operación Subway 28
Figura 10. Tabla RCON 28
Figura 11. Segunda subclave 28
Figura 12. XOR aplicada a la columna final y cuarta anterior 28
Figura 13. Nueva subclave 28
Figura 14. Aplicación de operaciones y claves 28
Figura 15. Operación AddRoundKey 28
Figura 16. Operación ShiftRows 28
Figura 17. Operación Mixcolums 28
Figura 18. Cifrado AES 28
Figura 19. Desciifrado AES. 28
Figura 20. Funcionamiento de algoritmo de clave privada 28
Figura 21. Estructura del proceso de cifrado IDEA 28
Figura 22. Funcionamiento del PRGA de RC4 28
Figura 23. Gráfica tiempo de encriptación/desencriptación RSA 46
Figura 24. Evolución del tiempo de cifrado AES 47
Figura 25. Tiempo encriptación / desencriptación RSA 48
Figura 26. Tiempo encriptación/desencriptación IDEA 50
Figura 27. Evolución tiempo de cifrado y descifrado RC4 51
Figura 28. Rendimiento cifrado algoritmos 53
Figura 29. Rendimiento descifrado de algoritmos 53
Figura 30. Diagrama de bloques para AES 128 bits 59

LISTA DE ANEXOS

Pág.

Anexo A FORMATO RAE 75

INTRODUCCIÓN

Con la evolución de las TIC y el uso de la Internet, la seguridad de la información se ve afectada por la cantidad de amenazas y vulnerabilidades que se identifican en un sistema, y se basan en técnicas desarrolladas en su mayoría por criminales informáticos. Para ellos, uno de los blancos principales es la información, y por ello, las organizaciones deben pensar en mecanismos de protección que asegure su información, así como su funcionamiento y sostenibilidad. Dicho lo anterior, esta monografía que lleva por título "ESTUDIO DE EFICIENCIA Y EFICACIA DE LOS ALGORITMOS CRIPTOGRÁFICOS RSA, AES, IDEA, RC4 EN LA SEGURIDAD INFORMÁTICA" analiza los algoritmos criptográficos RSA, AES, IDEA y RC4, resaltando características de ellos, su eficiencia y beneficios frente a las amenazas informáticas representativas, con el fin de determinar cuáles proporcionan mayor seguridad a la hora de proteger la información.

Para llevar a cabo el objetivo general, se divide el documento en tres capítulos:

En los capítulos denominados “Criptografía y Seguridad Informática”, “Descripción de los algoritmos de cifrado” y “Características de los algoritmos RSA, AES, IDEA y RC4” se busca desarrollar el primer objetivo de este documento, donde se resaltan características generales y específicas de los algoritmos criptográficos RSA, AES, IDEA y RC4.

El segundo objetivo de esta monografía se desarrolla en el capítulo llamado “Eficiencia de los algoritmos RSA, AES, IDEA y RC4”, donde se identifican cuáles de ellos cumplen con un óptimo uso de recursos y tiempo.

El tercer objetivo de esta monografía se desarrolla en los capítulos: “Análisis de algoritmos criptográficos frente a amenazas informáticas”, “Seguridad de los algoritmos criptográficos” y “Ataques a los algoritmos criptográficos”, donde se identifican de los algoritmos RSA, AES, IDEA y RC4, cuáles presentan mayores beneficios frente a las amenazas informáticas.

Cabe resaltar que esta es una investigación de tipo documental, puesto que se realiza con apoyo de fuentes documentales y de investigación bibliográfica basada en la consulta de libros, artículos, revistas; y en la cual, se considera como enfoque los algoritmos criptográficos RSA, AES, IDEA y RC4.

Finalmente, puede decirse que esta investigación se limita al estudio y análisis de características generales y específicas, optimo uso de recursos, tiempo, y beneficios frente a algunas amenazas informáticas, de los algoritmos RSA, AES, IDEA y RC4, y tiempo de desarrollo es 1 año.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN

En la actualidad, la información se ve afectada por la aparición y evolución de diferentes amenazas informáticas que pueden vulnerar los datos e información (alterarlos, modificarlos, borrarlos, enviarlos a un tercero, etc), tal es el caso de malwares, virus informáticos, entre otros, y junto a ello, los mecanismos y técnicas desarrolladas por terceros malintencionados que buscan atentar contra la confidencialidad, integridad y autenticidad en sistemas de cifrado, como ejemplo, el criptoanálisis, ataques de fuerza bruta, etc. Frente a esto, las organizaciones tienen a su disposición la implementación de diferentes métodos que permiten afrontar dichas vulnerabilidades e intrusiones consideradas como peligrosas o devastadoras, métodos que consisten en el uso, creación e implementación de algoritmos criptográficos con objeto de garantizar la seguridad de la información, protegerla y así evitar que terceros malintencionados la puedan manipular.

1.2. FORMULACIÓN

¿Cuál de los algoritmos criptográficos es el más eficaz y presenta mejores beneficios frente a las amenazas informáticas en los sistemas de información?

1.3. OBJETIVOS

1.3.1. Objetivo general.

Realizar un estudio de los algoritmos criptográficos RSA, AES, IDEA y RC4 para determinar la eficacia y mejores beneficios frente a las amenazas informáticas en los sistemas de información.

1.3.2. Objetivos específicos.

- Analizar las características de la criptografía y los algoritmos criptográficos RSA, AES, IDEA y RC4.
- Comparar la eficiencia de uso de recursos y tiempo de ejecución de los algoritmos RSA, AES, IDEA y RC4.

- Compilar los ataques más representativos a la seguridad informática según los algoritmos RSA, AES, IDEA y RC4.

1.4. JUSTIFICACIÓN

Lo que se pretende en el proyecto es conocer que tan confiables y efectivos son los algoritmos criptográficos RSA, AES, IDEA y RC4, partiendo de sus características generales y específicas, y determinar cuáles son más seguros en la protección de la información. Con ello, se busca aportar a aquellos interesados en implementar un sistema criptográfico, y ayudarlos a elegir el método o algoritmo adecuado que le brinde mayor confianza y seguridad para proteger la información.

El asegurar que la información sea integra y confidencial es un tema que preocupa a toda organización que maneja grandes cantidades de ella, ya sea, que este almacenada en bases de datos o albergadas en los diferentes equipos, y sobre todo cuando dicha información se transfiere por medios inseguros (como Internet o medios extraíbles). Por ello, es necesario para las organizaciones cifrar la información, buscando que no sea manipulada, transferida o eliminada por terceros.

Ahora, considerando el hecho que las amenazas informáticas se presentan constantemente y los atacantes trabajan día a día para obtener información relevante de usuarios víctimas, lo que se pretende en esta monografía es llevar a cabo un estudio de los algoritmos criptográficos RSA, AES, IDEA y RC4, para dar a conocer a los interesados características generales de estos y otros aspectos de importancia, como el óptimo uso de recursos, tiempos de ejecución y beneficios frente a las amenazas informáticas, con el fin de asegurar la información.

1.5. DELIMITACIÓN

Por tratarse de una revisión bibliográfica, el desarrollo de este trabajo es netamente teórico y tiene en cuenta el estudio y análisis de los cuatro algoritmos criptográficos RSA, AES, IDEA y RC4. Cabe resaltar que la evaluación o puesta en marcha de los algoritmos no hace parte de este trabajo.

2. MARCO DE REFERENCIA

2.1. ANTECEDENTES

Relacionado a esta monografía se encuentra.

CABRERA, Claudio evalúa los algoritmos DES, Rijndel y RC4 a partir de pruebas que relacionan tamaño de archivos a cifrar, longitud de clave y tiempos de cifrado y descifrado. Su investigación conduce a elegir a Rijndel como el algoritmo que menos tarda en cifrar y descifrar archivos[1].

CAPUÑAY, Denys et al. Realiza un análisis comparativo de los algoritmos criptográficos DES, AES Y 3DES para redes privadas virtuales, a partir de una metodología experimental, analizando de cada algoritmo tiempos, tamaños de paquetes, grados de encapsulación, etc. Su investigación llevó a elegir AES, siendo el mejor en tiempo de envío de cifrado y descifrado[2].

CHALA, Y profundiza en el cifrado de la información, con el fin de dar a conocer a las empresas los beneficios que puede ofrecerles. De igual manera, muestra algunas herramientas de implementación para dicha labor[3].

DE LA FUENTE, Elma hace un estudio de algoritmos y protocolos de seguridad en smarphones con Android, con el fin de determinar el algoritmo o algoritmos que ofrecen mejor seguridad en conexiones de internet, mayor protección en aplicaciones móviles o almacenamiento interno[4].

GALVEZ, Heber realiza una investigación comparando el tiempo de transmisión de video, aplicando algoritmos criptográficos a través de protocolos UDP o TCP. El fin

[1] CABRERA, C. ALGORITMOS DE ENCRIPTACIÓN, DESENCRIPTACIÓN - EVALUACIÓN Y VERIFICACIÓN. Universidad Técnica del Norte. {en línea}. {Consultado 20 septiembre de 2019}. Disponible en: https://docplayer.es/7972090-Algoritmos-de-encriptacion-desencriptacion-evaluacion-y-verificacion.html

[2] CAPUÑAY, Denys; GUERRERO, Ana & VILLEGAS, Juan. (2016). Análisis Comparativo de Algoritmos Criptográficos. Revista Internacional de TECNOLOGÍA DIGITAL Y ECONOMÍA. {en línea}. {Consultado 4 octubre de 2019}. Disponible en: http://revistas.uss.edu.pe/index.php/ING/article/view/440

[3] CHALA, Y. (2019). Trabajo de postgrado (Importancia de la aplicación del mecanismo de cifrado de Información en las empresas para la prevención de riesgos Como ataques, plagio y pérdida de la confidencialidad). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado marzo 14 de 2020}. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/30745/1/yfchala..pdf

[4] DE LA FUENTE, Elma. (2015). Tesis de pregrado (Estudio de la eficiencia de protocolos y algoritmos de Seguridad en Android). Universidad Carlos III de Madrid Escuela Politécnica Superior. {en línea}. {Consultado marzo 13 de 2019}. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/25278/PFC_Elma_Fuente_Barrios.pdf

es determinar cuál es el impacto generado al usar dichos algoritmos, partiendo de un servidor de vídeo, una entidad y el descifrado del vídeo.

MEDINA, Yuri & MIRANDA, Haider comparan los algoritmos DES, AES y 3DES a partir de 12 factores, entre las que se encuentran el tamaño de clave, cifrado, resistencia a criptoanálisis, entre otros. Su trabajo reconoce a AES como el algoritmo que ofrece las mejores características[5].

MONTAÑO, Juan desarrolla un análisis de los algoritmos criptográficos RSA y Shor, donde compara la eficiencia por medio de los métodos de factorización utilizados y teniendo en cuenta variables como los tiempos de ejecución de estos algoritmos.[6]

PRIYADARSHINI, Patil Hace una comparativa de los algoritmos DES, 3DES, AES, RSA y Blowfish, basado en fortalezas, debilidades, costos, rendimiento y tiempos de ejecución, para determinar los rendimientos de manera general[7].

SERRATO, Hernán hace una comparación de los tres métodos criptográficos DES, AES y RSA a partir de los procesos de cifrado, descifrado y rendimiento a partir de estos últimos procesos[8].

SOBREVILLA, Pedro hace un estudio del cifrado PES e IDEA, y analiza su seguridad contra ataques de criptoanálisis diferencial y lineal. Su objetivo es modificar el sistema IDEA y observar la seguridad de los ataques con dicha modificación del sistema[9].

---

[5] MEDINA, Yuri & MIRANDA, Haider. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. Revista MundoFesc,. {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55

[6] MONTAÑO, Juan. (2015). Tesis de postgrado (Algoritmos de encriptación: análisis del problema de la factorización prima en el método RSA de clave pública, algoritmo de shor). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 13 abril de 2020}. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3609/1/73192426.pdf

[7] PRIYADARSHINI, Patil; PARSHANT, Narayankar; NARAYAN, D.K.; MEENA, S. (2016). Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish. {en línea}. {Consultado 14 abril de 2019}. Disponible en http://www.sciencedirect.com/science/article/pii/S1877050916001101

[8] SERRATO, H. (2019). Trabajo de postgrado (Comparación de Métodos Criptográficos para la Seguridad Informática). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 12 abril de 2020}. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

[9] SOBREVILLA, Pedro. (2016). SEGURIDAD Y EFICIENCIA DE ALGUNAS VARIANTES DEL CRIPTOSISTEMA IDEA. (tesis de postgrado). Universidad Autónoma Metropolitana Iztapalapa. {en línea}. {Consultado 1 noviembre de 2019}. Disponible en: http://mat.izt.uam.mx/mcmai/documentos/tesis/Gen.12-O/Pedro_Sobrevilla.pdf

2.2. MARCO TEORICO

Teniendo en cuenta la necesidad de guardar en secreto la información y ser compartida sólo para personas en particular, se hizo necesario pensar en métodos para ocultar y acceder a dicha información bajo determinadas condiciones. Uno de ellos consiste simplemente en ocultarla, y otro, en modificarla o transformarla, de tal manera que, si un cae en manos no deseadas, esta no pueda conocerse, pero que pueda recuperarse cuando sea necesario.

A lo largo de la historia, se han conocido diferentes métodos para ocultar la información, asociados al primer método, y vale la pena tener en cuenta[10]:

- Escritura sobre tablilla y sobrepuesta con cera. Este hecho parece que la tablilla no estuviera escrita, y sólo podía verlo el remitente al quitar la cera.
- Escritura sobre la cabeza sin pelo. Al crecer el pelo se enviaba al destino, afeitaban su cabeza y podían ver el mensaje.
- Escritura con tinta invisible que podía verse al calentarse.
- Los acrósticos de la Celestina. Versos que llevaban el mensaje en las letras iniciales de cada línea.
- Entre otros.

De igual manera, se menciona otros métodos asociados al segundo método (los criptográficos):

- Método de transposición: consiste en barajar o colocar en distinta posición las letras del mensaje a ocultar.
- Método de sustitución: consiste en cambiar las letras del mensaje por letras o símbolos distintos.
- Método del cifrado: consiste en la codificación de las letras del mensaje, transformarlas en números y realizar operaciones matemáticas.

Ahora bien, en la actualidad las organizaciones albergan grandes cantidades de información en bases datos y archivos, siendo quizás esta el activo más importante para ella (sin dejar de lado el recurso humano), y el objetivo para ellas es protegerla. El desarrollo de la internet, medios de comunicación, dispositivos informáticos, software, entre otros, hace para los cibercriminales[11] que la información sea un objetivo a obtener, usando tantos mecanismos y técnicas como sean necesarias, como, por ejemplo, los relacionados con los ataques informáticos. Es por ello, que

[10] HERNANDEZ, E. L. (2016). La criptografía. {en línea} {Consultado 3 marzo de 2020}. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co

[11] Persona que practica el cibercrimen (creando software malicioso, virus informáticos, entre otros, orientados al robo de información, chantajes, promoción de productos, etc.). Fuente: https://www.kaspersky.es/resource-center/threats/cybercrime

el interés de dichas organizaciones es asegurar que la información no sea trasmitida, enviada, recibida o modificada por terceros no deseados, además de mantener su propiedad de autenticidad, integridad y confidencialidad. Eso lo permiten los sistemas criptográficos[12], que actualmente, pueden clasificarse en dos:

- Los de criptografía simétrica, que se basa en el uso de una clave para cifrar y descifrar la información.
- Los de criptografía asimétrica, que se basa en el uso de dos claves: una pública (conocida por cualquiera y sirve para cifrar) y una privada (que no se revela y sirve para descifrar la información).

2.3. MARCO CONCEPTUAL

En este apartado se tuvo en cuenta conceptos relacionados con la criptografía, seguridad informática e información, buscando características y aspectos relevantes necesarios para el desarrollo de esta monografía.

2.3.1. Criptografía.

La palabra criptografía proviene del griego "Kryptos", escondido, y "Graphos", escritura[13]. Es decir, se podría traducir como "Escritura escondida". El objetivo de la criptografía no es tanto ocultar la existencia del mensaje, sino ocultar el significado del mensaje, lo que se realiza mediante el cifrado o codificación del mensaje[14].

2.3.2. Pilares de la Seguridad Informática.

Los pilares de la seguridad de la información son tres[15]:

---

[12] En esta monografía se tratan los sistemas RSA, AES, IDEA y RC4.

[13] GARCIA, Roberto. (2009). Criptografía clásica y moderna. España: Septem Ediciones. {en línea}. {Consultado 18 de febrero de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10317082&tm=1465508388792

[14] DÍAZ, Gabriel, MUR, Francisco, & SANCRISTÓBAL, Elio. (2004). Seguridad en las comunicaciones y en la información. España UNED - Universidad Nacional de Educación a Distancia. {en línea}. {Consultado 15 febrero de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10560101&tm=1465508562939

[15] ÁLVAREZ, Gonzalo & PÉREZ, Pedro. (2004). Seguridad informática para empresas y particulares. España: McGraw-Hill España. {en línea}. {Consultado 20 febrero de 2019} Disponible en:

- Confidencialidad: Garantiza la lectura de recursos, datos y objetos sólo a legítimos destinatarios.
- Integridad: Garantiza que los recursos, datos y objetos mantengan propiedades fiabilidad, no alteración y estén completos.
- Disponibilidad: Garantiza que los datos permanecen accesibles, sin interrupciones cuando y donde se los necesita.

2.3.3. Seguridad Informática.

Este término hace referencia a proteger la infraestructura computacional o medios informáticos[16], y a esto se agrega que la protección debe realizarse a la información de un equipo a través de las redes[17].

2.3.4. Seguridad de la información.

La seguridad de la información se define como el conjunto de medidas de prevención de sistemas tecnológicos enfocados al resguardo y protección la información[18], lo que busca es mantener que los datos e información goce de propiedades de confidencialidad, disponibilidad e integridad junto a medidas preventivas y reactivas que las organizaciones deben generar y aplicar: políticas, normas, procedimientos, evaluar el riesgo, planes de contingencia, entre otras medidas, con el objetivo de mantener y asegurar las propiedades ya dichas.

2.3.5. Aritmética modular.

Para tres números naturales a, b y c se dice que a es congruente con b módulo n, si cumple:

---

http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10498593&tm=1466006497840

[16] SAMPEDRO, Carlos; MACHUCA, Silvio; PALMA, Diego & CARRERA, Frankz. (2019). Percepción De Seguridad De La Información en Las pequeñas y medianas empresas en santo domingo. Investigación Operacional, {en línea}. {Consultado 25 febrero de 2019}. Retrieved from http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=zbh&AN=136929577&lang=es&site=eds-live&scope=site

[17] ARROYO, Cilene. (2019). Implantación de un esquema de seguridad informática. {en línea}. {Consultado 28 febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BBED0E78&lang=es&site=eds-live&scope=site

[18] GOMEZ, Álvaro. (2014). Seguridad en equipos informáticos. España: RA-MA Editorial. {en línea}. {Consultado 29 de marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=13&docID=11046412&tm=1466006343174

$$a = b + kn \quad \text{para un entero k}$$

Y se expresa,

$$a \equiv b(mod\ n)$$

2.3.6. Algoritmo criptográfico.

Un algoritmo criptográfico puede definirse como un algoritmo que garantiza ciertas características de seguridad al modificar los datos, particularmente la confidencialidad, disponibilidad e integridad de los mismos. Para el desarrollo de este trabajo se estudian los siguientes algoritmos:

- Algoritmo RC4: es un esquema de cifrado de flujo simétrico extremadamente simple desarrollado por Ron Rivest en el año 1987, y predecesor del algoritmo WEP. Es muy utilizado mundialmente[19].

- Algoritmo RSA: El algoritmo RSA (Rivest, Shamir y Adleman) es de cifrado asimétrico desarrollado en el año 1977, y se basa en mantener en secreto dos números primos aleatorios de gran extensión, que son base del cifrado. La principal ventaja relacionada al tema de seguridad radica en la dificultad de factorizar números compuestos grandes[20].

- Algoritmo IDEA: este es uno de los algoritmos de cifrado que se utiliza ampliamente con fines de seguridad. El cifrado de bloque IDEA opera con un bloque de texto simple de 64 bits y un bloque de texto de cifrado de 64 bits, y una clave de 128 bits lo controla. El diseño fundamental del algoritmo utiliza tres operaciones algebraicas diferentes: OR exclusivo a nivel de bits, módulo de multiplicación y módulo de adición[21].

- Algoritmo AES: El estándar de cifrado AES (Advanced Encryption Standard) Se basa en operaciones a nivel de byte, cifra por bloques de 128 bits y trabaja con longitudes de clave de 128, 192 y 256 bits. Fue desarrollado en 1988 por Joan Daemen e incent Rijmen[22].

---

[19] GARCIA, Roberto. (2009). Op. cit

[20] SANCHEZ, Héctor; RODRIGUEZ, Carlos & NOTARIO, Alejandro. Critografía y métodos de cifrado. {en línea}. {Consultado 25 de abril de 2019}. Disponible en: http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

[21] ALMASRI, Osama & MAT, Hajar. (2013). Introducing an Encryption Algorithm based on IDEA. Universiti Tenaga Nasional. {en línea}. {16 de abril de 2019}. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.679.7495&rep=rep1&type=pdf

[22] MARTÍNEZ, Francisco. (2016). Criptosistemas de cifrado en flujo basados en matrices triangulares con múltiples bloques. {en línea}. {Consultado 20 de abril de 2019}. Disponible en:

2.3.7. Inverso multiplicativo modular.

Dado un número entero n módulo p, su inverso multiplicativo es otro entero m módulo p, de manera que $m \times n$ es congruente con 1 módulo p.

2.3.8. Números primos.

Un número es primo si es mayor a uno, y si admite sólo dos divisores: la unidad y el mismo número.

2.3.9. Operadores Bits a Bits.

- NOT: Es una operación unitaria que básicamente niega lógicamente cada bit, esto es 1 negado es 0, y viceversa.

  Tabla 1. Operador NOT

$\boldsymbol{a}$	$\neg \boldsymbol{a}$
1	0
0	1

  Fuente: Elaboración propia

- AND: Este operador toma dos enteros, si estos dos son 1, el operador AND lógico devuelve 1 como resultado, en otros casos será cero.

  Tabla 2. Operador AND

$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{a}$ & $\boldsymbol{b}$
1	1	1
1	0	1
0	1	1
0	0	0

  Fuente: Elaboración propia

- OR (|): Este operador toma dos enteros, si estos dos son 0, el operador OR lógico devuelve 0 como resultado, en otros casos será 1.

---

http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.58178TES&lang=es&site=eds-live&scope=site

Tabla 3. Operador OR

a	b	$a \mid b$
1	1	1
1	0	1
0	1	1
0	0	0

Fuente: Elaboración propia

- XOR ($\oplus$): Este operador toma dos enteros y realiza la operación OR Exclusivo. Esto es, devuelve 1 si ambos enteros son distintos, en otros casos devuelve. Es decir,
  Tabla 4. Operador XOR

a	b	$a \oplus b$
1	1	0
1	0	1
0	1	1
0	0	0

Fuente: Elaboración propia

2.3.10. Amenaza a la información.

Básicamente una amenaza es cualquier situación o evento que afecta a las organizaciones o usuarios en el desarrollo de sus actividades. De esta manera, las amenazas a la información afectan la información, y entre las causas más comunes están: los desastres naturales, fallas en sistemas de procesamiento de información o actos de terceros malintencionados[23].

2.3.11. Algoritmo de Fermat.

Este algoritmo tiene como fin representar un número impar n como producto de una suma por una diferencia, es eficiente para casos donde los factores son cercanos. El procedimiento es el siguiente:[24]

[23] TARAZONA, Cesar. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas, {en línea}. {Consultado 6 mayo de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3311853ART&lang=es&site=eds-live&scope=site

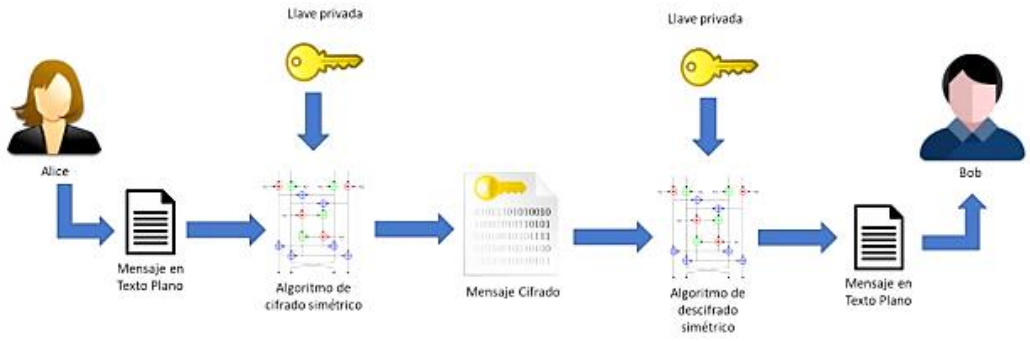
[24] MARÍ, Noelia. (2018). Una propuesta híbrida para el criptoanálisis RSA. {en línea}. {Consultado 6 mayo de 2019}. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.C6EE8D1&lang=es&site=eds-live&scope=site

Entrada:	n impar	
Se calcula	$a = \sqrt{n}$	
Se analiza	si $a^2 - n$	en caso negativo, se hace $a = a + 1$ y se repite análisis.
		en caso positivo, se calcula $b = \sqrt{a^2 - \boldsymbol{n}}$
Salida:	$(a + b)(a - b)$	

2.3.12. Criptografía simétrica.

Este tipo de cifrado pasa un texto plano a uno cifrado teniendo en cuenta una llave secreta y un algoritmo de cifrado. Para el descifrado del texto se usa la misma clave y un algoritmo de descifrado. Cabe resaltar que ambos algoritmos son públicos y el mensaje cifrado depende de la llave secreta. La siguiente figura muestra visualmente el proceso de este proceso[25].

Figura 1. Cifrado simétrico



Fuente: VARGAS, Juan

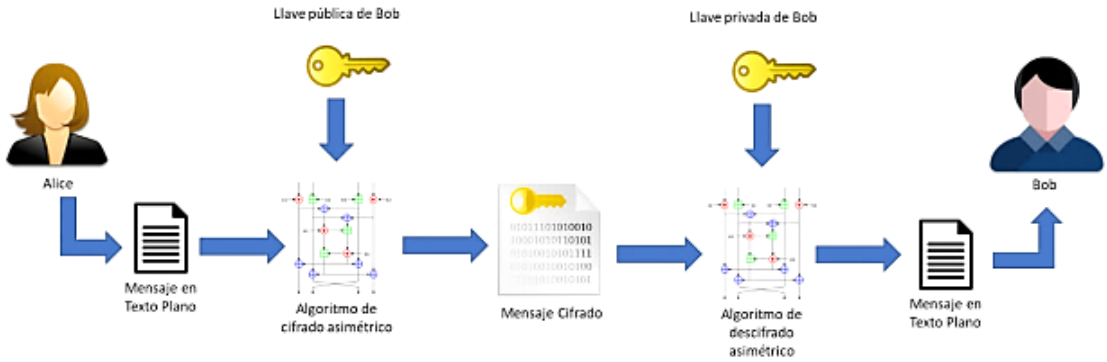
2.3.13. Cifrado asimetrico.

Este tipo de cifrado involucra dos llaves: una publica para cifrar el mensaje que puede ser revelada, y otra privada que descifra el mensaje y no puede ser revelada. A diferencia del cifrado simétrico que utiliza sustituciones y permutaciones, el cifrado

[25] VARGAS, Julio. (2019). OVI Unidad 2 - Criptografía. Bogotá, Colombia UNAD - Universidad Nacional Abierta y a Distancia. {en línea}. {6 mayo de 2019}. Disponible en: http://hdl.handle.net/10596/23682

asimétrico se basa en funciones matemáticas[26]. La siguiente imagen muestra visualmente el proceso de este.

Figura 2. Cifrado asimétrico



Fuente: VARGAS, Juan

2.3.14. Eficiencia de un algoritmo criptográfico.

La eficiencia de un algoritmo criptográfico se relaciona con la cantidad de recursos computacionales utilizados por este, la máxima eficiencia se logra minimizando uso de recursos. Para esto, es necesario analizar dos variables principales del algoritmo[27]:

- Espacio en disco: Cuidando que no sea limitante y se cuente con este.
- Tiempo de ejecución: buscando rapidez, sobre todo cuando los datos de entrada son más grandes.

2.3.15. Eficacia de un algoritmo criptográfico.

Un algoritmo criptográfico es eficaz si cuenta con dos características principales[28]:

- Posibilidad de proteger datos de ataques informático
- Rendimiento en el cifrado y descifrado

[26] VARGAS, Juan. (2019). ANÁLISIS DE EFICACIA Y EFICIENCIA PARA UN MÉTODO DE CIBERSEGURIDAD PARA EL PROTOCOLO DE COMUNICACIÓN ACARS EN AERONAVES COMERCIALES LEGADO. (Tesis de postgrado). Querétaro. (Tesis de postgrado). {en línea}. {Consultado 7 mayo de 2019}. Disponible en: https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/346/1/VargasSalvadorJuanP%20MSIM%202019.pdf

[27] VARGAS, Juan. Op. cit

[28] Ibid.

2.3.16. Promedio.

Para calcular el promedio $\bar{x}$ de un conjunto de datos $x_1, x_2, \dots, x_n$ se suman todos ellos y se divide entre la cantidad de ellos n.[29]

$$\bar{x} = \frac{x_1 + x_2 + \cdots + x_n}{n}$$

2.3.17. Rendimiento de un algoritmo.

El rendimiento de un algoritmo (R) se relaciona con la velocidad que realiza una tarea. Para calcularlo es necesario conocer el tiempo promedio que demora en cifrar (T_c) o descifrar (T_d) el algoritmo, junto al promedio de los tamaños paquetes (m).[30]

$R = \frac{m}{T_c}$ Rendimiento de cifrado

$R = \frac{m}{T_d}$ Rendimiento de descifrado

2.4. MARCO LEGAL

2.4.1. Ley 1273 de 2009.

Esta ley trata acerca de la protección de la información y de los datos, está dividida en dos capítulos trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; así como, de los atentados informáticos y otras infracciones[31].

El primer capítulo trata principalmente los siguientes atentados:

- Artículo 269A: Acceso abusivo a un sistema informático
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático

[29] MORALES, Aaron. (2012). Estadística y probabilidades. Chile. {en línea}. {Consultado 10 mayo de 2019}. Disponible en: http://www.x.edu.uy/inet/EstadisticayProbabilidad.pdf
[30] SAMANIEGO, Ana. Op. cit.
[31] MINTIC. (2017). Mintic. Decreto 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. {en línea}. {Consultado 30 abril de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-3705.html

- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.

El segundo capítulo trata de los siguientes atentados

- Artículo 269I: Hurto por medios informáticos y semejantes
- Artículo 269J: Transferencia no consentida de activos.
- Artículo 58. Circunstancias de mayor punibilidad

2.4.2. Ley 1581 de 2012.

Constituye el marco general de la protección de los datos personales en Colombia, se divide en 6 capítulos: disposiciones generales, autorización, políticas de tratamiento de la información, ejercicio de los derechos de los titulares, transferencias y transmisiones internacionales de datos personales, y la responsabilidad demostrada frente al tratamiento de datos personales[32].

Básicamente, es una ley complementaria a la regulación actual para proteger el derecho que toda persona natural tiene a la actualización, rectificación o autorización de su información personal almacenada ya sea en bases de datos o archivos.

2.4.3. Ley 1928 de 2018.

Ley que trata de la aprobación del convenio de ciberdelincuencia, se divide en cuatro capítulos: terminologías sobre sistemas informáticos, medidas que se deben tomar de delitos contra la confidencialidad, integridad y disponibilidad de la información, cooperación internacional, y disposiciones finales[33].

Particularmente, el segundo capítulo lo compone los ítems:

- Acceso ilícito a la información
- Interceptaciones ilícitas
- Interferencia en los datos

[32] MINTIC. (2001). Mintic. Decreto 1377 de 2001: Por medio de la cual se reglamenta parcialmente la ley 1581 de 2012 Ley de Protección de datos. {en línea}. {Consultado 30 abril de 2019}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-4274.html

[33] PRESIDENCIA DE LA REPÚBLICA. LEY 1928 DE 24 DE JULIO DE 2018: por la cual se aprueba el convenio de la ciberdelincuencia, adoptado del 23 de noviembre de 2001, en Budapest. Convenio de la ciberseguridad. {en línea}. {5 febrero de 2019}. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

- Interferencia en el sistema
- Abuso de los dispositivos
- Falsificación informática
- Delitos relacionados con pornografía infantil
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
- Entre otros

2.4.4. Ley 527 de 1999.

Busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

En esta ley " se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones[34]". Básicamente, da autorización del uso de mensajes de datos en sectores públicos y privados.

3. RESULTADOS

3.1. CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

La comunicación ha venido manejando diferentes sistemas de cifrado dependiendo de su contexto, donde la escritura cumple un papel fundamental en la evolución de este sistema. Para ello, es fundamental conocer la evolución de los mensajes a transmitir desde la antigüedad hasta nuestros tiempos, y el cifrado se involucra en esta evolución haciendo necesario proteger dicha información.

La criptografía como un sistema de protección de la información consiste en cifrar un mensaje de tal forma que un tercero no pueda entenderlo, y a través de los tiempos diferentes culturas (egipcia, árabe, griega, entre otras) han adoptado distintos mecanismos de cifrado que garantizan el secreto en la comunicación, por ello, puede recalcarse el papel de la criptografía[60]:

[34] LEY 527 de 1999. {en línea}. {Consultado 1 mayo de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf
[60] GARCIA, Roberto. Op. cit

“la criptografía deja de ser considerada un arte y pasa a considerarse una ciencia, dadas sus complejas relaciones con otras ciencias como la estadística, la teoría de los números y la teoría de la información, entre otras.”

Hoy en día, vista como un mecanismo, la criptografía puede relacionarse con las medidas de seguridad informática y puede aplicarse en toda empresa que maneje gran cantidad de la misma. Como lo dice Escrivá et al: “Cuando se habla de medidas de seguridad informática, lo primero que nos viene a cabeza son las medidas destinadas a impedir infecciones o accesos no autorizados en los equipos informáticos”[61]. Junto a esto, se encuentra la seguridad de la información, y son medidas que controlan, mitigan o previenen distintos problemas de seguridad a los que un sistema puede enfrentarse, como pueden ser el acceso a datos no autorizados o la recepción de datos maliciosamente modificados[62].

Ahora, la relación de estos dos se encamina al estudio de este trabajo, y partiendo de los accesos no autorizados o la modificación de la información, se hace necesario hablar de los diferentes sistemas de cifrado que permitirá asegurar aspectos básicos de la seguridad informática: confidencialidad, integridad y disponibilidad.[63]

Esto, se relaciona con la criptografía y el criptoanálisis, y este último “se enfoca al estudio de las debilidades en los diversos sistemas criptográficos sin conocer parte de la información que en este caso serían las llaves privadas”[64], en otras palabras, es el estudio de mecanismos para descifrar mensajes sin conocer las claves de cifrado.

El concepto de criptoanálisis dentro de una empresa garantiza la protección de la información y puede aplicarse en: la autenticación (asegurar que un mensaje no haya sido manipulado), la firma digital (creada a partir de por una clave privada), la certificación de firmas digitales y las funciones hash (que resume un texto largo o amplia un texto corto)[65].

---

[61] ESCRIVÁ, Gema, ROMERO, Rosa & RAMADA, David. Op. cit

[62] GONZALEZ, Lorena, & FUENTES, José. (2014). Sistemas seguros de acceso y transmisión de datos (MF0489_3). Madrid, ESPAÑA IC Editorial. {en línea}. {Consultado 3 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=11126449&tm=1465508507275

[63] DÍAZ, Gabriel, MUR, Francisco, & SANCRISTÓBAL, Elio. Op. cit

[64] QUINTERO, Juan. (2016). OVI Unidad 1 - Criptografía. Bogotá, Colombia UNAD - Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 4 junio de marzo de 2019}. Disponible en: http://stadium.unad.edu.co/ovas/10596_10131/index.html

[65] MOLINA, José. (2000). Seguridad de la información. Criptología. Argentina El Cid Editor. {en línea}. {Consultado 4 junio de 2019}. Disponible en:

Dentro de una empresa para proteger la información se habla de los dos tipos de cifrado: simétricos y asimétricos. Otros aspectos a tener en cuenta respecto a la seguridad informática, y que están relacionados con la criptografía son[66]:

- Reducir, gestionar y detectar problemas y amenazas de seguridad.
- Eficiente uso de recursos, aplicaciones y el sistema.
- Reducir pérdidas y adecuada reacción en la recuperación del sistema en incidentes de seguridad.
- Cumplir con normatividades y políticas de seguridad de la empresa.

Y junto a esto, con el surgimiento de redes de comunicación como la internet, el acceso a la información es tema central para los atacantes informáticos y las amenazas sobre los sistemas informáticos es más común. Entre algunos de ellos, se mencionan los siguientes[67].

- Intercambios de códigos de virus
- Suplantación de identidades
- Robo y destrucción de la información
- Entre otros

Frente a estos, se toman dos tipos de medida: Seguridad física (aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial) y seguridad lógica (aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo).[68]

Por lo dicho, la criptografía relacionada a la seguridad informática es la medida indicada para proteger la información de una empresa, y además, como herramienta es idónea para soportar un sistema de comercio seguro y confiable[69].

---

http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=12&docID=10018530&tm=1465508601401

[66] GOMEZ, Álvaro. (2007). Enciclopedia de la Seguridad Informática. Bogotá, Colombia: Alfaomega. {en línea}. {Consultado 4 junio 2019}. Disponible en: https://books.google.com.pe/books/about/Enciclopedia_de_la_seguridad_inform%C3%A1tic.html?id=MQ_kOgAACAAJ&redir_esc=y

[67] MARRERO, Yran. (2003). La Criptografía como elemento de la seguridad informática. {en línea}. {Consultado 17 junio de 2019}. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

[68] LOVOS, Francisco. Seguridad física y lógica en los centros de cómputo. {en línea}. {Consultado 17 junio de 2019}. Disponible en: https://webcache.googleusercontent.com/search?q=cache:ogqe1OyomHEJ:https://lovosfrancisco.jimdo.com/app/download/9167889769/SEGURIDAD%2BFISICA%2BY%2BLOGICA.pdf%3Ft%3D1504554721+&cd=17&hl=es-419&ct=clnk&gl=co

[69] ALZATE, Alonso & DUQUE, Néstor. Criptografía una excelente alternativa de seguridad. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://bdigital.unal.edu.co/58103/1/criptografia.pdf

Junto a lo dicho, se deben considerar también:

- Plan de continuidad: el permitir la recuperación continua de datos
- Accesibilidad de la información: la criptología no tiene que impedir el normal funcionamiento de la empresa.

Consideraciones que junto a lo ya mencionado la criptología se hace necesaria para otorgar a las empresas privacidad, confidencialidad y seguridad[70].

A continuación, describen algunos algoritmos que relacionan el trabajo de la criptografía.

3.2. DESCRIPCIÓN DE LOS ALGORITMOS DE CIFRADO

3.2.1. RSA (Rivest, Shamir, Adleman).

Es un algoritmo de clave pública que apareció en 1978 cuando la criptografía tenía diferentes áreas de aplicación, y además para este tipo de algoritmos de necesita una definición inicial de su perfil, se crean dos claves que están relacionadas pero que a su vez son diferentes; una clave, la privada, se mantiene secreta, sólo conocida por el usuario a quien le es asignada, mientras que la segunda clave, la pública, puede ser conocida por todos, está a disposición ya sea a través de correo o en directorios o en servidores de claves accesibles, cualquier persona puede verlas". Por su parte, el algoritmo RSA consiste de tres pasos, el primero, es la generación de la clave, usada para la encriptación y desencriptación del mensaje, el segundo, la encriptación, conversión del texto plano a texto cifrado, el tercero, el descifrado, la conversión del texto cifrado al texto plano[71].

RSA usa la exponenciación modular, denotada por la siguiente ecuación, dónde Z: resultado de operar la exponenciación modular, x: es la base de la operación, y: es el exponente, m: es el módulo de la operación.

$$Z = x^y mod\ m$$

Para generar las claves de RSA, el administrador debe encontrar dos números primos p y q con una longitud de bits grande (para desalentar ataques al sistema), de tal manera que se obtiene el producto:

$$m = p \cdot q$$

Y la función de Euler:

[70] SANCHEZ, Héctor; RODRIGUEZ, Carlos & NOTARIO, Alejandro. Criptografía y métodos de cifrado. Op. cit.
[71] ALZATE, Alonso & DUQUE, Néstor. Op. cit.

$$\sigma(n) = (p-1)(p-1))$$

Adicional a esto, se define la función $\emptyset(m)$ correspondiente al conjunto de números que tienen inverso multiplicativo, definidos en $m.$ Posterior a esto, se elige un número e, de tal manera que tenga un inverso multiplicativo en m. Este será la clave publica del usuario. La clave privada $d,$ será calculada por la siguiente expresión.

$$d = e^{-1}\ mod\ \emptyset(m)$$

El mensaje será desencriptado con esta última.

3.2.1.1. Cifrado RSA.

Para cifrar un mensaje x, se necesita la clave pública e y m. De esta manera, el mensaje a cifrar y, se obtiene por[72]:

$$y = x^e\ mod\ m$$

3.2.1.2. Descifrado RSA.

Para descifrar un mensaje y, se necesita de la clave privada d y m. Luego, el mensaje descifrado x se obtiene por la expresión[73]:

$$x = y^d\ mod\ m$$

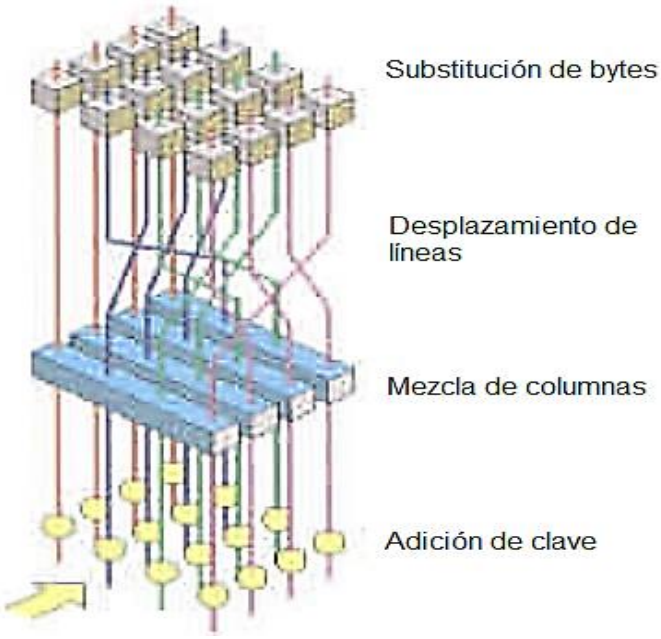
3.2.2. AES (Advanced Encryption Standard).

Es un esquema de cifrado por bloques, de simetría simétrica, considerado por Estados Unidos como estándar efectivo el 26 de mayo de 2002[74]. Este tipo de cifrado puede cifrar bloques de datos de 128 bits, que utiliza claves simétricas de 128, 192 0 256[75].

[72] MARÍ, Noelia. (2018). Op. cit.
[73] Ibid.
[74] GÁLVEZ, Nancy. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles. México D.F. {en línea}. {Consultado 10 junio de 2019}. Disponible en: http://148.204.210.201/tesis/1404316762511NPGMTesisAn.pdf
[75] MEDINA, Yuri & MIRANDA, Haider. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. Revista MundoFesc,. {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55

El funcionamiento de este algoritmo se basa en 4 capas: sustitución de bytes, desplazamiento de líneas, mezcla de columnas y adición de clave, como se muestra en la siguiente imagen[76]:

Figura 3. Funcionamiento algoritmo AES



Fuente: RIBEIRO, Vinicius

De donde[77]:

- Sustitución de bytes: Usa una tabla que realiza en el bloque una sustitución byte a byte.
- Desplazamiento de líneas: permutación simple fila a fila.
- Mezcla de columnas: Cada byte de la columna lo altera en función de todos los bytes de esta.
- Adición de clave: Utiliza la operación XOR bit a bit del bloque resultante con una porción de clave expandida.

[76] RIBEIRO, Vinicius. (2012). Um Estudo Comparativo entre algoritmos de criptografía DES – Lucifer (1977) e AES – Rijndael (2000). {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.5323FC16&lang=es&site=eds-live&scope=site

[77] SAMANIEGO, Ana. (2018). "Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información". Universidad Ricardo Palma. Lima, Perú. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://repositorio.urp.edu.pe/bitstream/handle/URP/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

AES cifra por bloques y los datos a encriptar los divide en segmentos de 16 bits, los cuáles pueden verse con una matriz de 4×4 bytes, llamado Estado. El proceso de funcionamiento de AES se muestra a continuación[78]:

Figura 4. Matriz de estado

Fuente: POUSA, Adrián

AES tiene la característica de algoritmo simétrico, utiliza una misma clave para la encriptación y desencriptación de datos. Se parte de una clave inicial de 16 bytes (128 bits), también vista como matriz de 4×4 bytes, se generan 10 claves, que junto a la inicial son llamadas subclaves.

Para generar las subclaves, se considera la clave inicial, una matriz de 4×4 bytes.

Figura 5. Clave de 128 bits

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

Fuente: POUSA, Adrián

Para calcular las subclaves, estas van una detrás de otra, y puede verse como un arreglo de 4×44.

Figura 6. Subclaves a calcular

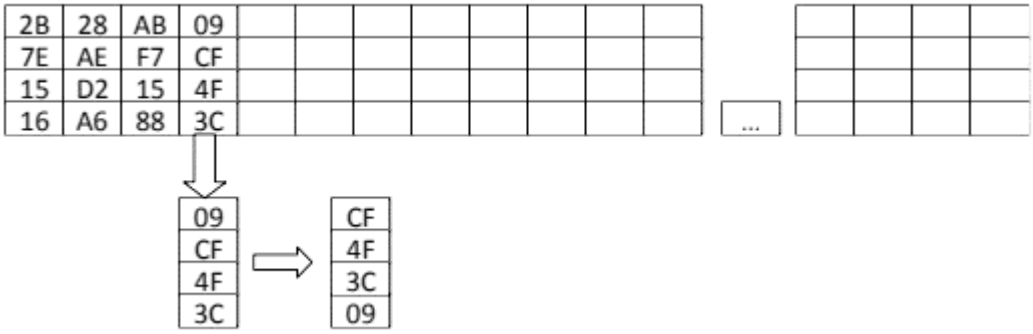
2B	28	AB	09												
7E	AE	F7	CF												
15	D2	15	4F												
16	A6	88	3C									...			

[78] POUSA, Adrián. (2011). Algoritmo de cifrado simétrico AES. Aceleración de tiempo de cómputo sobre arquitecturas multicore. Universidad Nacional de la Plata. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/4210/Documento_completo.pdf?sequence=1&isAllowed=y

Fuente: POUSA, Adrián

El paso que seguir consiste en calcular la columna que sigue inmediatamente después de la última subclave, y posteriormente la operación Rotword que rota el byte de primer al último lugar.

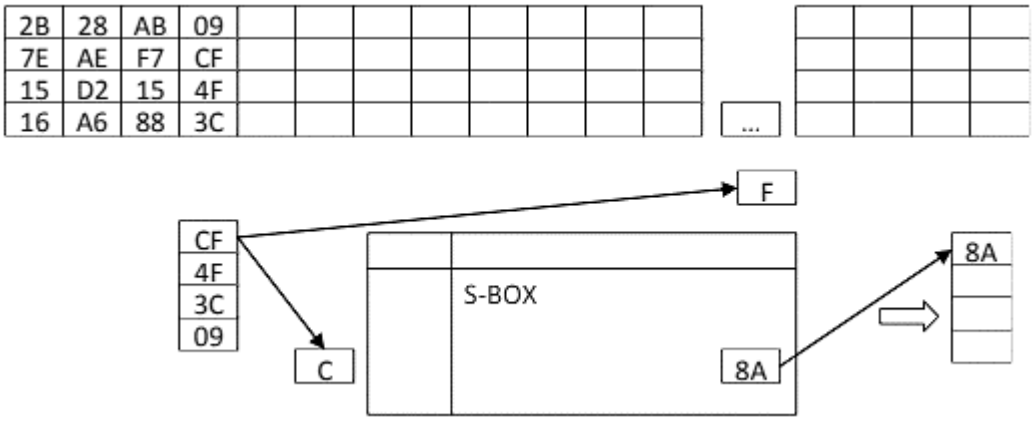
Figura 7. Operación Rotword



Fuente: POUSA, Adrián

A la columna obtenida, le sigue la operación SubBytes, que reemplaza cada byte de la columna que anteriormente se rotó en un byte de una Caja S-Box de 16x16 bytes, que contiene índices de 0 a F. Para obtener esa caja se toman 4 bits como el índice de las filas y los 4 bits siguientes como índices de la columna de la tabla.

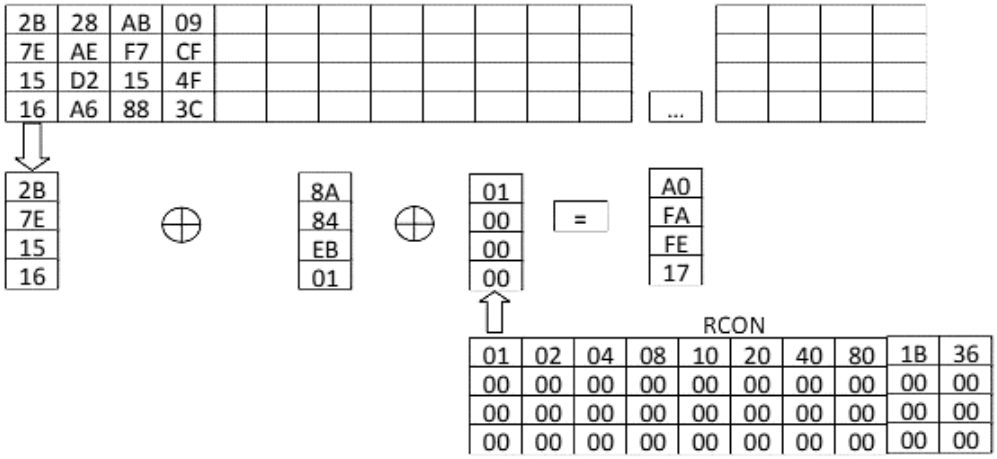
Figura 8. Operación Subway



Fuente: POUSA, Adrián

Al resultado obtenido con la columna ubicada cuatro posiciones atrás se aplica la operación XOR byte a byte, y al resultado nuevamente se le aplica un XOR byte a byte con una columna fija de una tabla llamada RCON para obtener la primera subclave. Para el cálculo de las siguientes subclaves se consideran las columnas siguientes.

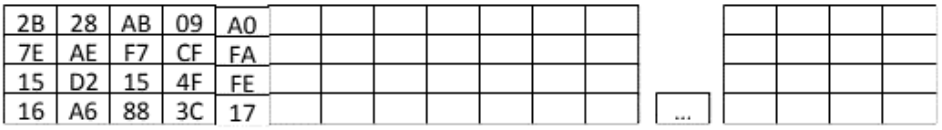
Figura 9. Tabla RCON



Fuente: POUSA, Adrián

Así, se obtendrá la columna que sigue a en la matriz 4×44, siendo la subclave siguiente a la clave inicial.

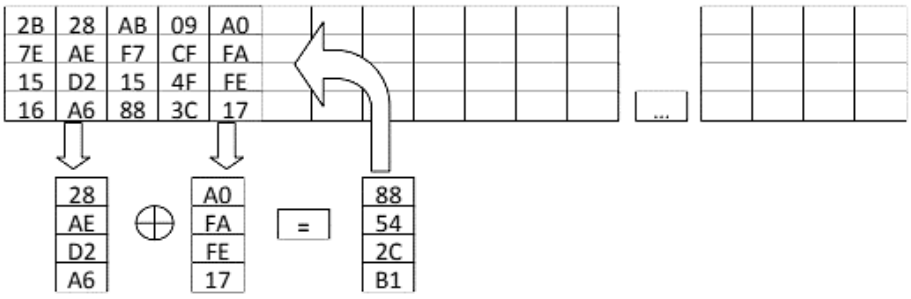
Figura 10. Segunda subclave



Fuente: POUSA, Adrián

Se continúa de manera similar para calcular las tres columnas que siguen. Esto es, aplicando la operación XOR a la columna final con la que se encuentra 4 posiciones atrás.

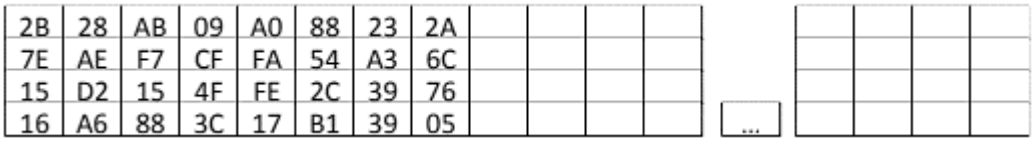
Figura 11. XOR aplicada a la columna final y cuarta anterior



Fuente: POUSA, Adrián

Al final, se obtiene la nueva subclave

Figura 12. Nueva subclave



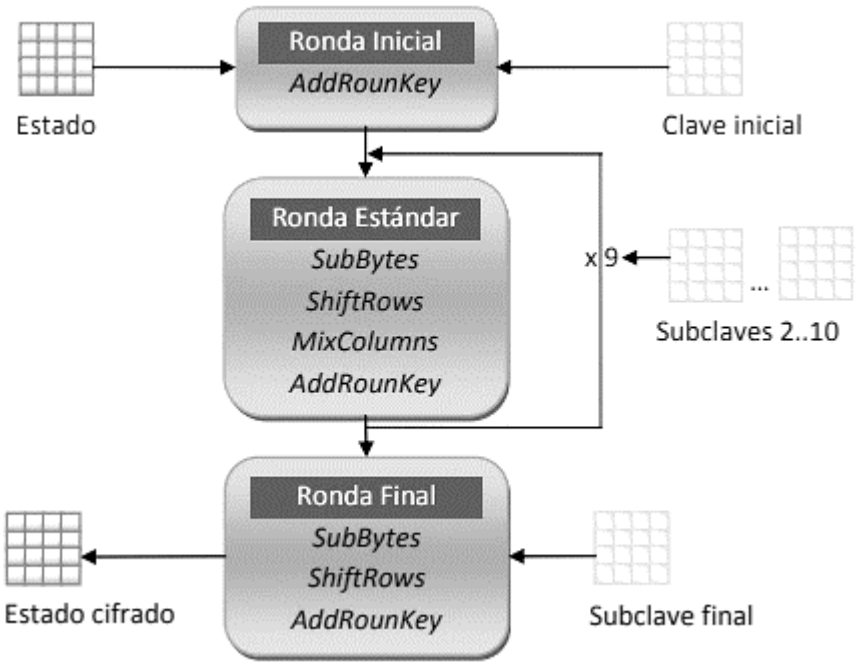
Fuente: POUSA, Adrián

El proceso es similar para calcular las 11 subclaves. Posteriormente, a estas se les aplica las siguientes rondas:

- 1 inicial (aplicada a la subclave inicial)
- 9 estándar (aplicadas a las 9 subclaves siguientes).
- 1 final (aplicada a la subclave final).

Y se utilizan en ellas las siguientes 4 operaciones básicas: SubBytes, ShiftRows, MixColumns y AddRoundKey, las cuales se explican más adelante.

Figura 13. Aplicación de operaciones y claves



Fuente: POUSA, Adrián

En la ronda inicial se aplica un XOR byte a byte del bloque a cifrar con la clave inicial. Esta operación se llama AddRoundKey.

Figura 14. Operación AddRoundKey

Fuente: POUSA, Adrián

En las siguientes 9 rondas estándar se tienen en cuenta las siguientes cuatro operaciones:

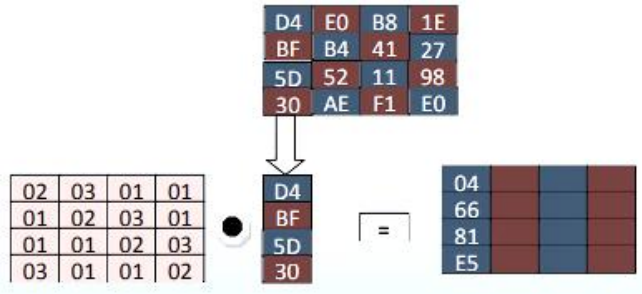
- **SubBytes:** Consiste en reemplazar cada byte de la matriz estado, por otro valor que depende de los valores en la caja S-Box..
- **ShiftRows:** Se mantiene fija la primera fila, y los bits de las otras filas se rotan hacia la izquierda el siguiente número de posiciones: una la segunda fila, dos la tercera fila y tres la cuarta fila.

Figura 15. Operación ShiftRows

Fuente: POUSA, Adrián

- **MixColumns:** Se multiplica a cada columna del estado una matriz ya dada en el campo GF.

Figura 16. Operación Mixcolums



Fuente: POUSA, Adrián

- **AddRoundKey:** Consiste en aplicar la misma operación aplicada en la ronda inicial, pero esta vez considerando otra subclave.

Finalmente, se aplica la ronda final, mediante las operaciones: **SubBytes** y **ShiftRows**, similares a la ronda estándar, y **AddRoundKey:** se parece a la ronda inicial y estándar, pero aplicando la última subclave.

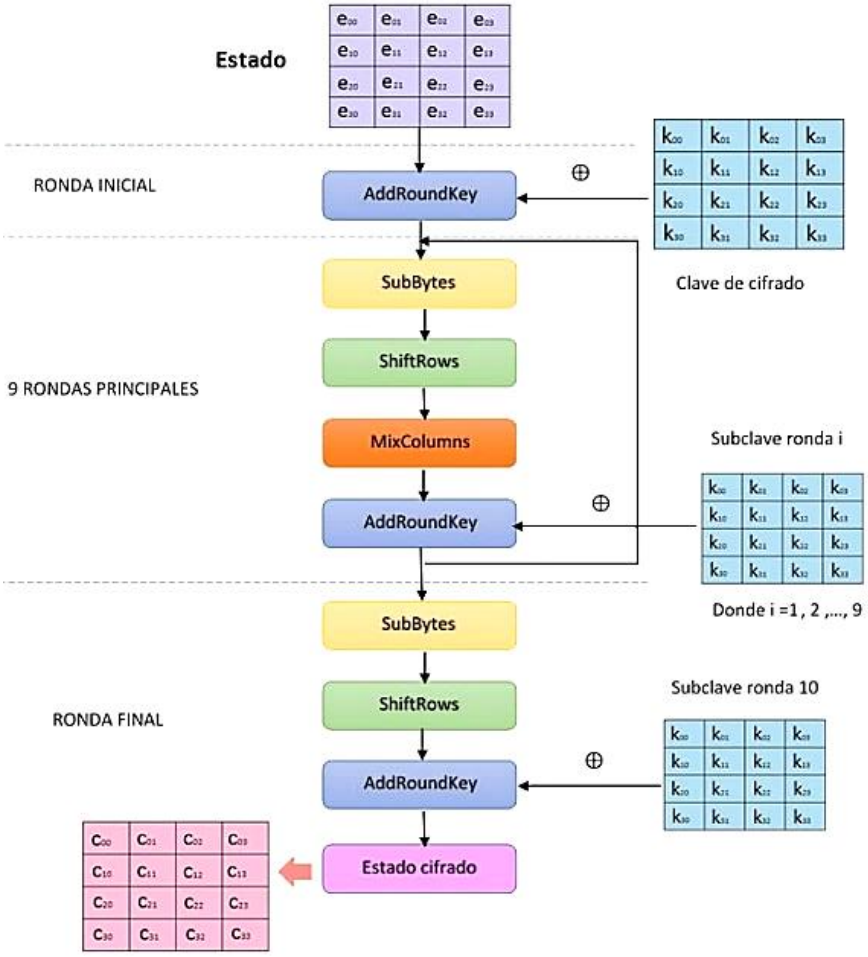
El proceso de descifrado de este algoritmo utiliza las mismas operaciones de cifrado, pero en forma inversa.

3.2.2.1. Cifrado AES.

El proceso de cifrado AES lo muestra visualmente de la siguiente manera[79]:

[79] RODRÍGUEZ, María. (2014). Implementación del algoritmo de cifrado AES mediante GPUS de Bajo Coste. {en línea}. {Consultado 25 julio de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.2540769C&lang=es&site=eds-live&scope=site

Figura 17. Cifrado AES



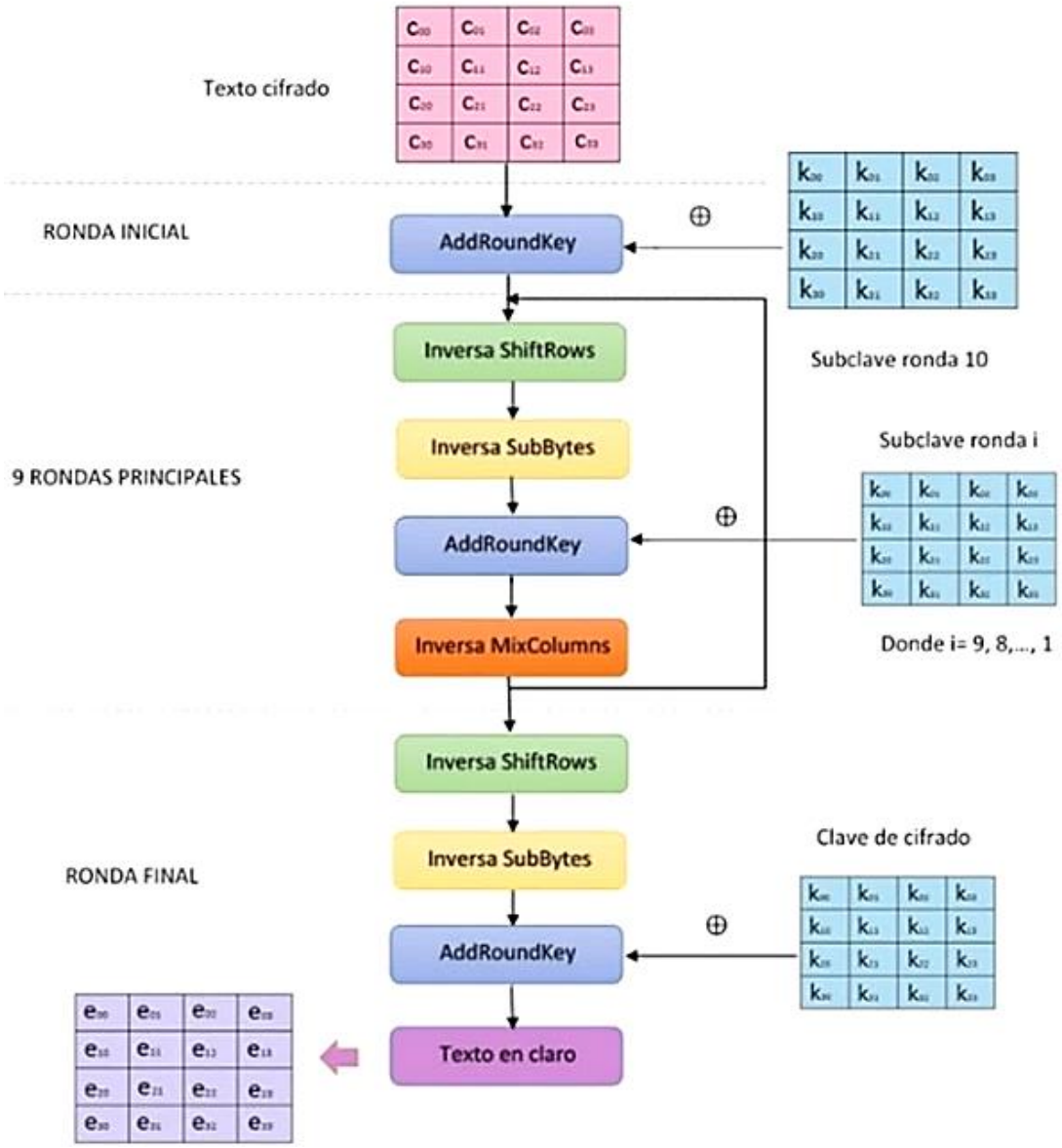
Fuente: RODRIGUEZ, María

3.2.2.2. Descifrado AES.

El proceso de descifrado del algoritmo AES puede verse visualmente por medio de la siguiente figura[80].

[80] RODRÍGUEZ, María. Op. cit

Figura 18. Descifrado AES.



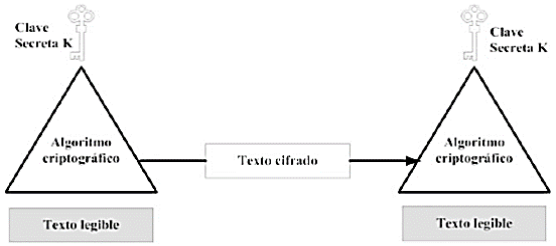
Fuente: RODRIGUEZ, María

3.2.3. IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM).

IDEA es un cifrado de clave privada (algoritmo simétrico) utiliza la misma clave para cifrar y descifrar datos, y su funcionamiento se basa considerando la siguiente figura[81]:

[81] DÍAZ, Gabriel, MUR, Francisco, & SANCRISTÓBAL, Elio. Op. cit

Figura 19. Funcionamiento de algoritmo de clave privada



Fuente: DIAZ et al.

El funcionamiento del algoritmo IDEA se muestra a continuación[82].

El algoritmo encripta un bloque de texto plano de 64 bits a un bloque cifrado de este mismo tamaño, usando una clave de 128 bits. Este algoritmo utiliza 8 rondas idénticas y una ronda intermedia (transformación de salida). Además, es controlado por una clave de 128 bits, y funciona con base a tres operaciones: XOR a nivel de bits $(\oplus)$ módulo multiplicativo y $(\boxplus)$ módulo aditivo $(\odot)$. La operación módulo aditivo 216, y la multiplicación módulo 216+1, indican qué existe 216 posibles bloques de 16 bit: $0000000000000000 \ldots 1111111111111111$. El texto plano con bloque de 64 bits se divide en cuatro bloques de 16 bits $(X1||\, X2||\, X3||\, X4)$. La clave es un bloque de 128 bits dividida en ocho subclaves de 16 bits. Cada Round usa seis subclaves de 16 bits y el resto de subclaves se usan en el siguiente Round implementando un desplazamiento de 25 posiciones a la izquierda. La totalidad de subclaves es 52.

Tabla 5. Cifrado y descifrado de subclaves

Ronda No.	Subclave de encriptación	Subclave de desencriptación
1	$Z_1^{(1)} Z_2^{(1)} Z_3^{(1)} Z_4^{(1)} Z_5^{(1)} Z_6^{(1)}$	$Z_1^{(9)-1} - Z_2^{(9)} - Z_3^{(9)} Z_4^{(9)-1} Z_5^{(8)} Z_6^{(8)}$
2	$Z_1^{(2)} Z_2^{(2)} Z_3^{(2)} Z_4^{(2)} Z_5^{(2)} Z_6^{(2)}$	$Z_1^{(8)-1} - Z_2^{(8)} - Z_3^{(8)} Z_4^{(8)-1} Z_5^{(7)} Z_6^{(7)}$
3	$Z_1^{(3)} Z_2^{(3)} Z_3^{(3)} Z_4^{(3)} Z_5^{(3)} Z_6^{(3)}$	$Z_1^{(7)-1} - Z_2^{(7)} - Z_3^{(7)} Z_4^{(7)-1} Z_5^{(6)} Z_6^{(6)}$
4	$Z_1^{(4)} Z_2^{(4)} Z_3^{(4)} Z_4^{(4)} Z_5^{(4)} Z_6^{(4)}$	$Z_1^{(6)-1} - Z_2^{(6)} - Z_3^{(6)} Z_4^{(6)-1} Z_5^{(5)} Z_6^{(5)}$
5	$Z_1^{(5)} Z_2^{(5)} Z_3^{(5)} Z_4^{(5)} Z_5^{(5)} Z_6^{(5)}$	$Z_1^{(5)-1} - Z_2^{(5)} - Z_3^{(5)} Z_4^{(5)-1} Z_5^{(4)} Z_6^{(4)}$
6	$Z_1^{(6)} Z_2^{(6)} Z_3^{(6)} Z_4^{(6)} Z_5^{(6)} Z_6^{(6)}$	$Z_1^{(4)-1} - Z_2^{(4)} - Z_3^{(4)} Z_4^{(4)-1} Z_5^{(3)} Z_6^{(3)}$
7	$Z_1^{(7)} Z_2^{(7)} Z_3^{(7)} Z_4^{(7)} Z_5^{(7)} Z_6^{(7)}$	$Z_1^{(3)-1} - Z_2^{(3)} - Z_3^{(3)} Z_4^{(3)-1} Z_5^{(2)} Z_6^{(2)}$
8	$Z_1^{(8)} Z_2^{(8)} Z_3^{(8)} Z_4^{(8)} Z_5^{(8)} Z_6^{(8)}$	$Z_1^{(2)-1} - Z_2^{(2)} - Z_3^{(2)} Z_4^{(2)-1} Z_5^{(1)} Z_6^{(1)}$
Salida/ transformación	$Z_1^{(9)} Z_2^{(9)} Z_3^{(9)} Z_4^{(9)}$	$Z_1^{(1)-1} - Z_2^{(1)} - Z_3^{(1)} Z_4^{(1)-1}$

Fuente: ALMASRI, Osama & MAT, Hajar

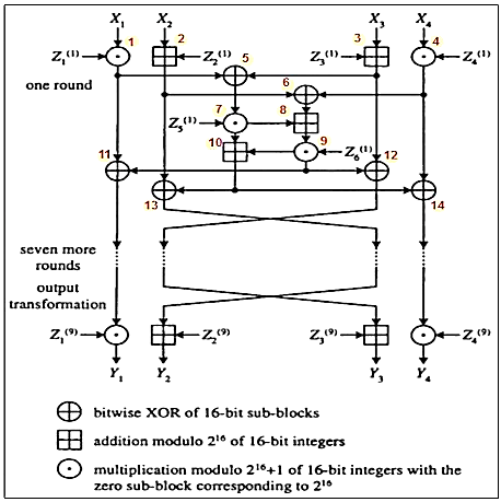
[82] ALMASRI, Osama & MAT, Hajar. Op. cit

Los siguientes pasos muestran el proceso de encriptación en cada Round.

1. La primera multiplicación entre X_1 y la primera subclave Z_1
2. La operación de adición de X_2 con la segunda subclave Z_2
3. La operación de adición de X_3 con la tercera subclave Z_3
4. La segunda multiplicación entre X_4 y la cuarta subclave Z_4
5. Calcular la operación XOR del nivel de bits de los resultados 1 y 3.
6. Calcular la operación XOR del nivel de bits de los resultados 2 y 4.

A continuación, se muestra la estructura del proceso de encriptación IDEA

Figura 20. Estructura del proceso de cifrado IDEA



Fuente: ALMASRI, Osama & MAT, Hajar

3.2.4. RC4 (RIVEST CIPHER 4).

RC4 es un tipo de cifrado simétrico, pero no de bloque. Es un esquema de cifrado de flujo, más utilizado en el mundo, que parte de una clave secreta conocida por el emisor y receptor, y la operación que utiliza habitualmente es XOR. Este tipo de cifrado funciona en tres partes: Inicialización del vector de estado (KSA, key-scheduling algorithm), generación del flujo de cifrado (PRGA, pseudo-random generation algorithm) y mezcla del texto con el flujo de cifrado[83].

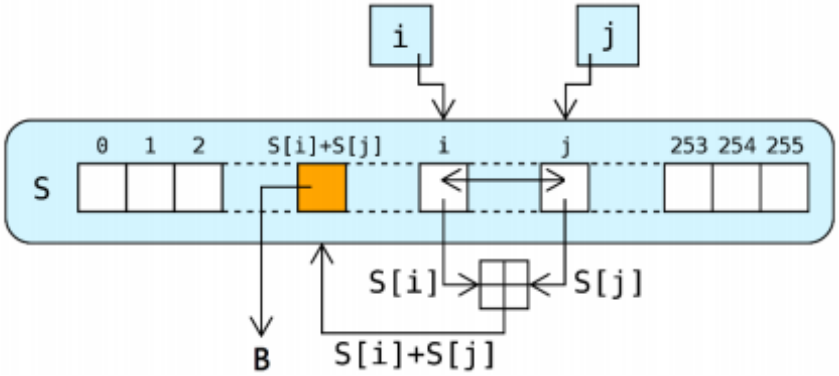
El algoritmo se describe como sencillo y eficaz, diferenciado en dos algoritmos, que crean y emplean una caja de sustitución 8×8, esto es, un arreglo de 256 bytes que

[83] GARCIA, Alicia. El cifrado RC4. Universidad de Salamanca. {en línea}. {Consultado 1 agosto de 2019}. Disponible en: http://rufian.eu/Cifrado_RC4/

emplea una permutación de los números 0 al 255, y menciona su funcionamiento como sigue[84]:

La Caja de sustitución (S-box) inicializa con el primer algoritmo, KSA (Key Scheduling Algorithm), permutando los 256 elementos que pertenecen al arreglo inicial. Continúa con el segundo algoritmo, PRGA (Pseudo-Random Generation Algorithm), que se describe en la siguiente imagen:

Figura 21. Funcionamiento del PRGA de RC4



Fuente: MARTINEZ, Francisco

En este, S hace referencia al arreglo inicial, en cada iteración se determinan los dos (i y j) componentes a intercambiarse para posteriormente sumarse módulo 256, y así obtener un byte de salida, llamado B.

Cabe resaltar en cada iteración, que tanto para KSA como PRGA el valor de i cambia en la expresión

$$(i + 1) mod\ 256$$

Mientras que para j en PRGA cambia teniendo en cuenta $(\mathrm{j} + \mathrm{S_i}) \bmod 256$, y para KSA teniendo en cuenta la expresión $(\mathrm{j} + \mathrm{S_i} + \mathrm{K_i}) \bmod 256$, donde $\mathrm{K_i}$ es el byte i de la clave (el vector de la clave de 256 bytes).

3.3. CARACTERÍSTICAS DE LOS ALGORITMOS

Teniendo en cuenta las características estudiadas de los sistemas RSA, AES, IDEA y RC4, se destacó de cada uno las siguientes características:

[84] MARTINEZ, Francisco. (2016). Op. cit.

Tabla 6. Características de los algoritmos RSA, IDEA, AES, RC4

	RSA	**AES**	**IDEA**	**RC4**
Tipo de algoritmo	Asimétrico	Simétrico	Simétrico	Simétrico
Creador	Rivest, Shamir, Adleman	Joan Daemen e incent Rijmen	James Massey	Ron Rivest
Año	1977	1988	1991	1987
Clave	Desde 1024 a 4096 bits	128 bits, 192 bits, 256 bits.	128 bits	40 bits
Operaciones	Exponenciación modular.	Desplazamiento y transposición.	XOR a nivel de bits, adición modular y multiplicación modular.	Adición modular, transposición.
Bases	Sustitución, transformación.	Sustitución, permutación, transformación lineal	Transformación idéntica.	Sustitución, intercambio, permutación
Esquema	Cifrado de flujo	Cifrado de bloque	Cifrado de bloque	Cifrado de flujo
Rondas	1	10, 12, 14	8	256
Características	Seguro, baja velocidad	Seguro, reemplazó a DES	Seguro bajo condiciones.	Cifrado rápido en SSL

Fuente: Elaboración propia

3.4. EFICIENCIA DE LOS ALGORITMOS RSA, AES, IDEA Y RC4

La eficiencia de un algoritmo depende de dos variables: espacio en disco y tiempo de ejecución. En el presente capítulo se darán a conocer resultados investigados en distintos documentos que relacionan estas características mencionadas[85].

3.4.1. Eficiencia RSA.

Vargas, Juan en su estudio, muestra que el peso del algoritmo RSA con el que trabaja ocupa 31.5 KB de memoria, mientras que el tiempo de cifrado y descifrado, en segundos, dependiendo del tamaño del paquete, se relaciona mediante la siguiente tabla:

[85] VARGAS, Juan. Op. cit

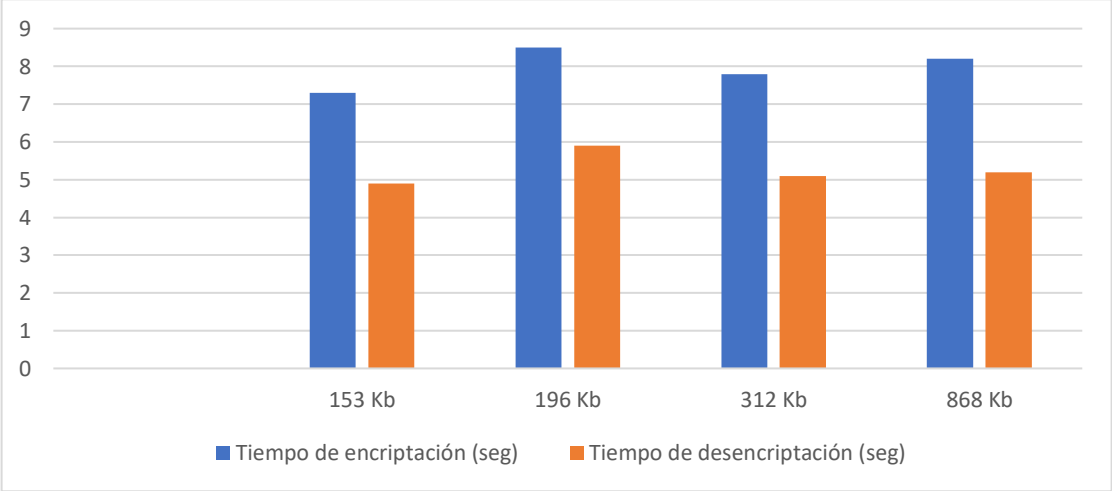
Tabla 7. Tiempo de cifrado y descifrado RSA

Tamaño del paquete	Tiempo de cifrado (s)	Tiempo de descifrado (s)
153 KB	7.3	4.9
196 KB	8.5	5.9
312 KB	7.8	5.1
868 KB	8.2	5.2

Fuente: VARGAS, Juan

Gráficamente, estos resultados se muestran a continuación.

Figura 22. Gráfica tiempo de cifrado y descifrado RSA



Fuente: VARGAS, Juan

Según la gráfica, puede notarse que las variables no tienen un comportamiento directa o inversamente proporcional.

Ahora, se procede a calcular el rendimiento del algoritmo. Para ello, se calcula el promedio de paquetes (382,250 KB), el promedio de tiempo de cifrado (7,950 s) y el promedio de tiempo de descifrado (5,275 s).

$$R = \frac{m}{Tc} = \frac{382{,}250\ Kb}{7{,}950\ s} = 48{,}081\ Kb/s$$

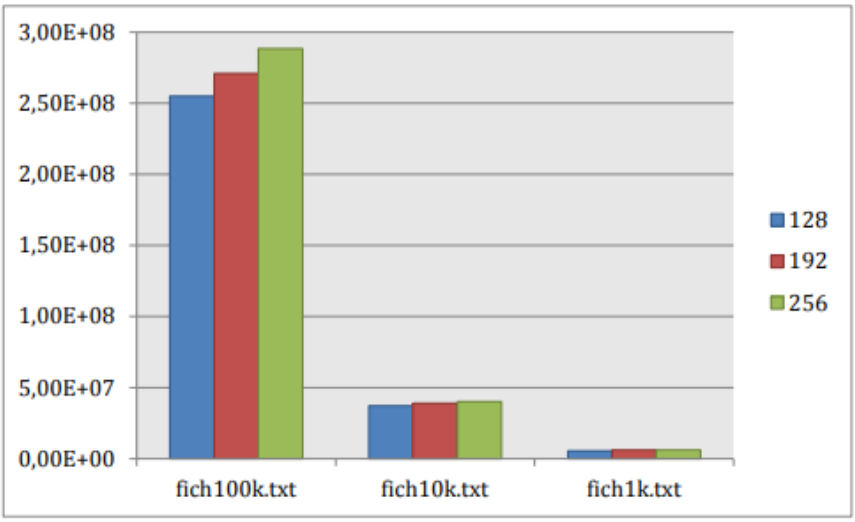
$$R = \frac{m}{T_d} = \frac{382{,}250\ Kb}{5{,}275\ s} = 74{,}464\ Kb/s$$

De acuerdo a lo obtenido, el rendimiento en el cifrado de RSA es $48{,}081\ Kb/s$, mientras que el rendimiento de descifrado es $74{,}464\ Kb/s$. Con esto, el algoritmo RSA tiene mejor rendimiento para el descifrado.

3.4.2. Eficiencia AES.

El algoritmo AES, trabaja con los tamaños de clave de 128, 192 y 256 bits, estos tamaños de clave se relacionan con la forma de operar del algoritmo, dependiendo del tamaño de ficheros a cifrar[86]. Los resultados los muestra en la siguiente figura:

Figura 23. Evolución del tiempo de cifrado AES



Fuente: De la Fuente, Elma

En el gráfico puede observarse lo siguiente:-

1. Si el tamaño del fichero es de 1k, el tiempo de cifrado es similar usando las tres claves.
2. Si el tamaño del fichero es de 10k, el tiempo de cifrado es ligeramente mayor en la clave de 256 bits.
3. Si el tamaño de fichero es de 100k, ya puede verse diferencias más notorias. Para este tamaño, el tiempo de encriptación tarda dependiendo del tamaño de la clave de bits utilizada.
4. Con esto, se puede concluir que el tamaño del fichero con el tiempo que tarda en cifrar son dos variables directamente proporcionales, entre mayor sea el tamaño del fichero, mayor será el tiempo de cifrado.

[86] DE LA FUENTE, Elma. Op. cit

De igual manera, el algoritmo AES con el que trabaja ocupa 14,7 KB de memoria, y los tiempos de cifrado y descifrado se muestran a continuación[87].

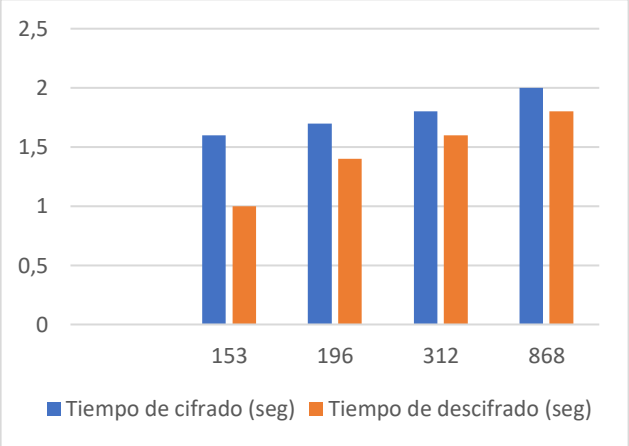
Tabla 8. Tiempo de cifrado y descifrado AES

Tamaño del paquete	Tiempo de cifrado (seg)	Tiempo de descifrado (seg)
153 KB	1.6	1
196 KB	1.7	1.4
312 KB	1.8	1.6
868 KB	2.0	1.8

Fuente: VARGAS, Juan

Gráficamente, estos resultados pueden verse a continuación

Figura 24. Tiempo de cifrado y descifrado RSA



Fuente: VARGAS, Juan

De lo anterior, puede deducirse que:

- Las variables estudiadas tienen un comportamiento directamente proporcional, esto es, entre mayor es el tamaño del paquete mayor tiempo gasta en encriptar o desencriptar el documento.

Se procede ahora a calcular el rendimiento de cifrado R_c y descifrado R_d del algoritmo. Para ello, se calcula el promedio de paquetes (382,250 KB), el promedio de tiempo de cifrado (1,775 s) y el promedio de tiempo de descifrado (1,450 s).

$$R = \frac{m}{T_c} = \frac{382{,}250\ Kb}{1{,}775\ s} = 215{,}35\ KB/s$$

[87] VARGAS, Juan. Op. cit

$$R = \frac{m}{T_d} = \frac{382{,}250\ Kb}{1{,}450\ s} = 263{,}62\ KB/s$$

Teniendo en cuenta estos resultados, el rendimiento de cifrado de AES es $215{,}35\ KB/s$, mientras que el rendimiento de descifrado es $263{,}62\ KB/s$. Por consiguiente, el algoritmo tiene mejor rendimiento en el descifrado

3.4.3. Eficiencia IDEA.

El algoritmo IDEA trabaja con clave de 128 bits, los tiempos de cifrado y descifrado de archivos con diferente tamaño son los siguientes[88]:

Tabla 9. Tiempo de cifrado y descifrado IDEA

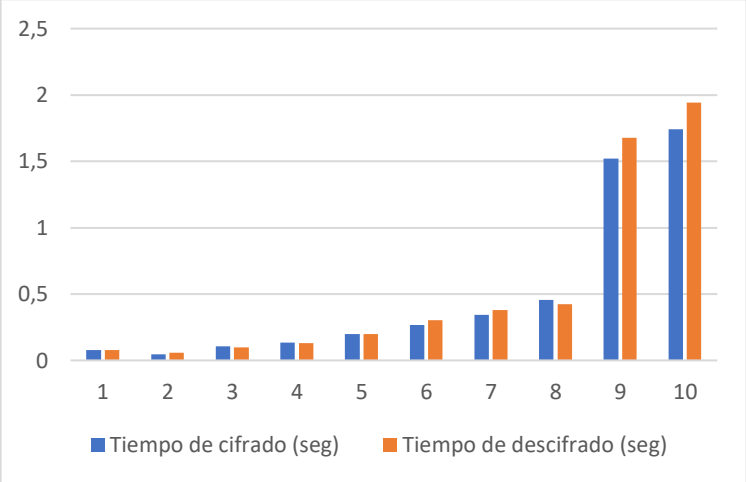
Paquete (KB)	Cifrado (s)	Descifrado (s)
49	0.078	0.078
59	0.046	0.056
100	0.104	0.097
247	0.134	0.131
321	0.198	0.198
694	0.267	0.301
899	0.342	0.378
963	0.456	0.423
5345	1.521	1.676
7310	1.743	1.943

Fuente: BHARATI et al.

Gráficamente, estos resultados pueden verse a continuación:

[88] BHARATI, B & MANIVASAGAM, G & KUMAR, M. (2017). Metrics for performance evaluation of encryption algorithms. International journal of advance research in science and engineering. {en línea}. {Consultado 19 septiembre de 2019}. Disponible en: https://pdfs.semanticscholar.org/32af/f95d61af85e45970c5051d3be79e66163fdc.pdf

Figura 25. Tiempo de cifrado y descifrado IDEA



Fuente: BHARATI et al.

Teniendo en cuenta estos valores, se procede a calcular el rendimiento del algoritmo. Para ello, se calcula el promedio de cifrado (0,4889 s), el promedio de tiempo de descifrado (0,5281 s) y el promedio de paquetes (1598,7 KB).

$$R_c = \frac{m}{T_c} = \frac{1598.7}{0.4889} = 3.269{,}99\ KB/s$$

$$R_d = \frac{m}{T_d} = \frac{1598.7}{0.5281} = 3027{,}26\ KB/s$$

De acuerdo a los resultados obtenidos, el rendimiento de cifrado es $3.269{,}99\ KB/s$ y de descifrado $3027{,}26\ KB/s$. Por consiguiente, IDEA tiene mejor rendimiento en el cifrado.

3.4.4. Eficiencia RC4.

El algoritmo RC4 trabaja con tamaños de las claves de 64, 128 y 256 bits, y algunos resultados de este algoritmo, que pueden resumirse en la siguiente tabla[89]:

[89] CABRERA, Claudio. Op. cit.

Tabla 10. Evolución tiempo de cifrado RC4

T. archivo / T. Clave	500k	1 Mb	10 Mb
64 bit	0,094	0,172	1,484
128 bit	0,094	0,156	1,453
256 bit	0,078	0,156	1,469

Fuente: CABRERA, Claudio

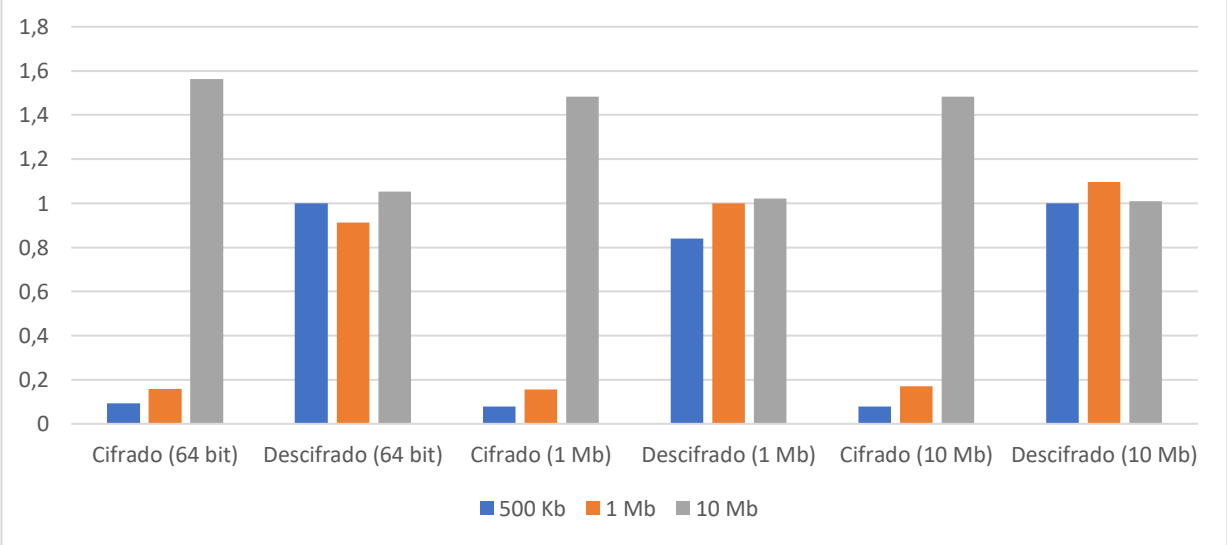
Tabla 11. Evolución tiempo de descifrado RC4

T. archivo / T. Clave	500k	1 Mb	10 Mb
64 bit	0,094	0,157	1,563
128 bit	0,079	0,156	1,484
256 bit	0,078	0,171	1,484

Fuente: CABRERA, Claudio

La gráfica que los relaciona se muestra a continuación:

Figura 26. Evolución tiempo de cifrado y descifrado RC4



Fuente: CABRERA, Claudio

En este tipo de algoritmo puede notarse que las variables no tienen un comportamiento directa o inversamente proporcional. Ahora, se muestra el cálculo de rendimiento del algoritmo.

Tabla 12. Rendimiento RC4

Rendimiento cifrado (KB/s)	
64 bit	6339,581
128 bit	6689,936
256 bit	6635,891

Fuente: CABRERA, Claudio

Tabla 13. Rendimiento descifrado RC4

Rendimiento descifrado (KB/s)	
64 bit	3877,243
128 bit	4018,505
256 bit	3702,076

Fuente: CABRERA, Claudio

Con el fin de tomar el mejor representante, para el rendimiento del algoritmo, se procede a tomar el promedio de los rendimientos de cifrado R_c y descifrado R_d. Esto es,

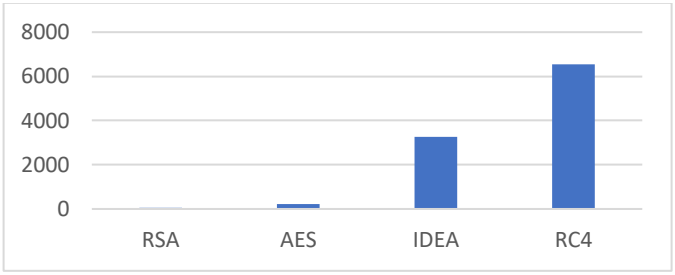
$$R_c = 6555{,}13\ Kb/s \qquad\qquad R_d = 3865{,}94\ Kb/s$$

De lo anterior, puede concluirse que el algoritmo RC4 tiene mejor rendimiento en el cifrado.

3.5. COMPARACIÓN DE RENDIMIENTO DE LOS ALGORITMOS

A continuación, se muestra el compilado de los rendimientos obtenidos anteriormente.

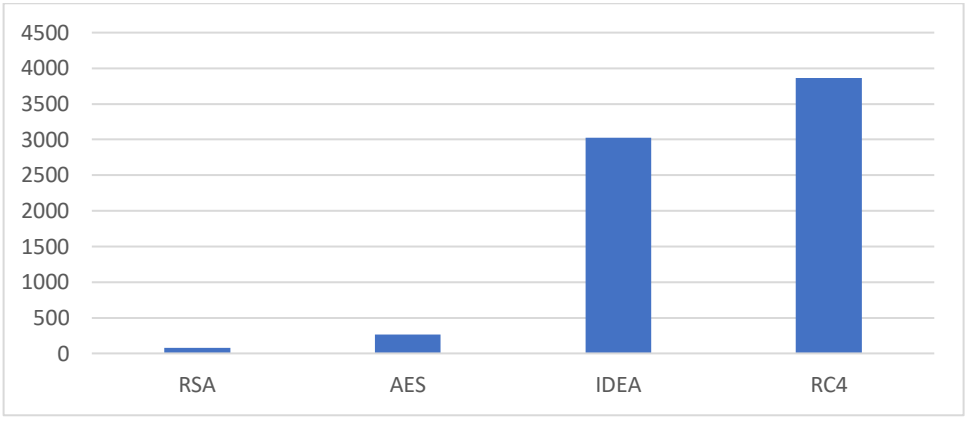
Figura 27. Rendimiento cifrado algoritmos



Fuente: Elaboración propia

Claramente, puede observarse que de los cuatro algoritmos el de mejor rendimiento de cifrado es RC4.

Figura 28. Rendimiento descifrado de algoritmos



Fuente: Elaboración propia

De igual manera, de los cuatro algoritmos el de mejor rendimiento en el descifrado también es RC4.

3.6. ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS FRENTE A AMENAZAS INFORMÁTICAS

En la actualidad lo concerniente a la seguridad de transferencia de información es algo a lo cual debe darse importancia, particularmente hablando, del continuo desarrollo de la comunicación en redes (como Internet). Junto a esto, las amenazas van en desarrollo paralelo y buscan vulnerar la seguridad de la información transmitida por medio de diversos algoritmos que atentan contra los pilares de la seguridad informática. En los siguientes subcapítulos se darán a conocer ataques

representativos de los cuatro algoritmos tratados en esta monografía: RSA, AES, IDEA y RC4.

3.7. SEGURIDAD DE LOS ALGORITMOS CRIPTOGRÁFICOS

3.7.1. Seguridad de RSA.

Este tipo de algoritmo basa su seguridad en la dificultad de hallar dos factores primos de un número compuesto muy grande, los cuáles también son grandes. El cifrado parte al dar dos números primos cualquiera y multiplicarlos (el procedimiento es sencillo), pero, el proceso contrario es más complicado, es decir, hallar a partir de un número compuesto dos factores. Se considera el caso de dos números primos de 155 dígitos (esto es 512 bits), su producto resulta un número de alrededor de 310 dígitos (es decir 1024 bits). Computacionalmente esto se vuelve intratable cuando los números primos tienen cada vez más dígitos[90].

3.7.2. Seguridad de AES.

Este algoritmo se reconoce por ser estándar de cifrado simétrico que reemplazó el 2 de octubre del 2000 a Triple DES. Considerado por ser un algoritmo robusto y según estudios, eficiente en seguridad a la hora de recibir un ataque de fuerza bruta, cuando la clave es de longitud grande. Considerando esto, el atacante debe tener en cuenta las siguientes dos características[91]:

- Si hay desconocimiento del texto y la clave, debe suponerse un bloque de "$v\ bits$" y clave de "$n\ bits$" para que el atacante pruebe cada clave 2^v bloques posibles, repitiendo el proceso 2^n veces para todas las claves. Esto es computacionalmente intratable.

- Ahora, si el atacante conoce el texto en claro y el texto cifrado podría pensar en un ataque por fuerza bruta, probando todas las claves posibles hasta obtener un resultado parecido que lleve al texto cifrado. El atacante necesita probar el texto en claro el siguiente número de veces:

  La clave de 128 bits

[90] AGUIRRE, Jorge. (2018). Curso de criptografía aplicada. Madrid. {en línea}. {consultado 18 marzo de 2019}. : Disponible en: http://www.criptored.upm.es/descarga/CursoCriptografiaAplicada2018.pdf
[91] MUÑOZ, Alfonso. (2004). CRIPTOSISTEMA RIJNDAEL. A FONDO, Algoritmo Criptografico Rijndael. {en línea}. {Consultado 26 septiembre de 2019}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m480a.htm

Así, hoy en día este tipo de cálculos son computacionalmente intratables e imprácticos.

3.7.3. Seguridad de IDEA.

La seguridad de este algoritmo se basa en los siguientes aspectos[92]:

- La imposibilidad de calcular computacionalmente las claves.
- Este algoritmo tiene 8 vueltas, y la aplicación de criptoanálisis diferencial no puede hacerse a partir de la cuarta vuelta.

Pero, estas características no son suficientes para determinar 100% al algoritmo seguro. Por ser un algoritmo que trabaja por bloques para una clave, si se deducen varios subbloques de esta, se puede deducir la clave. Es decir, no es seguro.

Además, con la característica de manejar clave secreta se presentarían los siguientes inconvenientes:

- La selección de la clave secreta de los dos usuarios que se comunican no siempre es segura.
- La obtención de claves se facilita al atacante, si se hace uso de un canal inseguro.
- Por no contar con firma digital quien recibe el mensaje no puede saber con seguridad quien envía el mensaje.

Estas características hacen que el algoritmo IDEA, bajo estas condiciones, se considere un algoritmo no fiable en un 100%.

3.7.4. Seguridad de RC4.

Respecto a la seguridad de RC4 podría decirse que no es tan fiable en el proceso de encriptación. De hecho, este algoritmo está en desuso debido a vulnerabilidades críticas descubiertas. En febrero de 2015 la organización internacional IETF recomienda que eliminen este cifrado para conexiones TLS entre cliente y servidor[93]. Además, las llaves de este algoritmo tienen una extensión de 40 bits, lo que traduce un alto grado de vulnerabilidad frente a ataques de fuerza bruta.

[92] LITWAK, Noelia & ESCALANTE, Jaquelina. (2004). Seguridad Informática y criptografía. (trabajo de pregrado). Universidad Nacional de Nordeste, Argentina. {en línea}. {Consultado 1 octubre de 2019}. Disponible en: http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf
[93] AGUIRRE, Jorge. Op. cit

3.8. ATAQUES A LOS ALGORITMOS CRIPTOGRAFICOS

3.8.1. Ataques a RSA.

Este sistema que apareció en 1977 ha sido blanco de numerosos ataques desde entonces, pero a pesar de los distintos intentos hasta ahora, no se conoce ataque que comprometa su seguridad. A continuación, se muestran algunos ataques a RSA que son conocidos[94].

3.8.1.1. Cifrado cíclico

Consiste en el cifrado repetido del criptograma que ha sido interceptado con clave pública del destinatario, tantas veces como sea necesario hasta obtener nuevamente dicho criptograma. Para dar un ejemplo del caso, se toma un valor pequeño del módulo, $n = 52841$, ahora suponiendo que el criptograma interceptado es $c^e = 1855$, se tiene:

$$\downarrow$$

$$c_1 = c^e (mod\ n) = 1.855 (mod\ 52.841) = 23.797$$

$$c_2 = c_1^e (mod\ n) = 23797 (mod\ 52.841) = 25.334$$

$$c_3 = c_2^e (mod\ n) = 25334 (mod\ 52.841) = 12.508$$

...

$$c_{40} = c_{39}^e (mod\ n) = 46.640 (mod\ 52.841) = 17.225$$

$$c_{41} = c_{40}^e (mod\ n) = \boxed{17.225} (mod\ 52.841) = 1.855 \leftarrow$$

En este caso, podemos notar que conseguimos el mensaje cifrado **17225** cuando han ocurrido 41 iteraciones. Sin embargo, este es un caso particular para n, el algoritmo original, como ya se ha mencionado, trabaja para valores de n muy grandes, lo que hace que utilizando este método la cantidad de ciclos es extremadamente elevada. Por ello estos ataques no son considerados como una amenaza real a la seguridad del criptosistema.

3.8.1.2. Factorización

Básicamente este tipo de ataque consiste en conseguir la clave privada de RSA, por medio de algoritmos de factorización. Sin embargo, esto es útil para casos particulares (para valores de n pequeños), como ya se dijo anteriormente, resulta computacionalmente intratable para valores de n muy grandes (por ejemplo, de 310

[94] MARI, Noelia. Op. cit

dígitos). Para el ejemplo, se considera el algoritmo de Fermat, cuya entrada es el número impar 5959 y la salida el producto de la suma por la diferencia.

Ingresa $n = 5959$

Se obtiene $a = \sqrt{5959} \sim 78$

Se analiza $a^2 - n$ sea un cuadrado perfecto

$78^2 - 5959$ no es cuadrado perfecto

Se procede $a = 78 + 1 = 79$

$79^2 - 5959$ no es cuadrado perfecto

Se procede $a = 79 + 1 = 80$

$80^2 - 5959 = 441$ es cuadrado perfecto

Se calcula $b = \sqrt{441} = 21$

Se obtiene $(80 + 21)(80 - 21)$

Sin embargo, esto es práctico para valores de n pequeños, en el caso del algoritmo RSA maneja valores de n muy grandes, lo que hace este algoritmo impráctico y computacionalmente imposible de tratar. Este tipo de ataque no es una amenaza a la seguridad de RSA.

3.8.2. Ataques a AES.

El sistema AES se caracteriza por su fortaleza en el cifrado y el hecho de que teóricamente es imposible conseguir el texto original partiendo del texto cifrado, sin conocer la clave de cifrado. Además, por tratarse de un estándar adoptado por el NIST y siendo base de encriptado de documentos oficiales, así como también, por su elevada seguridad ha sido blanco de gran cantidad de ataques. A continuación, se mencionan los más representativos[95].

[95] LUMBIARRES, Rubén; LÓPEZ, Mariano & CANTO, Enrique. (2013). Ataques por canal lateral sobre el algoritmo de encriptación AES implementado en MicroBlaze. {en línea}. {Consultado 19 octubre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.C3E6C7DD&lang=es&site=eds-live&scope=site

3.8.2.1. Ataque por fuerza bruta a AES

Este tipo de ataque básicamente consiste en probar todas las combinaciones de caracteres hasta hallar la palabra correcta, y consta de los siguientes elementos[96]:

- Un diccionario (archivo con todas las posibles combinaciones)

- Una longitud de palabra (para determinar las posibles combinaciones)

- Palabra cifrada (la clave de cifrado)

- Algoritmo de cifrado (definido por el usuario).

Para el caso particular de AES, este tipo de ataque se lleva a cabo si se conoce el texto en claro y el texto cifrado. Por ejemplo, se supone que la clave a buscar sea de cuatro caracteres 'UNAD', entonces, el diccionario debe almacenar 2^4 combinaciones (que se muestran a continuación), y probar cada una hasta dar con la correcta.

Tabla 14. Combinaciones posibles de "UNAD"

AUND	AUDN	ADUN	ADNU
NUAD	NUDA	NAUD	NADU
UNAD	UNDA	UAND	UADN
DAUN	DANU	DNUA	DNAU

Fuente: Elaboración propia

Cabe resaltar que AES maneja claves de hasta 256 bit, y siendo este el caso la cantidad de permutaciones, como se mencionó es de 2^{255}. Lo que computacionalmente se vuelve intratable, lo que en estos casos no es una amenaza real frente a la seguridad del algoritmo.

3.8.2.2. Ataque por canal lateral

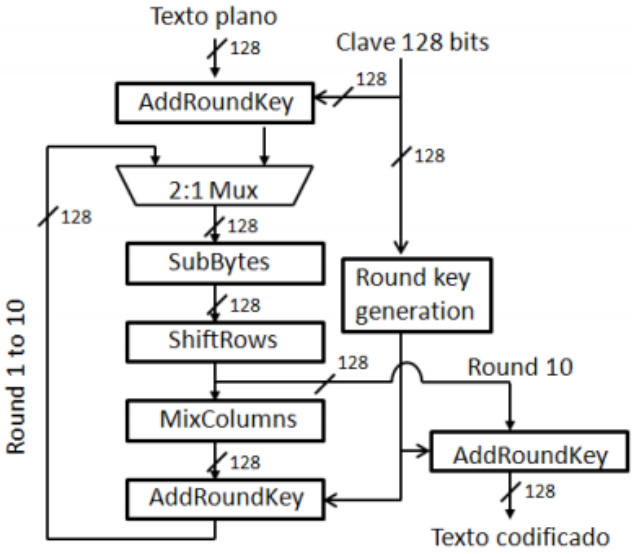
Este tipo de ataque se basa en implementar físicamente un sistema informático, se basa en medir información precisa de una pieza de hardware sobre operaciones que realiza AES[97]. El proceso de ataque a AES consiste en la elección de un punto de ataque descrito en la siguiente figura, para obtener cada byte de la clave del

[96] DOMINGUEZ, Hernán, MAYA, Edgar. & PELUFO, Diego. (2016). Aplicación de Técnicas de Fuerza Bruta con Diccionario de Datos, para vulnerar servicios con métodos de autenticación simple "Contraseñas", pruebas de concepto con software libre y su remediación. {en línea}. {25 octubre de 2019}. Disponible en: https://www.researchgate.net/publication/311922037_Aplicacion_de_Tecnicas_de_Fuerza_Bruta_con_Diccionario_de_Datos_para_vulnerar_servicios_con_metodos_de_autenticacion_simple_Contrasenas_pruebas_de_concepto_con_software_libre_y_su_remediacion

[97] MARI, Noelia. Op. cit

algoritmo[98]. Por extensión de este proceso y la complejidad de fundamentos necesarios para conseguir el ataque, no se describe el proceso, pero se deja la referencia de (Lumbiarres, 2013) en la bibliografía para ser consultada.

Figura 29. Diagrama de bloques para AES 128 bits



Fuente: LUMBIARRES, Rubén

3.8.3. Ataques a IDEA.

Varios han sido los intentos de ataques al algoritmo IDEA y los siguientes son los más representativos y comunes, sin embargo, sólo tienen éxito para claves débiles (que no es común tratarlas) que suelen encontrarse en versiones anteriores de IDEA. En la actualidad se considera uno de los algoritmos más seguros de los de cifrado simétrico[99].

3.8.3.1. Criptoanálisis diferencial

Este ataque puede realizarse a todos los cifrados simétricos y las funciones hash. Consiste en observar las diferencias existentes entre el texto plano y el cifrado (generado por una misma clave) con el fin de extraer la clave más probable[100]. El

[98] LUMBIARRES, Rubén. Op. cit

[99] SOBREVILLA, Pedro. (2016). SEGURIDAD Y EFICIENCIA DE ALGUNAS VARIANTES DEL CRIPTOSISTEMA IDEA. (tesis de postgrado). Universidad Autónoma Metropolitana Iztapalapa. {en línea}. {Consultado 1 noviembre de 2019}. Disponible en: http://mat.izt.uam.mx/mcmai/documentos/tesis/Gen.12-O/Pedro_Sobrevilla.pdf

[100] SAHU, Harish., JADHAV, Vikas., SONAVANE, Shefali, & SHARMA, R.K. (2016). Cryptanalytic Attacks on International Data Encryption Algorithm Block Cipher. Defence Science Journal. {en

ataque de criptoanálisis diferencial, puede usarse ataques lineales para tres y media rondas, pero debido a la complejidad de notación, conocimientos previos para realizarlo se deja como referencia en bibliografía para ser consultado[101]. El autor (Sobrevilla, 2016) muestra que el sistema IDEA es resistente al criptoanálisis diferencial, por lo que se puede concluir que no es una amenaza al mismo.

3.8.3.2. Ataque por fuerza bruta a IDEA

El algoritmo IDEA maneja un espacio de claves de $128\,bits$, esto es 2^{128} posibilidades de claves que sería necesario probar. Lo cual se convierte en algo computacionalmente intratable, por lo que el algoritmo IDEA también es resistente a este ataque[102].

3.8.4. Ataques A RC4.

Este algoritmo es considerado inseguro, por las razones descritas en los siguientes ataques, a continuación, se muestran los más representativos de este sistema.

3.8.4.1. Ataque por fuerza bruta a RC4

Uno de los ataques más efectivos sobre RC4 es el ataque por fuerza bruta, y es que RC4 es susceptible a este, debido a la especificación de manejar clave de 40 bits en el estándar IEEE 802.11, que realmente es corta y que un computador común tardaría máximo un mes en hallarla[103].

3.8.4.2. Ataque Fluhrer, Mantin y Shami (FMS)

Este ataque se basa en una correlación que existe entre los primeros bytes que tiene la clave secreta K de RC4 para generar el keystream[104] X, junto al primer byte de X. Con esta información es posible conseguir el siguiente byte de K, lo que da al atacante una pequeña ventaja de adivinar el siguiente, esto es, una probabilidad mayor a 1/256. Al final, del proceso del ataque, que puede ser consultado en

---

línea}. {Consultado 1 noviembre de 2019}. https://doi-org.bibliotecavirtual.unad.edu.co/10.14429/dsj.66.10798

[101] BORST, Johan. (1996). Differential-linear cryptanalysis of IDEA. ESAT– COSIC Technical Report. {en línea}. {Consultado 10 noviembre de 2019}. Disponible en: https://pdfs.semanticscholar.org/ff93/5085644465a127d73995b747cb45e416a143.pdf?_ga=2.12800759.1533181467.1574699588-190295632.1573436562

[102] International Data Encryption Algorithm (IDEA). {en línea}. {Consultado 10 noviembre}. Disponible en: http://almarip.com/otros/idea/documentacion/index.php

[103] PRIETO, Diego. (2014). Seguridad en redes inalámbricas: el protocolo WEP. (tesis de pregrado). Universidad de Cantabria. {en línea}. {Consultado 10 noviembre de 2019}. Disponible en: https://repositorio.unican.es/xmlui/bitstream/handle/10902/5944/Diego%20Garcia%20Prieto01.pdf?sequence=5&isAllowed=y

[104] Secuencia de caracteres aleatorios combinados con el texto en claro para producir un mensaje cifrado.

PRIETO, Diego la efectividad de conocer la clave depende de la cantidad de paquetes capturados por el atacante, pero no existe un 100% de dicha efectividad, son varias las condiciones a cumplir y muchas claves generadas serán incorrectas. Cabe resaltar que para llevar a cabo el ataque se debe conocer la primera palabra del texto claro, el cual está cifrado. Con ello, es posible averiguar la clave secreta, pero el proceso es demasiado complejo.

3.9. SÍNTESIS DEL ESTUDIO

Teniendo en cuenta las características de seguridad estudiadas en cada algoritmo criptográfico se recuperaron las siguientes características.

Tabla 15. Resumen seguridad algoritmos criptográficos

	RSA	**AES**	**IDEA**	**RC4**
Ataques representativos	Cifrado cíclico, factorización	Ataque por fuerza bruta, ataque por canal lateral	Criptoanálisis diferencial, ataque por fuerza bruta	Ataque por fuerza bruta, Ataque FMS
Tamaño de la clave	Hasta 4096 bits	Hasta 256 bits	128 bits	40 bits
Fortaleza de la clave	Muy segura, cuando ocupa más bits.	Muy segura, cuando ocupa más bits.	Muy segura, si la clave no es débil	Insegura
Dificultad de adivinar la clave	Computacionalmente intratable cuando más grande es la clave.	Computacionalmente intratable cuando más grande es la clave.	Computacionalmente intratable cuando más grande es la clave	No tiene dificultad
Característica de seguridad	Hallar los factores de un número compuesto muy grande.	Los intentos para probar una clave para ataques por fuerza bruta van de 2^{217}a 2^{255} veces.	Tiene 8 vueltas y los ataques de criptoanálisis diferencial no se pueden hacer después de la cuarta vuelta.	Ninguna

Fuente: Elaboración propia

4. CONCLUSIONES

- En el séptimo capítulo de esta monografía correspondiente al primer objetivo, se mostró características de los algoritmos RSA, AES, IDEA y RC4, donde se evidencia que el algoritmo RSA cuenta con las mejores características para catalogarse como un buen sistema de cifrado, por manejar un tamaño de clave superior a los otros algoritmos (hasta 4096 bits) y el hecho de que una clave ocupe más espacio en disco, emplea más tiempo en descifrarla por medio de un ataque informático. A esto se agrega que el sistema maneja dos claves una pública conocida y otra privada que no puede ser compartida a cualquiera, lo que hace más difícil para un atacante tratar de obtenerla.

- En cuestiones de extensión, el sistema RC4 cuenta con un algoritmo corto y fácil de implementar, lo que implica que requiere un mínimo espacio de memoria. Sin embargo, por su poca memoria que ocupa la clave (40 bits), por ser única y fija, entre otras cosas más, no proporciona el nivel de seguridad deseado. Por ello, no es un buen candidato como sistema de cifrado.

- RSA consume más tiempo en el cifrado y descifrado, y consecuente a esto, es el sistema criptográfico que tiene menor rendimiento comparado con AES, IDEA y RC4.

- En el tema de seguridad, ya se dijo que RC4 proporciona un bajo nivel, contrario a este, RSA es el mejor candidato que presenta los mejores niveles, por he hecho de manejar una extensión de clave de hasta 4096 bits (como característica principal), de contar con un algoritmo complejo capaz de soportar múltiples ataques informáticos, sin éxito alguno. Los intentos de conseguir la llave privada, hace que el trabajo de un computador se haga intratable. Por ello, se considera el mejor sistema criptográfico respecto a AES, IDEA y RC4, aunque consecuentemente ocupa más tamaño en disco.

- El sistema de cifrado IDEA sería un buen candidato para cifrado, pero depende mucho de la clave que se use. Si se trata de una clave débil, un ataque de fuerza bruta podría conseguirla sin usar muchos recursos computacionales, frente a esto el mejor candidato sigue siendo RSA.

- Si se considera la variable tiempo de cifrado, respecto a tamaño en disco entonces el mejor candidato a elegir es el sistema AES, que maneja una clave máxima de 256 bits, es decir, como RSA el sistema AES soporta ataques de fuerza bruta, sobre todo cuando la clave es de 128 bits o 256 bits.

RECOMENDACIONES

1. Dado el caso quiera usarse el algoritmo IDEA como sistema de cifrado, se recomienda no usar claves débiles, esto con el fin de evitar que el atacante las obtenga por ataque de fuerza bruta.

2. Para pequeñas empresas o redes virtuales de tipo privadas, se recomienda el uso del sistema criptográfico AES, que ofrece buenos niveles de seguridad y por el hecho de ser estándar internacional, es confiable.

3. Para los sistemas AES y RSA, es recomendable usar el máximo tamaño de clave posible, esto con el fin de garantizar la confidencialidad e integridad de los datos cifrados.

4. Una vez implementado un sistema criptográfico en una organización, es necesario capacitar al personal que lo manipule, puesto que, aunque el sistema elegido sea el más seguro, existen diversas formas de obtener la clave por parte del atacante. Lo conveniente es prevenir a dicho personal frente a las diferentes amenazas que se le puede presentar.

BIBLIOGRAFÍA

AGUIRRE, Jorge. (2018). Curso de criptografía aplicada. Madrid. {en línea}. {consultado 18 marzo de 2019}. : Disponible en: http://www.criptored.upm.es/descarga/CursoCriptografiaAplicada2018.pdf

ALMASRI, Osama & MAT, Hajar. (2013). Introducing an Encryption Algorithm based on IDEA. Universiti Tenaga Nasional. {en línea}. {16 de abril de 2019}. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.679.7495&rep=rep1&type=pdf

ÁLVAREZ, Gonzalo & PÉREZ, Pedro. (2004). Seguridad informática para empresas y particulares. España: McGraw-Hill España. {en línea}. {Consultado 20 febrero de marzo de 2019} Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10498593&tm=1466006497840

ALZATE, Alonso & DUQUE, Néstor. Criptografía una excelente alternativa de seguridad. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://bdigital.unal.edu.co/58103/1/criptografia.pdf

ANGEL, Jose. (2005). Advanced Encryption Standard. México. {en línea}. {Consultado 30 octubre de 2019}. Disponible en: www.criptored.upm.es/guiateoria/gt_m117i.htm

ARROYO, Cilene. (2019). Implantación de un esquema de seguridad informática. {en línea}. {Consultado 28 febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BBED0E78&lang=es&site=eds-live&scope=site

BALBAS, David. (2019). Ataques al criptosistema RSA. (trabajo pregrado). {en línea}. {30 septiembre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.33D0FB00&lang=es&site=eds-live&scope=site

BELTRAN, Julian. (2015). Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. {en línea}. {consultado 3 noviembre de 2019}. Disponible en: https://riunet. upv.es/bitstream/handle/025/5602/Memoria.pdf?sequence=1

BHARATI, B & MANIVASAGAM, G & KUMAR, M. (2017). Metrics for performance evaluation of encryption algorithms. International journal of advance research in science and engineering. {en línea}. {Consultado 19 septiembre de 2019}.

Disponible en: https://pdfs.semanticscholar.org/32af/f95d61af85e45970c5051d3be79e66163fdc.pdf

BOLAÑOS, Fredy; NIETO, Rubén & BERNAL, Álvaro. (2004). Implementación de un Hardware Reconfigurable de los Bloques de un Sistema RSA. Ingeniería y Competitividad, 6(2), 25–34. {en línea}. {Consultado 15 de abril de 2019}. Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=zbh&AN=20417528&lang=es&site=eds-live&scope=site

BORST, Johan. (1996). Differential-linear cryptanalysis of IDEA. ESAT– COSIC Technical Report. {en línea}. {Consultado 10 noviembre de 2019}. Disponible en: https://pdfs.semanticscholar.org/ff93/5085644465a127d73995b747cb45e416a143.pdf?_ga=2.12800759.1533181467.1574699588-190295632.1573436562

BURNETT, M., & KLEIMAN, D. (2006). Perfect Passwords Selection, Protection, Authentication. Rockland, Mass: Syngress. {en línea}. {Consultado 15 septiembre de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=149590&lang=es&site=ehost-live

CABRERA, Claudio. ALGORITMOS DE ENCRIPTACIÓN, DESENCRIPTACIÓN - EVALUACIÓN Y VERIFICACIÓN. Universidad Técnica del Norte. {en línea}. {Consultado 20 septiembre de 2019}. Disponible en: https://docplayer.es/7972090-Algoritmos-de-encriptacion-desencriptacion-evaluacion-y-verificacion.html

CANAVELLI, Juan & AÑINO, María. (2012). Educación en Tecnología y Matemática en Criptografía. {en línea}. {Consultado 7 marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.6CA460F&lang=es&site=eds-live&scope=site

CAÑIHUA, Ruben (2007). Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de tercera generación/Ipv6. Chile Universidad de Chile. {en línea}. {Consultado 27 de marzo} Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10198466&tm=1465508433109

CAPUÑAY, Denys; GUERRERO, Ana & VILLEGAS, Juan. (2016). Análisis Comparativo de Algoritmos Criptográficos. Revista Internacional de TECNOLOGÍA DIGITAL Y ECONOMÍA. {en línea}. {Consultado 4 octubre de 2019}. Disponible en: http://revistas.uss.edu.pe/index.php/ING/article/view/440

CASTILLO, Marco; SANTANA, Nancy; DÍAZ, Alicia; ALMANZA, Germán & CASTILLO, Felipe. (2011). Teoría de números en criptografía y su debilidad ante la posible era de las computadoras cuánticas. Universidad Autónoma del Estado de México. Toluca, México. {en línea}. {Consultado 1 noviembre de 2019}. Disponible en: https://www.redalyc.org/pdf/104/10420073007.pdf

CHALA, Y. (2019). Trabajo de postgrado (Importancia de la aplicación del mecanismo de cifrado de Información en las empresas para la prevención de riesgos Como ataques, plagio y pérdida de la confidencialidad). Universidad Nacional Abierta y a Distancia. {en -línea}. {Consultado marzo 14 de 2020}. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/30745/1/yfchala..pdf

CODIS CORRECTORS D'ERRORS I CRIPTOGRAFIA POSTQUÀNTICA. (2019). {en línea}. {Consultado 8 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.8CE1543F&lang=es&site=eds-live&scope=site

CONTRERAS, Javier & MAYOL, Reinaldo. (2016). Variacion De Parametros De Criptografia Con Curvas Elipticas Usados en La Firma Digital De Datos Sobre Una Red De Sensores Inalambricos. {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.F21CCCDD&lang=es&site=eds-live&scope=site

DAVIES, Joshua (2011). Implementing SSL/TLS Using Cryptography and PKI. Hoboken, N.J. Wiley. {en línea}. {Consultado 28 julio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=354757&lang=es&site=ehost-live

DE LA FUENTE, Elma. (2015). Tesis de pregrado (Estudio de la eficiencia de protocolos y algoritmos de Seguridad en Android). Universidad Carlos III de Madrid Escuela Politécnica Superior. {en línea}. {Consultado marzo 13 de 2019}. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/25278/PFC_Elma_Fuente_Barrios.pdf

DE SOUZA ABREU, Jacqueline. Past, present, and future of strong encryption: Technological development and regulation. Revista Brasileira de Politicas Publicas, 7(3), 25–42. {en línea}. {Consultado 11 de marzo de 2019}. Disponible en: https://doi-org.bibliotecavirtual.unad.edu.co/10.5102/rbpp.v7i3.4869

DI MARE HERING, Adolfo, & NOGUERA, Jose. (2014). Uso de la criptografía simétrica para la comunicación de mensajes cortos en dispositivos móviles. {en

línea}. {Consultado 10 septiembre de 2019}. Retrieved from http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.48C5A9C&lang=es&site=eds-live&scope=site

DÍAZ, Gabriel, MUR, Francisco, & SANCRISTÓBAL, Elio. (2004). Seguridad en las comunicaciones y en la información. España UNED - Universidad Nacional de Educación a Distancia. {en línea}. {Consultado 15 febrero de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10560101&tm=1465508562939

DOMINGUEZ, Hernán, MAYA, Edgar. & PELUFO, Diego. (2016). Aplicación de Técnicas de Fuerza Bruta con Diccionario de Datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación. {en línea}. {Consultado 25 octubre de 2019}. Disponible en: https://www.researchgate.net/publication/311922037_Aplicacion_de_Tecnicas_de_Fuerza_Bruta_con_Diccionario_de_Datos_para_vulnerar_servicios_con_metodos_de_autenticacion_simple_Contrasenas_pruebas_de_concepto_con_software_libre_y_su_remediacion

ESCRIVÁ, Gema, ROMERO, Rosa & RAMADA, David (2013). Seguridad informática. España: Macmillan Iberia, S.A. {en línea}. {Consultado 28 de abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=2&docID=10820963&tm=1466006456772

FERNÁNDEZ, Pallarés & ROCA, Martínez. (2018). Criptografía simétrica avanzada: diseño y análisis de eficiencia en mejoras avanzadas del estándar de cifrado simétrico DES. {en línea}. {Consultado 19 septiembre de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.2EF0CFBD&lang=es&site=eds-live&scope=site

FILHO, Jose & AZEREDO, Paula (2017). Tecnologia, criptografia e matemática: da troca de mensagens ao suporte em transações econômicas. {en línea}. {Consultado 24 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.4867B66C&lang=es&site=eds-live&scope=site

FOSTER, James. (2005). Buffer Overflow Attacks Detect, Exploit, Prevent. Rockland, MA Syngress. . {en línea}. {Consultado 1 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=126911&lang=es&site=ehost-live

GALENDE, Juan. (2018). Carlos Taranilla de la Varga, 'Criptografía. Los lenguajes secretos a lo largo de la Historia', Córdoba, Guadalmazán, 2018, 297 pp. ISBN: 978-84-94608-59-9. {en línea}. {Consultado 4 mayo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.74384FF9&lang=es&site=eds-live&scope=site

GALLEGO, Ignacio. (2016). Estructuras algebraicas aplicables en criptografía. {en línea}. {Consultado 12 abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.3D1D13FB&lang=es&site=eds-live&scope=site

GÁLVEZ, Heber. (2014). Análisis de algoritmos criptográficos en una red híbrida P2P. Universidad del Bío-Bío. Concepción, Chile. {en línea}. {Consultado 15 de abril de 2019}. Disponible en: http://repobib.ubiobio.cl/jspui/bitstream/123456789/1460/1/Galvez_Ojeda_Heber_Dario.pdf

GÁLVEZ, Nancy. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles. México D.F. {en línea}. {Consultado 10 junio de 2019}. Disponible en: http://148.204.210.201/tesis/1404316762511NPGMTesisAn.pdf

GARCÍA, Roberto. (2009). Criptografía clásica y moderna. España: Septem Ediciones. {en línea}. {Consultado 18 de febrero de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10317082&tm=1465508388792

GARCIA, Alicia. El cifrado RC4. Universidad de Salamanca. {en línea}. {Consultado 1 agosto de 2019}. Disponible en: http://rufian.eu/Cifrado_RC4/

GOMEZ, Álvaro. (2014). Seguridad en equipos informáticos. España: RA-MA Editorial. {en línea}. {Consultado 29 de marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=13&docID=11046412&tm=1466006343174

GOMEZ, Álvaro. (2007). Enciclopedia de la Seguridad Informática. Bogotá, Colombia: Alfaomega. {en línea}. {Consultado 4 junio de 2019}. Disponible en: https://books.google.com.pe/books/about/Enciclopedia_de_la_seguridad_inform%C3%A1tic.html?id=MQ_kOgAACAAJ&redir_esc=y

GONZALEZ, Lorena, & FUENTES, José. (2014). Sistemas seguros de acceso y transmisión de datos (MF0489_3). Madrid, ESPAÑA IC Editorial. {en línea}. {Consultado 3 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=11126449&tm=1465508507275

GONZALEZ, Ana & GONZALES, María (2018). “Crypto Go”: criptografía simétrica en tapete verde. {en línea}. {Consultado 2 abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C7FA086A&lang=es&site=eds-live&scope=site

GONZALEZ, Ana & MARTÍN, Pablo. (2018). Criptografía en el mundo real para futuros ingenieros informáticos UC3M : respuesta coral a la pregunta “¿en serio es importante la criptografía en la vida real de un ingeniero informático?”. {en línea}. {Consultado 2 abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.A1B41FF2&lang=es&site=eds-live&scope=site

HERNANDEZ, E. L. (2016). La criptografía. {en línea} {Consultado 3 marzo de 2020}. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co

HERRERA, Edward. (2014). Principios fundamentales que se busca proteger con la seguridad informática - CIA. {en línea}. {Consultado 10 octubre de 2019}. Disponible en: https://informaticaseguraupc.wordpress.Com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/

LEY 527 de 1999. {en línea}. {Consultado 1 mayo de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

LITWAK, Noelia & ESCALANTE, Jaquelina. (2004). Seguridad Informática y criptografía. (trabajo de pregrado). Universidad Nacional de Nordeste, Argentina. {en línea}. {Consultado 1 octubre de 2019}. Disponible en: http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf

LONG, Johnny. (2008). Google Hacking for Penetration Testers. Burlington, MA: Syngress. {en línea}. {Consultado 30 mayo de 2019}. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=230833&lang=es&site=ehost-live

LOVOS, Francisco. Seguridad física y lógica en los centros de cómputo. {en línea}. {Consultado 17 junio de 2019}. Disponible en:

https://webcache.googleusercontent.com/search?q=cache:ogqe1OyomHEJ:https://lovosfrancisco.jimdo.com/app/download/9167889769/SEGURIDAD%2BFISICA%2BY%2BLOGICA.pdf%3Ft%3D1504554721+&cd=17&hl=es-419&ct=clnk&gl=co

LUCENA, Manuel. (2014) Criptografía y Seguridad en Computadores. {en línea}. {Consultado 9 abril de 2019}. Disponible en: http://sertel.upc.edu/tdatos/Libros/Lucena.pdf

LUMBIARRES, Rubén; LÓPEZ, Mariano & CANTO, Enrique. (2013). Ataques por canal lateral sobre el algoritmo de encriptación AES implementado en MicroBlaze. {en línea}. {Consultado 19 octubre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.C3E6C7DD&lang=es&site=eds-live&scope=site

MADARRO, Evaristo; JUSTIZ, Oristela; LEGON, Carlos & SOSA Guillermo. (2017). Debilidad SAC en el algoritmo de cifrado en flujo RC4. {en línea}. {Consultado 4 octubre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.7596E211&lang=es&site=eds-live&scope=site

MARRERO, Yran. (2003). La Criptografía como elemento de la seguridad informática. {en línea}. {Consultado 17 junio de 2019}. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

MARTÍNEZ, Francisco. (2016). Criptosistemas de cifrado en flujo basados en matrices triangulares con múltiples bloques. {en línea}. {Consultado 20 de abril de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.58178TES&lang=es&site=eds-live&scope=site

MCCLURE, Stuart; SCAMBRAY, Joel, & KURTZ, George. (2010). Hackers 6 secretos y soluciones de seguridad en redes. México McGraw-Hill Interamericana. {en línea}. {Consultado 23 octubre de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10433876&tm=1465509236690

MEDINA, Yuri & MIRANDA, Haider. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. Revista MundoFesc,. {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55

MARÍ, Noelia. (2018). Una propuesta híbrida para el criptoanálisis RSA. {en línea}. {Consultado 6 mayo de 2019}. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.C6EE8D1&lang=es&site=eds-live&scope=site

MIERES, Jorge. (2009). Ataques Informáticos (Debilidades de seguridad comúnmente explotadas). {en línea}. {Consultado 13 octubre de 2019}. https://www.evilfingers.com/publications/ white_AR/01_Ataques_informaticos.pdf

MINTIC. (2017). Mintic. Decreto 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. {en línea}. {Consultado 30 abril de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-3705.html

MINTIC. (2001). Mintic. Decreto 1377 de 2001: Por medio de la cual se reglamenta parcialmente la ley 1581 de 2012 Ley de Protección de datos. {en línea}. {Consultado 30 abril de 2019}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-4274.html

MINTIC. (1999). Mintic. Ley 527 de 1999: CONPES 3701 de 2011 Lineamientos de política para la Ciberseguridad y Ciberdefensa. {en línea}. {Consultado 30 abril de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-3510.html

MOLINA, José. (2000). Seguridad de la información. Criptología. Argentina El Cid Editor. {en línea}. {Consultado 4 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=12&docID=10018530&tm=1465508601401

MONTAÑO, Juan. (2015). Tesis de postgrado (Algoritmos de encriptación: análisis del problema de la factorización prima en el método RSA de clave pública, algoritmo de shor). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 13 abril de 2020}. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3609/1/731924 26.pdf

MORALES, Aaron. (2012). Estadística y probabilidades. Chile. {en línea}. {Consultado 10 mayo de 2019}. Disponible en: http://www.x.edu.uy/inet/EstadisticayProbabilidad.pdf

MUÑOZ, Alfonso. (2004). CRIPTOSISTEMA RIJNDAEL. A FONDO, Algoritmo Criptografico Rijndael. {en línea}. {Consultado 20 agosto de 2019}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m480a.htm

NARVÁEZ, Roberto. (2018). Cryptography in the history of paranormal research. A few notable cases ; La criptografía en la historia de la investigación paranormal. Algunos casos notables. {en línea}. {Consultado 18 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.asp

x?direct=true&db=edsbas&AN=edsbas.A2708884&lang=es&site=eds-live&scope=site

NEVEN, Gregory & JOYE, Marc. (2009). Identity-based Cryptography. Amsterdam, Netherlands IOS Press. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=269152&lang=es&site=ehost-live

OXMAN, Nicolás. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. Universidad Santo Tomás, Santiago de Chile. Recuperado de: https://www.redalyc.org/pdf/1736/173629692007.pdf

PRIYADARSHINI, Patil; PARSHANT, Narayankar; NARAYAN, D.K.; MEENA, S. (2016). Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish. {en línea}. {Consultado 14 abril de 2019}. Disponible en http://www.sciencedirect.com/science/article/pii/S1877050916 001101

POUSA, Adrián. (2011). Algoritmo de cifrado simétrico AES. Aceleración de tiempo de cómputo sobre arquitecturas multicore. Universidad Nacional de la Plata. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/4210/Documento_completo.pdf?sequence=1&isAllowed=y

PRESIDENCIA DE LA REPÚBLICA. LEY 1928 DE 24 DE JULIO DE 2018: por la cual se aprueba el convenio de la ciberdelincuencia, adoptado del 23 de noviembre de 2001, en Budapest. Convenio de la ciberseguridad. {en línea}. {5 febrero de 2019}. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

PRIETO, Diego. (2014). Seguridad en redes inalámbricas: el protocolo WEP. (tesis de pregrado). Universidad de Cantabria. {en línea}. {Consultado 10 noviembre de 2019}. Disponible en: https://repositorio.unican.es/xmlui/bitstream/handle/10902/5944/Diego%20Garcia%20Prieto01.pdf?sequence=5&isAllowed=y

PROAÑO, Juan. (2018). Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas. {en línea}. {Consultado 30 marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.ECAF7F1D&lang=es&site=eds-live&scope=site

QUINTERO, Juan. (2016). OVI Unidad 1 - Criptografía. Bogotá, Colombia UNAD - Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 4 junio de 2019}. Disponible en: http://stadium.unad.edu.co/ovas/10596_10131/index.html

RIBEIRO, Vinicius, & WEBER, Raúl. (2012). Esquemas de criptografia de chave pública: elementos comuns e diferenciais. {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.48F2BE04&lang=es&site=eds-live&scope=site

RIBEIRO, Vinicius. (2012). Um Estudo Comparativo entre algoritmos de criptografia DES – Lucifer (1977) e AES – Rijndael (2000). {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.5323FC16&lang=es&site=eds-live&scope=site

RODRÍGUEZ, María. (2014). Implementación del algoritmo de cifrado AES mediante GPUS de Bajo Coste. {en línea}. {Consultado 25 julio de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.2540769C&lang=es&site=eds-live&scope=site

SAMANIEGO, Ana. (2018). “Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información”. Universidad Ricardo Palma. Lima, Perú. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://repositorio.urp.edu.pe/bitstream/handle/URP/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

SAMPEDRO, Carlos; MACHUCA, Silvio; PALMA, Diego & CARRERA, Frankz. (2019). Percepción De Seguridad De La Información en Las pequeñas y medianas empresas en santo domingo. Investigación Operacional, {en línea}. {Consultado 25 febrero de 2019}. Retrieved from http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=zbh&AN=136929577&lang=es&site=eds-live&scope=site

SAHU, Harish., JADHAV, Vikas., SONAVANE, Shefali, & SHARMA, R.K. (2016). Cryptanalytic Attacks on International Data Encryption Algorithm Block Cipher. Defence Science Journal. {en línea}. {Consultado 1 noviembre de 2019}. https://doi-org.bibliotecavirtual.unad.edu.co/10.14429/dsj.66.10798

SANCHEZ, Héctor; RODRIGUEZ, Carlos & NOTARIO, Alejandro. Critografía y métodos de cifrado. {en línea}. {Consultado 25 de abril de 2019}. Disponible en:

http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

SERRATO, H. (2019). Trabajo de postgrado (Comparación de Métodos Criptográficos para la Seguridad Informática). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 12 abril de 2020}. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

SOBREVILLA, Pedro. (2016). SEGURIDAD Y EFICIENCIA DE ALGUNAS VARIANTES DEL CRIPTOSISTEMA IDEA. (tesis de postgrado). Universidad Autónoma Metropolitana Iztapalapa. {en línea}. {Consultado 1 noviembre de 2019}. Disponible en: http://mat.izt.uam.mx/mcmai/documentos/tesis/Gen.12-O/Pedro_Sobrevilla.pdf

TARAZONA, Cesar. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas, {en línea}. {Consultado 6 mayo de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3311853ART&lang=es&site=eds-live&scope=site

TRINIDAD, G. (2007). Esquema de Cifrado y Compresión sin Pérdida para datos de ECG en Telemedicina. (Tesis de postgrado) Inade. {en línea}. {Consultado 30 agosto de 2019}. Disponible en: https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/667/1/TrinidadBGJ.pdf

VARGAS, Julio. (2019). OVI Unidad 2 - Criptografía. Bogotá, Colombia UNAD - Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 6 mayo de 2019}. Disponible en: http://hdl.handle.net/10596/23682

VARGAS, Juan. (2019). ANÁLISIS DE EFICACIA Y EFICIENCIA PARA UN MÉTODO DE CIBERSEGURIDAD PARA EL PROTOCOLO DE COMUNICACIÓN ACARS EN AERONAVES COMERCIALES LEGADO. (Tesis de postgrado). Querétaro. (Tesis de postgrado). {en línea}. {Consultado 7 mayo de 2019}. Disponible en: https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/346/1/VargasSalvadorJuanP%20MSIM%202019.pdf

ANEXOS

Anexo A FORMATO RAE

Fecha de Realización: 12/12/2019
Título: ESTUDIO DE EFICIENCIA Y EFICACIA DE LOS ALGORITMOS CRIPTOGRÁFICOS RSA, AES, IDEA y RC4 EN LA SEGURIDAD INFORMÁTICA
Autor: ALVARADO PRADO, Edisson Esteban
Palabras Claves: algoritmo criptográfico, AES, IDEA, RC4, RSA, seguridad informática, seguridad de la información, amenazas informáticas.
Descripción: Esta monografía muestra un estudio realizado a los algoritmos RSA, AES, IDEA y RC4, con el fin de determinar cuál de ellos ofrece mejores características de seguridad de la información. El trabajo se divide en tres capítulos, que relaciona los tres objetivos específicos de la monografía, parte mostrando características generales y específicas de cada algoritmo, identificando óptimo uso de recursos y tiempos de ejecución y los beneficios frente a amenazas informáticas más representativas en cada uno.
Fuentes: AGUIRRE, Jorge. (2018). Curso de criptografía aplicada. Madrid. {en línea}. {consultado 18 marzo de 2019}. : Disponible en: http://www.criptored.upm.es/descarga/CursoCriptografiaAplicada2018.pdf ALMASRI, Osama & MAT, Hajar. (2013). Introducing an Encryption Algorithm based on IDEA. Universiti Tenaga Nasional. {en línea}. {16 de abril de 2019}. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.679.7495&rep=rep1&type=pdf ÁLVAREZ, Gonzalo & PÉREZ, Pedro. (2004). Seguridad informática para empresas y particulares. España: McGraw-Hill España. {en línea}. {Consultado 20 febrero de marzo de 2019} Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10498593&tm=1466006497840 ALZATE, Alonso & DUQUE, Néstor. Criptografía una excelente alternativa de seguridad. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://bdigital.unal.edu.co/58103/1/criptografia.pdf ANGEL, Jose. (2005). Advanced Encryption Standard. México. {en línea}. {Consultado 30 octubre de 2019}. Disponible en: www.criptored.upm.es/guiateoria/gt_m117i.htm

ARROYO, Cilene. (2019). Implantación de un esquema de seguridad informática. {en línea}. {Consultado 28 febrero de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BBED0E78&lang=es&site=eds-live&scope=site

BALBAS, David. (2019). Ataques al criptosistema RSA. (trabajo pregrado). {en línea}. {30 septiembre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.33D0FB00&lang=es&site=eds-live&scope=site

BELTRAN, Julian. (2015). Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. {en línea}. {consultado 3 noviembre de 2019}. Disponible en: https://riunet. upv.es/bitstream/handle/025/5602/Memoria.pdf?sequence=1

BHARATI, B & MANIVASAGAM, G & KUMAR, M. (2017). Metrics for performance evaluation of encryption algorithms. International journal of advance research in science and engineering. {en línea}. {Consultado 19 septiembre de 2019}. Disponible en: https://pdfs.semanticscholar.org/32af/f95d61af85e45970c5051d3be79e66163fdc.pdf

BOLAÑOS, Fredy; NIETO, Rubén & BERNAL, Álvaro. (2004). Implementación de un Hardware Reconfigurable de los Bloques de un Sistema RSA. Ingeniería y Competitividad, 6(2), 25–34. {en línea}. {Consultado 15 de abril de 2019}. Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=zbh&AN=20417528&lang=es&site=eds-live&scope=site

BORST, Johan. (1996). Differential-linear cryptanalysis of IDEA. ESAT– COSIC Technical Report. {en línea}. {Consultado 10 noviembre de 2019}. Disponible en: https://pdfs.semanticscholar.org/ff93/5085644465a127d73995b747cb45e416a143.pdf?_ga=2.12800759.1533181467.1574699588-190295632.1573436562

BURNETT, M., & KLEIMAN, D. (2006). Perfect Passwords Selection, Protection, Authentication. Rockland, Mass: Syngress. {en línea}. {Consultado 15 septiembre de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=149590&lang=es&site=ehost-live

CABRERA, Claudio. ALGORITMOS DE ENCRIPTACIÓN, DESENCRIPTACIÓN - EVALUACIÓN Y VERIFICACIÓN. Universidad Técnica del Norte.{en línea}. {Consultado 20 septiembre de 2019}. Disponible en:

https://docplayer.es/7972090-Algoritmos-de-encriptacion-desencriptacion-evaluacion-y-verificacion.html

CANAVELLI, Juan & AÑINO, María. (2012). Educación en Tecnología y Matemática en Criptografía. {en línea}. {Consultado 7 marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.6CA460F&lang=es&site=eds-live&scope=site

CAÑIHUA, Ruben (2007). Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de tercera generación/Ipv6. Chile Universidad de Chile. {en línea}. {Consultado 27 de marzo} Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10198466&tm=1465508433109

CAPUÑAY, Denys; GUERRERO, Ana & VILLEGAS, Juan. (2016). Análisis Comparativo de Algoritmos Criptográficos. Revista Internacional de TECNOLOGÍA DIGITAL Y ECONOMÍA. {en línea}. {Consultado 4 octubre de 2019}. Disponible en: http://revistas.uss.edu.pe/index.php/ING/article/view/440

CASTILLO, Marco; SANTANA, Nancy; DÍAZ, Alicia; ALMANZA, Germán & CASTILLO, Felipe. (2011). Teoría de números en criptografía y su debilidad ante la posible era de las computadoras cuánticas. Universidad Autónoma del Estado de México. Toluca, México. {en línea}. {Consultado 1 noviembre de 2019}. Disponible en: https://www.redalyc.org/pdf/104/10420073007.pdf

CHALA, Y. (2019). Trabajo de postgrado (Importancia de la aplicación del mecanismo de cifrado de Información en las empresas para la prevención de riesgos Como ataques, plagio y pérdida de la confidencialidad). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado marzo 14 de 2020}. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/30745/1/yfchala..pdf

CODIS CORRECTORS D'ERRORS I CRIPTOGRAFIA POSTQUÀNTICA. (2019). {en línea}. {Consultado 8 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.8CE1543F&lang=es&site=eds-live&scope=site

CONTRERAS, Javier & MAYOL, Reinaldo. (2016). Variacion De Parametros De Criptografia Con Curvas Elipticas Usados en La Firma Digital De Datos Sobre Una Red De Sensores Inalambricos. {en línea}. {Consultado 15 junio de 2019}.

Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.F21CCCDD&lang=es&site=eds-live&scope=site

DAVIES, Joshua (2011). Implementing SSL/TLS Using Cryptography and PKI. Hoboken, N.J. Wiley. {en línea}. {Consultado 28 julio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=354757&lang=es&site=ehost-live

DE LA FUENTE, Elma. (2015). Tesis de pregrado (Estudio de la eficiencia de protocolos y algoritmos de Seguridad en Android). Universidad Carlos III de Madrid Escuela Politécnica Superior. {en línea}. {Consultado marzo 13 de 2019}. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/25278/PFC_Elma_Fuente_Barrios.pdf

DE SOUZA ABREU, Jacqueline. Past, present, and future of strong encryption: Technological development and regulation. Revista Brasileira de Politicas Publicas, 7(3), 25–42. {en línea}. {Consultado 11 de marzo de 2019}. Disponible en: https://doi-org.bibliotecavirtual.unad.edu.co/10.5102/rbpp.v7i3.4869

DI MARE HERING, Adolfo, & NOGUERA, Jose. (2014). Uso de la criptografía simétrica para la comunicación de mensajes cortos en dispositivos móviles. {en línea}. {Consultado 10 septiembre de 2019}. Retrieved from http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.48C5A9C&lang=es&site=eds-live&scope=site

DÍAZ, Gabriel, MUR, Francisco, & SANCRISTÓBAL, Elio. (2004). Seguridad en las comunicaciones y en la información. España UNED - Universidad Nacional de Educación a Distancia. {en línea}. {Consultado 15 febrero de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10560101&tm=1465508562939

DOMINGUEZ, Hernán, MAYA, Edgar. & PELUFO, Diego. (2016). Aplicación de Técnicas de Fuerza Bruta con Diccionario de Datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación. {en línea}. {Consultado 25 octubre de 2019}. Disponible en: https://www.researchgate.net/publication/311922037_Aplicacion_de_Tecnicas_de_Fuerza_Bruta_con_Diccionario_de_Datos_para_vulnerar_servicios_con_metodos_de_autenticacion_simple_Contrasenas_pruebas_de_concepto_con_software_libre_y_su_remediacion

ESCRIVÁ, Gema, ROMERO, Rosa & RAMADA, David (2013). Seguridad informática. España: Macmillan Iberia, S.A. {en línea}. {Consultado 28 de abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=2&docID=10820963&tm=1466006456772

FERNÁNDEZ, Pallarés & ROCA, Martínez. (2018). Criptografía simétrica avanzada: diseño y análisis de eficiencia en mejoras avanzadas del estándar de cifrado simétrico DES. {en línea}. {Consultado 19 septiembre de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.2EF0CFBD&lang=es&site=eds-live&scope=site

FILHO, Jose & AZEREDO, Paula (2017). Tecnologia, criptografia e matemática: da troca de mensagens ao suporte em transações econômicas. {en línea}. {Consultado 24 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.4867B66C&lang=es&site=eds-live&scope=site

FOSTER, James. (2005). Buffer Overflow Attacks Detect, Exploit, Prevent. Rockland, MA Syngress. . {en línea}. {Consultado 1 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=126911&lang=es&site=ehost-live

GALENDE, Juan. (2018). Carlos Taranilla de la Varga, 'Criptografía. Los lenguajes secretos a lo largo de la Historia', Córdoba, Guadalmazán, 2018, 297 pp. ISBN: 978-84-94608-59-9. {en línea}. {Consultado 4 mayo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.74384FF9&lang=es&site=eds-live&scope=site

GALLEGO, Ignacio. (2016). Estructuras algebraicas aplicables en criptografía. {en línea}. {Consultado 12 abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.3D1D13FB&lang=es&site=eds-live&scope=site

GÁLVEZ, Heber. (2014). Análisis de algoritmos criptográficos en una red híbrida P2P. Universidad del Bío-Bío. Concepción, Chile. {en línea}. {Consultado 15 de

abril de 2019}. Disponible en: http://repobib.ubiobio.cl/jspui/bitstream/123456789/1460/1/Galvez_Ojeda_Heber_Dario.pdf

GÁLVEZ, Nancy. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles. México D.F. {en línea}. {Consultado 10 junio de 2019}. Disponible en: http://148.204.210.201/tesis/1404316762511NPGMTesisAn.pdf

GARCÍA, Roberto. (2009). Criptografía clásica y moderna. España: Septem Ediciones. {en línea}. {Consultado 18 de febrero de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10317082&tm=1465508388792

GARCIA, Alicia. El cifrado RC4. Universidad de Salamanca. {en línea}. {Consultado 1 agosto de 2019}. Disponible en: http://rufian.eu/Cifrado_RC4/

GOMEZ, Álvaro. (2014). Seguridad en equipos informáticos. España: RA-MA Editorial. {en línea}. {Consultado 29 de marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=13&docID=11046412&tm=1466006343174

GOMEZ, Álvaro. (2007). Enciclopedia de la Seguridad Informática. Bogotá, Colombia: Alfaomega. {en línea}. {Consultado 4 junio de 2019}. Disponible en: https://books.google.com.pe/books/about/Enciclopedia_de_la_seguridad_inform%C3%A1tic.html?id=MQ_kOgAACAAJ&redir_esc=y

GONZALEZ, Lorena, & FUENTES, José. (2014). Sistemas seguros de acceso y transmisión de datos (MF0489_3). Madrid, ESPAÑA IC Editorial. {en línea}. {Consultado 3 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=11126449&tm=1465508507275

GONZALEZ, Ana & GONZALES, María (2018). “Crypto Go”: criptografía simétrica en tapete verde. {en línea}. {Consultado 2 abril de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C7FA086A&lang=es&site=eds-live&scope=site

GONZALEZ, Ana & MARTÍN, Pablo. (2018). Criptografía en el mundo real para futuros ingenieros informáticos UC3M : respuesta coral a la pregunta “¿en serio es importante la criptografía en la vida real de un ingeniero informático?”. {en línea}. {Consultado 2 abril de 2019}. Disponible en:

http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.A1B41FF2&lang=es&site=eds-live&scope=site

HERNANDEZ, E. L. (2016). La criptografía. {en línea} {Consultado 3 marzo de 2020}. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co

HERRERA, Edward. (2014). Principios fundamentales que se busca proteger con la seguridad informática - CIA. {en línea}. {Consultado 10 octubre de 2019}. Disponible en: https://informaticaseguraupc.wordpress.Com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/

LEY 527 de 1999. {en línea}. {Consultado 1 mayo de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

LITWAK, Noelia & ESCALANTE, Jaquelina. (2004). Seguridad Informática y criptografía. (trabajo de pregrado). Universidad Nacional de Nordeste, Argentina. {en línea}. {Consultado 1 octubre de 2019}. Disponible en: http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf

LONG, Johnny. (2008). Google Hacking for Penetration Testers. Burlington, MA: Syngress. {en línea}. {Consultado 30 mayo de 2019}. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=230833&lang=es&site=ehost-live

LOVOS, Francisco. Seguridad física y lógica en los centros de cómputo. {en línea}. {Consultado 17 junio de 2019}. Disponible en: https://webcache.googleusercontent.com/search?q=cache:ogqe1OyomHEJ:https://lovosfrancisco.jimdo.com/app/download/9167889769/SEGURIDAD%2BFISICA%2BY%2BLOGICA.pdf%3Ft%3D1504554721+&cd=17&hl=es-419&ct=clnk&gl=co

LUCENA, Manuel. (2014) Criptografía y Seguridad en Computadores. {en línea}. {Consultado 9 abril de 2019}. Disponible en: http://sertel.upc.edu/tdatos/Libros/Lucena.pdf

LUMBIARRES, Rubén; LÓPEZ, Mariano & CANTO, Enrique. (2013). Ataques por canal lateral sobre el algoritmo de encriptación AES implementado en MicroBlaze. {en línea}. {Consultado 19 octubre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.C3E6C7DD&lang=es&site=eds-live&scope=site

MADARRO, Evaristo; JUSTIZ, Oristela; LEGON, Carlos & SOSA Guillermo. (2017). Debilidad SAC en el algoritmo de cifrado en flujo RC4. {en línea}. {Consultado 4 octubre de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.7596E211&lang=es&site=eds-live&scope=site

MARRERO, Yran. (2003). La Criptografía como elemento de la seguridad informática. {en línea}. {Consultado 17 junio de 2019}. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

MARTÍNEZ, Francisco. (2016). Criptosistemas de cifrado en flujo basados en matrices triangulares con múltiples bloques. {en línea}. {Consultado 20 de abril de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.58178TES&lang=es&site=eds-live&scope=site

MCCLURE, Stuart; SCAMBRAY, Joel, & KURTZ, George. (2010). Hackers 6 secretos y soluciones de seguridad en redes. México McGraw-Hill Interamericana. {en línea}. {Consultado 23 octubre de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10433876&tm=1465509236690

MEDINA, Yuri & MIRANDA, Haider. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. Revista MundoFesc,. {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55

MARÍ, Noelia. (2018). Una propuesta híbrida para el criptoanálisis RSA. {en línea}. {Consultado 6 mayo de 2019}. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.C6EE8D1&lang=es&site=eds-live&scope=site

MIERES, Jorge. (2009). Ataques Informáticos (Debilidades de seguridad comúnmente explotadas). {en línea}. {Consultado 13 octubre de 2019}. https://www.evilfingers.com/publications/ white_AR/01_Ataques_informaticos.pdf

MINTIC. (2017). Mintic. Decreto 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. {en línea}. {Consultado 30 abril de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-3705.html

MINTIC. (2001). Mintic. Decreto 1377 de 2001: Por medio de la cual se reglamenta parcialmente la ley 1581 de 2012 Ley de Protección de datos. {en línea}. {Consultado 30 abril de 2019}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-4274.html

MINTIC. (1999). Mintic. Ley 527 de 1999: CONPES 3701 de 2011 Lineamientos de política para la Ciberseguridad y Ciberdefensa. {en línea}. {Consultado 30 abril de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/w3-article-3510.html

MOLINA, José. (2000). Seguridad de la información. Criptología. Argentina El Cid Editor. {en línea}. {Consultado 4 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=12&docID=10018530&tm=1465508601401

MORALES, Aaron. (2012). Estadística y probabilidades. Chile. {en línea}. {Consultado 10 mayo de 2019}. Disponible en: http://www.x.edu.uy/inet/EstadisticayProbabilidad.pdf

MONTAÑO, Juan. (2015). Tesis de postgrado (Algoritmos de encriptación: análisis del problema de la factorización prima en el método RSA de clave pública, algoritmo de shor). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 13 abril de 2020}. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3609/1/73192426.pdf

MUÑOZ, Alfonso. (2004). CRIPTOSISTEMA RIJNDAEL. A FONDO, Algoritmo Criptografico Rijndael. {en línea}. {Consultado 20 agosto de 2019}. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m480a.htm

NARVÁEZ, Roberto. (2018). Cryptography in the history of paranormal research. A few notable cases ; La criptografía en la historia de la investigación paranormal. Algunos casos notables. {en línea}. {Consultado 18 agosto de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.A2708884&lang=es&site=eds-live&scope=site

NEVEN, Gregory & JOYE, Marc. (2009). Identity-based Cryptography. Amsterdam, Netherlands IOS Press. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=269152&lang=es&site=ehost-live

OXMAN, Nicolás. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. Universidad Santo Tomás, Santiago de Chile. Recuperado de: https://www.redalyc.org/pdf/1736/173629692007.pdf

PRIYADARSHINI, Patil; PARSHANT, Narayankar; NARAYAN, D.K.; MEENA, S. (2016). Evaluación completa de algoritmos criptográficos: DES, 3DES, AES, RSA and Blowfish. {en línea}. {Consultado 14 abril de 2019}. Disponible en http://www.sciencedirect.com/science/article/pii/S1877050916 001101

POUSA, Adrián. (2011). Algoritmo de cifrado simétrico AES. Aceleración de tiempo de cómputo sobre arquitecturas multicore. Universidad Nacional de la Plata. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/4210/Documento_completo.pdf?sequence=1&isAllowed=y

PRESIDENCIA DE LA REPÚBLICA. LEY 1928 DE 24 DE JULIO DE 2018: por la cual se aprueba el convenio de la ciberdelincuencia, adoptado del 23 de noviembre de 2001, en Budapest. Convenio de la ciberseguridad. {en línea}. {5 febrero de 2019}. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

PRIETO, Diego. (2014). Seguridad en redes inalámbricas: el protocolo WEP. (tesis de pregrado). Universidad de Cantabria. {en línea}. {Consultado 10 noviembre de 2019}. Disponible en: https://repositorio.unican.es/xmlui/bitstream/handle/10902/5944/Diego%20Garcia%20Prieto01.pdf?sequence=5&isAllowed=y

PROAÑO, Juan. (2018). Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas. {en línea}. {Consultado 30 marzo de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.ECAF7F1D&lang=es&site=eds-live&scope=site

QUINTERO, Juan. (2016). OVI Unidad 1 - Criptografía. Bogotá, Colombia UNAD - Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 4 junio de 2019}. Disponible en: http://stadium.unad.edu.co/ovas/10596_10131/index.html

RIBEIRO, Vinicius, & WEBER, Raúl. (2012). Esquemas de criptografia de chave pública: elementos comuns e diferenciais. {en línea}. {Consultado 15 junio de 2019}. Disponible en:

http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.48F2BE04&lang=es&site=eds-live&scope=site

RIBEIRO, Vinicius. (2012). Um Estudo Comparativo entre algoritmos de criptografia DES – Lucifer (1977) e AES – Rijndael (2000). {en línea}. {Consultado 15 junio de 2019}. Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.5323FC16&lang=es&site=eds-live&scope=site

RODRÍGUEZ, María. (2014). Implementación del algoritmo de cifrado AES mediante GPUS de Bajo Coste. {en línea}. {Consultado 25 julio de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.2540769C&lang=es&site=eds-live&scope=site

SAMANIEGO, Ana. (2018). “Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información”. Universidad Ricardo Palma. Lima, Perú. {en línea}. {Consultado 20 junio de 2019}. Disponible en: http://repositorio.urp.edu.pe/bitstream/handle/URP/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

SAMPEDRO, Carlos; MACHUCA, Silvio; PALMA, Diego & CARRERA, Frankz. (2019). Percepción De Seguridad De La Información en Las pequeñas y medianas empresas en santo domingo. Investigación Operacional, {en línea}. {Consultado 25 febrero de 2019}. Retrieved from http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=zbh&AN=136929577&lang=es&site=eds-live&scope=site

SAHU, Harish., JADHAV, Vikas., SONAVANE, Shefali, & SHARMA, R.K. (2016). Cryptanalytic Attacks on International Data Encryption Algorithm Block Cipher. Defence Science Journal. {en línea}. {Consultado 1 noviembre de 2019}. https://doi-org.bibliotecavirtual.unad.edu.co/10.14429/dsj.66.10798

SANCHEZ, Héctor; RODRIGUEZ, Carlos & NOTARIO, Alejandro. Critografía y métodos de cifrado. {en línea}. {Consultado 25 de abril de 2019}. Disponible en: http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

SERRATO, H. (2019). Trabajo de postgrado (Comparación de Métodos Criptográficos para la Seguridad Informática). Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 12 abril de 2020}. Disponible en:

https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

SOBREVILLA, Pedro. (2016). SEGURIDAD Y EFICIENCIA DE ALGUNAS VARIANTES DEL CRIPTOSISTEMA IDEA. (tesis de postgrado). Universidad Autónoma Metropolitana Iztapalapa. {en línea}. {Consultado 1 noviembre de 2019}. Disponible en: http://mat.izt.uam.mx/mcmai/documentos/tesis/Gen.12-O/Pedro_Sobrevilla.pdf

TARAZONA, Cesar. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas, {en línea}. {Consultado 6 mayo de 2019}. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3311853ART&lang=es&site=eds-live&scope=site

TRINIDAD, G. (2007). Esquema de Cifrado y Compresión sin Pérdida para datos de ECG en Telemedicina. (Tesis de postgrado) Inade. {en línea}. {Consultado 30 agosto de 2019}. Disponible en: https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/667/1/TrinidadBGJ.pdf

VARGAS, Julio. (2019). OVI Unidad 2 - Criptografía. Bogotá, Colombia UNAD - Universidad Nacional Abierta y a Distancia. {en línea}. {Consultado 6 mayo de 2019}. Disponible en: http://hdl.handle.net/10596/23682

VARGAS, Juan. (2019). ANÁLISIS DE EFICACIA Y EFICIENCIA PARA UN MÉTODO DE CIBERSEGURIDAD PARA EL PROTOCOLO DE COMUNICACIÓN ACARS EN AERONAVES COMERCIALES LEGADO. (Tesis de postgrado). Querétaro. (Tesis de postgrado). {en línea}. {Consultado 7 mayo de 2019}. Disponible en: https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/346/1/VargasSalvadorJuanP%20MSIM%202019.pdf

Contenido del documento:

INTRODUCCIÓN
1. EL PROBLEMA DE INVESTIGACIÓN
1.1. DESCRIPCIÓN
1.2. FORMULACIÓN
1.3. OBJETIVOS
1.3.1. Objetivo general.
1.3.2. Objetivos específicos.
1.4. JUSTIFICACIÓN
1.5. DELIMITACIÓN

2. MARCO DE REFERENCIA
2.1. ANTECEDENTES
2.2. MARCO TEORICO
2.3. MARCO CONCEPTUAL
2.3.1. Criptografía.
2.3.2. Pilares de la Seguridad Informática.
2.3.3. Seguridad Informática.
2.3.4. Seguridad de la información.
2.3.5. Aritmética modular.
2.3.6. Algoritmo criptográfico.
2.3.7. Inverso multiplicativo modular.
2.3.8. Números primos.
2.3.9. Operadores Bits a Bits.
2.3.10. Amenaza a la información.
2.3.11. Algoritmo de Fermat.
2.3.12. Criptografía simétrica.
2.3.13. Cifrado asimetrico.
2.3.14. Eficiencia de un algoritmo criptográfico.
2.3.15. Eficacia de un algoritmo criptográfico.
2.3.16. Promedio.
2.3.17. Rendimiento de un algoritmo.
2.4. MARCO LEGAL
2.4.1. Ley 1273 de 2009.
2.4.2. Ley 1581 de 2012.
2.4.3. Ley 1928 de 2018.
2.4.4. Ley 527 de 1999.
3. RESULTADOS
3.1. CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
3.2. DESCRIPCIÓN DE LOS ALGORITMOS DE CIFRADO
3.2.1. RSA (Rivest, Shamir, Adleman).
3.2.2. AES (Advanced Encryption Standard).
3.2.3. IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM).
3.2.4. RC4 (RIVEST CIPHER 4).
3.3. CARACTERÍSTICAS DE LOS ALGORITMOS
3.4. EFICIENCIA DE LOS ALGORITMOS RSA, AES, IDEA Y RC4
3.4.1. Eficiencia RSA.
3.4.2. Eficiencia AES.
3.4.3. Eficiencia IDEA.
3.4.4. Eficiencia RC4.
3.5. COMPARACIÓN DE RENDIMIENTO DE LOS ALGORITMOS

3.6. ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS FRENTE A AMENAZAS INFORMÁTICAS
3.7. SEGURIDAD DE LOS ALGORITMOS CRIPTOGRÁFICOS
3.7.1. Seguridad de RSA.
3.7.2. Seguridad de AES.
3.7.3. Seguridad de IDEA.
3.7.4. Seguridad de RC4.
3.8. ATAQUES A LOS ALGORITMOS CRIPTOGRAFICOS
3.8.1. Ataques a RSA.
3.8.2. Ataques a AES.
3.8.3. Ataques a IDEA.
3.8.4. Ataques A RC4.
3.9. SÍNTESIS DEL ESTUDIO
4. CONCLUSIONES
RECOMENDACIONES
BIBLIOGRAFÍA
ANEXOS

Metodología:

Este trabajo se desarrolla en tres capítulos que relacionan los tres objetivos específicos a tratar y dan respuesta a la formulación del problema de esta monografía. Se basa en investigación de fuentes documentales y bibliográficas.

Conclusiones:

- En el séptimo capítulo de esta monografía correspondiente al primer objetivo, se mostró características de los algoritmos RSA, AES, IDEA y RC4, donde se evidencia que el algoritmo RSA cuenta con las mejores características para catalogarse como un buen sistema de cifrado, por manejar un tamaño de clave superior a los otros algoritmos (hasta 4096 bits) y el hecho de que una clave ocupe más espacio en disco, emplea más tiempo en descifrarla por medio de un ataque informático. A esto se agrega que el sistema maneja dos claves una pública conocida y otra privada que no puede ser compartida a cualquiera, lo que hace más difícil para un atacante tratar de obtenerla.

- En cuestiones de extensión, el sistema RC4 cuenta con un algoritmo corto y fácil de implementar, lo que implica que requiere un mínimo espacio de memoria. Sin embargo, por su poca memoria que ocupa la clave (40 bits), por ser única y fija, entre otras cosas más, no proporciona el nivel de seguridad deseado. Por ello, no es un buen candidato como sistema de cifrado.

- RSA consume más tiempo en el cifrado y descifrado, y consecuente a esto, es el sistema criptográfico que tiene menor rendimiento comparado con AES, IDEA y RC4.

- En el tema de seguridad, ya se dijo que RC4 proporciona un bajo nivel, contrario a este, RSA es el mejor candidato que presenta los mejores niveles, por he hecho de manejar una extensión de clave de hasta 4096 bits (como característica principal), de contar con un algoritmo complejo capaz de soportar múltiples ataques informáticos, sin éxito alguno. Los intentos de conseguir la llave privada, hace que el trabajo de un computador se haga intratable. Por ello, se considera el mejor sistema criptográfico respecto a AES, IDEA y RC4, aunque consecuentemente ocupa más tamaño en disco.

- El sistema de cifrado IDEA sería un buen candidato para cifrado, pero depende mucho de la clave que se use. Si se trata de una clave débil, un ataque de fuerza bruta podría conseguirla sin usar muchos recursos computacionales, frente a esto el mejor candidato sigue siendo RSA.

- Si se considera la variable tiempo de cifrado, respecto a tamaño en disco entonces el mejor candidato a elegir es el sistema AES, que maneja una clave máxima de 256 bits, es decir, como RSA el sistema AES soporta ataques de fuerza bruta, sobre todo cuando la clave es de 128 bits o 256 bits.

AUTOR: EDISSON ESTEBAN ALVARADO PRADO