ESTUDIO COMPARATIVO DE LA EFICIENCIA DE LOS ALGORITMOS SIMÉTRICO, ALGORITMO ASIMÉTRICO Y HASH FRENTE ATAQUES CIBERNÉTICOS

JUAN DAVID MOLINA GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MELGAR – TOLIMA 2023

ESTUDIO COMPARATIVO DE LA EFICIENCIA DE LOS ALGORITMOS SIMÉTRICO, ALGORITMO ASIMÉTRICO Y HASH FRENTE ATAQUES CIBERNÉTICOS

JUAN DAVID MOLINA GARCÍA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
Esp. Daniel Felipe Palomo Luna

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MELGAR – TOLIMA 2023

Nota de aceptación

_____
_____
_____
_____
_____
_____
____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Melgar – Tolima

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

RESUMEN

En la actualidad, la criptografía se ha convertido en una herramienta esencial para proteger documentos y datos. Su función principal consiste en ocultar la representación lingüística de mensajes o información, con el propósito de hacerla incomprensible para aquellos receptores que no estén autorizados a acceder a ella. A través de los resultados obtenidos en esta investigación, se pretende determinar cuáles son los métodos criptográficos más efectivos para salvar la información.

Esta monografía se enfocará en el estudio de diversos tipos de algoritmos criptográficos, incluyendo los algoritmos simétricos, asimétricos y HASH, con el objetivo de evaluar la eficiencia de cada uno de ellos.

Palabras clave: *Algoritmos, Criptografía, Informática, Seguridad*

ABSTRACT

Cryptography is an essential tool for protecting documents and data, it works mainly by hiding the Linguistic representation of messages or information in order to make them unintelligible to unauthorized recipients. With the results of the investigation we will be able to determine the best cryptographic methods to use in the use of social networks to protect the information. Some of the types of Cryptographic Algorithms that will be studied in this Monograph are Symmetric Algorithms, Asymmetric Algorithms and HASH, determining the efficiency of each of them against cyber-attacks on social networks.

Keywords: *Algorithms, Cryptography, Computing, Social networks, Security*

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El crecimiento tecnológico y el uso de las tecnologías de la información han ido incrementando el uso de las redes sociales, dándoles un valor inimaginable en todos los niveles empresariales y en las mismas personas; son herramientas que no solo elevan el valor productivo, sino que crean y facilitan lazos de comunicación más fuertes que ayudan a cumplir las metas organizacionales[1]. A la par con el crecimiento informático y el uso de las redes se han generado nuevas formas para acceder a esa información no permitida de manera ilegal con ataques maliciosos cibernéticos que infectan miles de equipos en un tiempo mínimo, un ejemplo de ellos fue el que se dio en el año 2017 afectando más de diez mil equipos la primera hora, casi doscientos treinta mil en un dia, en este, se vieron afectadas compañías muy reconocidas como Telefónica, FedEx, Renault, además de muchas instituciones universitarias, agencias gubernamentales e instituciones de salud[1]

[1] RÍOS, Lucas Giraldo. Ciberseguridad y redes sociales. *Revista de las Fuerzas Armadas*, 2021, no 257, p. 69-88.: https://esdegrevistas.edu.co/index.php/refa/article/view/417/648

1.2 FORMULACIÓN DEL PROBLEMA

En la época actual todas las empresas de mensajería, que manejan datos, correos y otros materiales deben contar con un sistema de encriptación que los proteja contra ciberataques y que genere confianza a clientes e inversores.

A partir de lo mencionado anteriormente, se puede orientar a los profesionales sobre la importancia de la criptografía, su proceso, estándar y los diversos tipos de algoritmo criptográfico. En la actualidad, toda empresa debe proteger rigurosamente los datos que almacena. En el caso de la aplicación de mensajería instantánea, como WhatsApp o Telegram, esta empresa utiliza un sistema de cifrado de extremo a extremo para evitar que personas no autorizadas puedan acceder al mensaje en su forma legible. En la era actual, todos estamos expuestos a posibles ataques cibernéticos. Si la empresa o entidad gubernamental que gestiona o almacena nuestra información no es diligente en la implementación de medidas de encriptación adecuada en caso de fuga de datos, podríamos enfrentar problemas personales.

A raíz de lo anterior, surge la siguiente pregunta: ¿Cuál es el algoritmo más efectivo para protegerse contra ataques cibernéticos?

2. JUSTIFICACIÓN

Lo que se presenta en el proyecto es conocer la eficiencia de los Algoritmos Simétricos, Algoritmos Asimétricos y HASH, definiendo sus características generales y específicas y determinar cuál es más eficiente a la hora de un ataque cibernético. Con ellos se busca orientar a aquellos el sistema criptográfico y les ayude a implementar el método o algoritmo adecuado para proteger la información.

El asegurar que la información sea confidencial es un tema que preocupa a toda organización que almacene información tanto interna, de sus aliados y de sus clientes, y más cuando dicha información se transfiere por medios inseguros (como el internet o almacenamientos extraíbles). Es importante para las organizaciones proteger la información ya que esta puede llegar a ser eliminada, manipulada o transferida por terceros no autorizados.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio sobre la eficiencia de los Algoritmos Asimétricos, Algoritmos Simétricos y HASH frente ataques Cibernéticos mediante la búsqueda de investigaciones y documentación vigente con el fin de brindar recomendaciones sobre un uso adecuado.

3.2 OBJETIVOS ESPECÍFICOS

Examinar las características particulares y elementos principales de los algoritmos simétricos, asimétricos y Hash a partir de fuentes bibliográficas especializadas con el ánimo de comparar las principales características, ventajas y desventajas.

Comparar fortalezas y debilidades de los algoritmos simétricos, asimétricos y Hash a través de una revisión sistemática de literatura, identificando el nivel de seguridad y rendimiento de cada uno de manera que se pueda establecer cuál es el más práctico.

Analizar las implicaciones prácticas de los resultados obtenidos en investigaciones anteriores sobre la eficiencia de los diferentes métodos de cifrado y protección de la información, y hacer recomendaciones para su uso en entornos reales

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

En este apartado se tuvo en cuenta los conceptos relacionados con los Algoritmos Simétricos, Algoritmos Asimétricos y HASH buscando características y aspectos relevantes necesarios para el desarrollo de esta Monografía.

Criptografía: Significado de escritura oculta, permite mantener mensajes ocultos, garantizando la confidencialidad, autenticación e integridad. Una parte importante de ellos son las claves que son similares a las claves físicas que se usan para abrir o cerrar una puerta. Cada algoritmo criptográfico necesita una clave con un número correcto de bits y el patrón correcto[2]. Está conformada matemáticamente por un alfabeto para la construcción de un mensaje, espacios o claves finitos para encriptar o desencriptar, transformaciones de cifrado y transformaciones de descifrado. Puede ser usada en firmas digitales, certificados digitales, sistemas de autenticación, y correos electrónicos seguros[3].

Componentes:

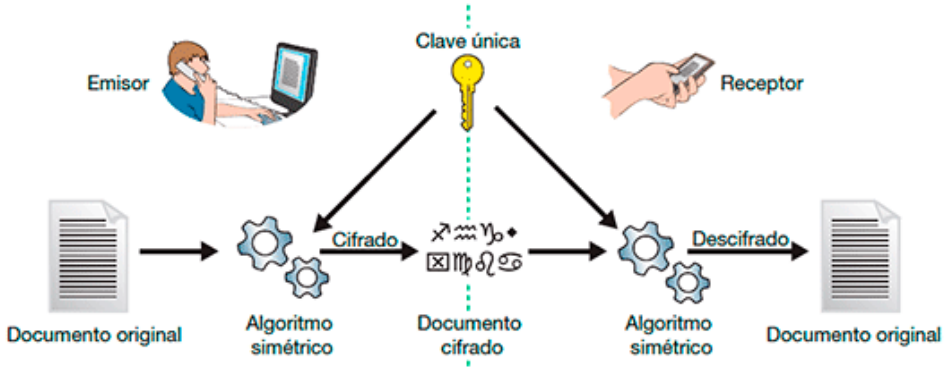
Algoritmos Simétricos: Son aquellos que tienen 1 clave para cifrar y descifrar los mensajes que debe ser conocida tanto por el emisor y el receptor; este es el punto más débil pues resulta fácil de interceptar.

---

[2] MENDOZA, Julio César. "Demostración de cifrado simétrico y asimétrico." *Ingenius: Revista de Ciencia y Tecnología* 3 (2008): 46-53.

[3] MEDINA VELANDIA, Lucy Noemy. Criptografía y mecanismos de seguridad. 2017. https://digitk.areandina.edu.co/handle/areandina/1423

Figura 1. Algoritmo Simétrico[4]



Fuente: Roca Busó (2015)

Los algoritmos simétricos tienen dos versiones según el cifrador, puede ser de bloque o de flujo, el primero codifica los datos en bloques pequeños de longitud fija de 64 bits de longitud, ejemplo de estos son DES, 3-DES, RC2, RC5, RC6, Rijndael (AES) [4].

Algoritmos Asimétricos: Los algoritmos asimétricos tienen 2 claves, una pública y otra privada, la primera la conoce todo el público y la privada solo la persona que quiere acceder a la información o los datos.

Figura 2. Algoritmo Asimétrico[9]

Fuente: Roca Busó (2015)

[4] FERNÁNDEZ TOLEDO, J. (2020). Criptografía simétrica. https://jesusfernandeztoledo.com/criptografia-simetrica/

Son diferentes a los algoritmos simétricos porque en estos simplemente se escoge un número aleatorio de la longitud apropiada, mientras que al generar claves asimétricas el proceso es más complejo. Estos realizan codificación y decodificación y en cada proceso usan claves diferentes que están asociadas matemáticamente, una clave no puede descifrar lo que cifra. Algunos ejemplos de ellos son el *Diffie-hellman* y el RSA [4].

Dentro de sus aplicaciones están el proceso de cifrar información sin transmitir la clave para decodificar lo que le permite ser usado en canales inseguros, los mensajes pueden autenticarse con una firma digital de manera que sea más difícil encontrar otro mensaje con la misma firma.[5].

Encriptación: La encriptación es una técnica que se utiliza para transformar información de manera que solo las personas autorizadas puedan comprenderla. En términos simples, es como convertir un mensaje claro y comprensible en algo que parece completamente confuso y sin sentido, a lo que llamamos texto cifrado. Para lograr esto, la encriptación toma la información que queremos proteger y la mezcla de una manera que parece ser aleatoria y caótica. La encriptación no funciona sola; requiere el uso de una especie de "llave secreta", que es un conjunto de valores matemáticos acordados tanto por la persona que envía el mensaje cifrado como por la persona que lo recibe. Esta llave es esencial para desencriptar y volver a hacer legible la información.

Desencriptar: Es la acción opuesta a la encriptación, busca obtener la información legible a través de una información encriptada. Para hacerla se debe utilizar una clave como parámetro para las fórmulas matemáticas que se usaron en la encriptación[6].

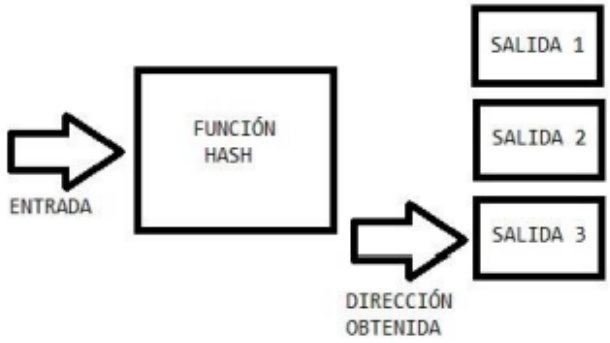
---

[5] MOYA, José Manuel. Introducción a la Protección de la Información. "Criptografía" (Paper). [En línea]. Colegio Oficial de Ingenieros de Telecomunicación, Telecomunicaciones, In Escrituras silenciado: paisaje como cistografía, 2013. págs. 495-513. http://www.academia.edu/21679789/INTRODUCCION_A_LA_PROTECCIÓN_DE_LA_INFORMACIÓN._CRIPTOGRAFÍA_

[6] PAGUAY CUVI, Mario Humberto. "Análisis de algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de ingeniería en sistemas de la ESPOCH." (2015).

Funciones HASH: Es un algoritmo matemático que permite transformar un conjunto de datos en un código alfanumérico de longitud fija. Sin importar el número de datos el código siempre tendrá el mismo número de caracteres.

Figura 3. Funciones HASH[7]



Fuente: HASHING. UN CONCEPTO (2018)

Este tipo de funciones se realizan sobre conjuntos de datos que son resúmenes de los datos originales de tipo fijo e independiente del tamaño original y que se asocia unívocamente a los datos iniciales esto hace que sean imposible encontrar mensajes distintos con un hash idéntico[8]. La diferencia entre el cifrado y el hashing es la forma en cómo se almacenan los datos, en este caso los datos ingresados y convertidos utilizando la función donde el texto plano se pierde. Al igual que el cifrado el hash garantiza la confidencialidad[9].

Tipos de claves criptográficas: La criptografía de llaves puede ser pública o privada, que utilizan dos llaves distintas, una para codificar y otra para decodificar. La pública puede ser divulgada libremente y la privada es mantenida en secreto. Los mensajes

[7] TEJEDOR-MORALES, María Yahaira. HASHING. UN CONCEPTO. UNA REALIDAD.

[8] MUÑOZ-MENDOZA, Luís, Jodamia U. Murillo-Rosado, and Cristian R. Amen-Chinga. "Algo sobre la firma electrónica en el contexto actual." *Polo del Conocimiento* 2.7 (2017): 1016-1028. http://polodelconocimiento.com/ojs/index.php/es/article/view/322

[9] ARIANSEN MONCADA, Renzo Agusto, ROJAS DÍAZ, José Iván. Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016. (2016).. De: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/348/TESIS_Ariansen_Rojas%20.pdf?sequence=1&isAllowed=y

codificados con una llave pública se decodifican con la llave privada que le corresponde, un problema al respecto es que debe existir un proceso que genere las claves privadas y en casos en que el usuario final no tenga la llave no va a poder acceder al mensaje[10].

Gestión de claves: Es una técnica de generación, almacenamiento, distribución y mantenimiento que se aplica a la información almacenada y transmitida tanto en redes como en ordenadores; en la generación de los algoritmos generan las claves pseudoaleatorias de manera que sean impredecibles, los métodos más utilizados son los generadores aleatorios de bits, mediante registros de desplazamiento y con algoritmos matemáticos[11].

Aplicaciones:

Seguridad informática y criptografía: La criptografía garantiza la seguridad o privacidad asegurando que los mensajes sean accedidos solo por el remitente o los destinatarios garantizando la integridad de la información. Actualmente son métodos muy seguros y eficientes gracias al uso de llaves que pueden contener letras, símbolos y dígitos[12].

Criptografía en redes: Al utilizar el internet el cifrado de información está presente con el objetivo de proteger la información y privacidad. Cuando accedemos a webs cuya url inicia con “HTTPS” encontramos un cifrado con una clave pública y una privada que cuando inicia sesión en el servidor web, este envía una clave pública al navegador llevando a cabo un “SSL Handshake” o saldo entre el navegador y el servidor. Al iniciar sesión el navegador reconoce el link y lo muestra como seguro[13].

---

[10] Tecnología + informática. ¿Qué es la criptografía? [En línea]. 2020. [Fecha de consulta: 10 abril 2023]. Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/.

[11] HUIDOBRO, José Manuel. Introducción a la protección de la información. “criptografía”.

[12] TORRES CARDONA, Renson. "Criptografía simétrica y asimétrica y su aplicación en medios digitales como las imágenes, video y audio.". https://repository.unad.edu.co/handle/10596/40365

13 OFICINA DE SEGURIDAD DEL INTERNAUTA. Tipos de cifrado para proteger nuestra información en internet. . 2019. <De: https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad>.

DSS: Es un estándar propuesto para firmar digitalmente dentro del cual se propuso usar un algoritmo llamado DSA. El DSA es una variante del algoritmo Gamal, su seguridad se basa en la resolución de problemas basándose en un logaritmo discreto, hace uso de la función hash. Tiene una longitud de firma de 320 bits con una clave que varía entre 512 a 1024 bits[14].

Algoritmo: Un algoritmo es un conjunto de instrucciones o reglas bien definidas, finitas y ordenas que llevan a cabo una actividad mediante una serie de pasos sucesivos que al hacer dicha actividad no generan dudas[15].

Algoritmos criptográficos: Se modifican los datos de un documento con el fin de alcanzar características respecto a disponibilidad, integridad y autenticación. Son de dos tipos: Simétricos y Asimétricos.

La criptografía es una forma de almacenar o transmitir información evitando que sea utilizada por terceros, hace que la información no sea transparente para todos con un proceso de descifrado que permite verla en su estado normal[16]. Existen dos tipos de criptografía, una simétrica y una asimétrica que se abordarán en este trabajo. La criptografía simétrica ha sido siempre el núcleo de las aplicaciones criptográficas; el más famoso algoritmo es el DES (*Data Encryption Standard*) que surgió en los años setenta hasta la década de los noventa donde fue reemplazado por el algoritmo AES (*Advanced Encryption Standard*), un algoritmo de estructura simple y matemática, con gran rapidez y versatilidad de implementación; fue un algoritmo que en su época pudo demostrar

[14] ALMENARES MENDOZA, Florina, ARIAS CABARCOS, Patricia. *Estudio de la eficiencia de protocolos y algoritmos de seguridad en Android*. BS thesis. 2015.
[15] MUNDT BRICEÑO, Carlos André. *Análisis comparativo entre algoritmos simétricos orientados al IOT*. Diss. Universidad Andrés Bello, 2018. A. (2018). Análisis Comparativo entre Algoritmos Simétricos orientados al IOT.
[16] MÉNDEZ NARANJO, Pablo Martí. 2015. Nuevo Algoritmo Criptográfico con la Incorporación de la Estenografía en Imágenes. (Tesis)(Maestría). [En línea]. Escuela Superior Politécnica de Chimborazo, Posgrado y Educación Continua. Riobamba. 2015. págs. 13-50Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/4374/1/20T00628.pdf

seguridad[17]. Los algoritmos simétricos y sus beneficios se basan en el procesamiento rápido para encriptar y desencriptar un alto volumen de datos, con una desventaja en la distribución y gestión de claves.

Tipos de Ataques:

Ataque de Fuerza bruta: Es un método utilizado en ciberseguridad y en otros contextos para intentar descifrar una contraseña o una clave encriptada mediante la prueba sistemática y repetitiva de todas las combinaciones posibles de caracteres hasta encontrar la correcta. Es un enfoque de prueba y error en el que un programa o un atacante intenta todas las posibles combinaciones de contraseñas, desde las más simples hasta las más complejas, hasta que se logra el acceso no autorizado a un sistema, cuenta o protegido. [18].

Cifrado Cíclico: Es un ataque que consiste en cifrar repetidas veces el criptograma con clave pública que se intercepta del destinatario hasta volver a obtener el criptograma[19] . Es un ataque a una propiedad del RSA, que consiste en cifrar repetidamente el criptograma hasta encontrar el ciclo, es considerado una amenaza importante cuando existe un exponente pequeño[20].

Ataques por canal lateral: Es un tipo de ataque pasivo no invasivo que no deja evidencia de que el sistema haya sido atacado. Puede dividirse en ataques por análisis de tiempo, la información a la que se accede está relacionada con el tiempo de ejecución; ataques

---

[17] PENAZZI, Daniel. CRIPTOGRAFIA DE CLAVE SIMETRICA: AES (Notas de curso para las Jornadas de Criptografía y Códigos Auto correctores.) [En línea]. Universidad Nacional de Córdoba, Facultad de Matemática, Astronomía y Física. Mar de Plata, 2006. págs. 3-10. Disponible en: http://www.famaf.unc.edu.ar/~penazzi/17NovAESMardePlata.pdf

[18] ARÉVALO-RODRÍGUEZ, Anderson Smith, Diana Marcela Hurtado-Gómez, and Gilber Jhon Galindo-Sierra. "Algoritmo internacional de cifrado de datos (IDEA) que utiliza la variante de cifrado SHA-256." *Revista Vínculos* 19.2 (2022). De: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/20826/19136

[19] MARÍ SALVADOR, Noelia. *Una propuesta híbrida para el criptoanálisis RSA*. Diss. Universitat Politècnica de València, 2018.

[20] BALBÁS GUTIÉRREZ, David. "Ataques al criptosistema RSA." (2019).

por análisis de la radiación electromagnética, se analizan las perturbaciones del espectro próximo al sistema provocando el funcionamiento del dispositivo; y, ataques por análisis de consumo, en los que se analiza el consumo del dispositivo[21].

Criptoanálisis diferencial: Se da cuando el atacante tiene acceso al texto plano y al archivo cifrado y quiere conseguir la clave de encriptación. Busca las diferencias en las transformaciones durante el cifrado de manera que pueda encontrar cuando el proceso de cifrado está haciendo un proceso no aleatorio encontrando patrones estadísticos que le lleven a descifrar la clave[22].

Criptoanálisis lineal: Se busca encontrar correlaciones entre el texto claro y texto cifrado obtenido en la salida del sistema criptográfico. Se da en ataques con la posibilidad de escoger los mensajes para los posteriores procesos de cifrado. Se basa en el análisis de las dependencias lineales entre los bits de los datos entrantes[23].
Colisiones: Es cuando se dan dos tipos de entradas distintas que producen la misma salida en la misma dirección, en lugar de diferentes, se da en las funciones hash generalmente.

4.2 MARCO TEÓRICO Y ANTECEDENTES

A lo largo de los años se ha creado la necesidad de comunicarse y transmitir información manteniendo la confidencialidad, desde hace siglos se han venido desarrollando señales, signos, gestos y jeroglíficos que han servido para remitir información de una manera más segura y en clave.

[21] LUMBIARRES LÓPEZ, Rubén. "Generación de falsas claves criptográficas como medida de protección frente a ataques por canal lateral." (2015).
[22] BARREIRO MONT, Claudia. *Desarrollo de una plataforma de criptoanálisis basada en medidas de consumo sobre el algoritmo de encriptación DES*. BS thesis. Universitat Politècnica de Catalunya, 2019.
[23] TRAYNO, VLADLENA. "Ataque diferencial mediante inyección de un error en AES-128." (2016).

Hoy en día debido a los avances tecnológicos, el internet y el auge de las redes sociales se ha tenido que incrementar la seguridad en estos procesos de comunicación e intercambio de mensajes en aras de que no sea utilizada para perjudicar a otras personas[24]. La criptografía brinda la seguridad necesaria para guardar o enviar información, es algo que ha venido siendo estudiado desde hace mucho tiempo. Es así como para garantizar la seguridad en las transacciones realizadas a través de redes e internet se han diseñado protocolos criptográficos que ofrecen servicios de seguridad que se basan en:

Confidencialidad: Garantiza que la información transmitida o almacenada permanezca privada y solo sea accesible para aquellos con permisos para verla.

Integridad: Asegura que la información no sea alterada ni modificada durante la transmisión o almacenamiento, manteniendo su precisión y confiabilidad.

Autenticación: Verifica la identidad de las partes involucradas en la transacción, asegurando que son quienes dicen ser.

No repudiación: Evita que alguna de las partes pueda negar su participación en la transacción, estableciendo responsabilidad y autenticidad en las acciones realizadas.

Flexibilidad y facilidad de uso: La capacidad de adaptarse a diferentes entornos y a la comodidad en la utilización de los servicios de seguridad sin complicaciones excesivas.

Eficiencia y confianza en el sistema: Se trata de la capacidad del sistema para funcionar sin problemas, de manera rápida y fiable, generando confianza en su operatividad.

[24] JYOTI, Gaba y KUMAR, Mukesh. Implementation of Steganography Using CES Technique. (Conference Paper) [En línea]. The Technological Institute of Textile & Sciences, Department of Computer Engineering, IEEE Second International Conference on Image Information Processing (ICIIP), 2013. Págs. 395-399. Disponible en: https://www.researchgate.net/publication/261458593_Implementation_of_steganography_using _CES_technique

Los protocolos criptográficos emplean cifrado simétrico, asimétrico, funciones hash, entre otros. En el caso de plataformas de comercio electrónico existen protocolos específicos que permiten realizar transacciones seguras, el SSL y el SET; Sin embargo, estos protocolos solo permiten proteger los datos intercambiados en una transacción entre un servidor web y un navegador, pero no garantizan la seguridad más allá, lo que los vuelve vulnerables a ataques y robos por parte de usuarios remotos[25]. Es así como la criptografía es vital en la protección de la información evitando los malware, códigos maliciosos y ataques cibernéticos.

Ahora bien, el desarrollo del internet y otras estructuras han permitido mejorar la velocidad de navegación y de transferencia, dando lugar a un mayor volumen de información que transita a través de la red haciendo necesario controlar la información para que esta sea utilizada con fines concretos. En el caso de las redes sociales los datos que se ingresan en ellas dejan un rastro, algo que es utilizado para detectar patrones o preferencias de consumo. En el momento en el que se aceptan las políticas de cookies de cada sitio se otorga un consentimiento para que esos datos sean utilizados con fines comerciales o que en caso de ser necesitados por el gobierno se puedan ceder. Todo esto ha creado una serie de opiniones y conceptos acerca de la vulnerabilidad de las leyes de la privacidad que en casos son consideradas como insuficientes dando paso a la adecuación de normas y mecanismos para la vigilancia y el control.

La vigilancia y el control han sido compañeros de la información durante mucho tiempo, a partir del siglo XX han sido muchos los dispositivos que se han utilizado para esto, uno de ellos son el documento de identidad, el registro de huella dactilar y el control biométrico[26]. Es así como autores como Gottfried Wilhelm Leibniz y otros de sus contemporáneos prevenían la necesidad de utilizar algoritmos para responder a las

[25] VELASCO ESCOBAR, Moisés. Seguridad de la información en la red basada en el sistema de criptografía RSA. De: https://tesis.ipn.mx/bitstream/handle/123456789/21731/TESIS.pdf?sequence=1&isAllowed=y

[26] MATTELART, ARMAND, and André Vitalis. *De Orwell al cibercontrol*. Editorial Gedisa, 2015.

exigencias de la información. Más adelante Francisco Sierra Caballero en su obra “De Orwell al cibercontrol, 2015” advirtió la necesidad de propiciar una seguridad total extendiendo políticas de información para preservar la seguridad. Todo esto se incrementó después de los atentados del 11 de septiembre, un momento que dio inicio a los gobiernos para desarrollar leyes que permitieran un control sistemático de la información creando medidas de seguridad y vigilancia[27].

Después de las filtraciones de Edward Snowden a medios de comunicación en el año 2013, se cambió la percepción de vigilancia y control generando debates acerca de cómo algunas medidas vulneran la privacidad. Hoy en dia las personas se ven sometidas a una transparencia impuesta por la ideología de Facebook que, según Bauman y Lyon, 2013, p.21: “La nueva vigilancia, basada en el procesamiento de la información […] permite una nueva transparencia en la que no solamente los ciudadanos como tal sino todos nosotros, en cada uno de los roles que asumimos en nuestra vida cotidiana, somos constantemente controlados, observados, examinados, evaluados, valorados y juzgados. Pero no ocurre lo mismo en el sentido contrario. A medida que los detalles de nuestra vida cotidiana se hacen más transparentes para los organismos que nos vigilan, más difícil resulta discernir cuáles son sus propias actividades”[28]

El uso de algoritmos y procesos de encriptación con todo esto se ha hecho más sofisticado y discriminatorio, evolucionando sus técnicas a diferentes escalas de operatividad y complejidad, llegando a que los esquemas de cifrado tengan un mayor uso, tanto que en la actualidad los navegadores brindan a sus usuarios canales seguros que usan la criptografía a través de protocolos SSL.

Un ejemplo de los procesos de integración viene dado por las imágenes digitales por su lado a finales del siglo XX e inicios del XXI vagaban por las páginas de forma

[27] SANCHEZ RUBIO, Dionisio. "Diseño gráfico en la era post-Snowden. Criptografía tipográfica y otros modos de camuflaje." *INMATERIAL. Diseño, Arte y Sociedad* 1.2 (2016): 33-67.
[28] MARCOS, Manuel Gavira. "Zygmunt Bauman y David Lyon. Vigilancia líquida 2013. Barcelona: Paidos, 176 pp." *Encrucijadas: Revista Crítica de Ciencias Sociales* 16 (2018): 17.

desordenada, hoy en día incluso no es posible saber si una imagen es original o copia de otra igual; con el nacimiento del blockchain, el sistema de codificación vinculado a obras digitales se ha configurado con el fin de salvaguardar su autoría. Algo muy popular del *blockchain* son las criptomonedas que se usan para transacciones monetarias como método de pago digital que se apoya en un código criptográfico. Otro ejemplo, son los tokens No Fungibles o NFTs que aparecieron en 2014, un activo criptográfico que se vincula a un certificado digital que está conectado al bien para confirmar una transacción[29].

Así pues, la criptografía fue inventada hace más de cuatro mil años, creada para garantizar la confidencialidad de medios escritos en entornos bélicos, hoy en día es usada bajo los mismos principios de permutación y sustitución para convertir textos legibles en ilegibles, usando claves secretas. Los algoritmos son mucho más sofisticados con el fin de que garanticen que aun las computadoras más potentes no sean atacadas. El cifrado en la actualidad ha hecho posible que se cuenten con aplicaciones para realizar compras en línea, mensajes en los teléfonos inteligentes, tecnología disruptiva como criptomonedas y cadenas de bloque[30]

[29] LUQUE LODEIRO, Rubén, et al. Blockchain: Estado del arte, tendencias y retos. 2020.
[30] SANDOVAL, Miguel Morales; De La Fuente, José Antonio Molina; DE LA FUENTE ANAYA, Héctor Alán. Criptografía: una tecnología antigua en aplicaciones modernas de alto impacto. 2022..

6. RECONOCIMIENTO DE LAS CARACTERÍSTICAS PARTICULARES Y ELEMENTOS PRINCIPALES DE LOS ALGORITMOS ASIMÉTRICOS, ALGORITMOS SIMÉTRICOS Y HASH

6.1 Algoritmos Asimétricos

Los algoritmos asimétricos surgieron en la década de los setenta como respuesta a la necesidad de crear sistemas irrompibles que garantizaran la máxima seguridad informática, fue así como se crearon los primeros algoritmos cuya complejidad matemática soportara cualquier tipo de criptoanálisis. Sus características principales eran la de incluir una clave pública y otra privada sin requerir un acuerdo previo de clave. Se basan en funciones cuyo inverso es computacionalmente imposible de determinar[31].

Es conocido como una criptografía de clave pública utilizando dos claves, la pública que es conocida por el público y la cifrada que es privada sólo conocida por quien la creó, estas claves se relacionan entre sí por cualquier medio matemático. En este tipo de criptografía la distribución de las claves se hace mediante un canal inseguro y la firma digital[32] (Andrade Bazurto)

Esta criptografía tiene tres operaciones básicas: El cifrado, en el que se cifra con una clave pública y se descifra con una privada; la firma, que garantiza la autenticidad de los datos, mas no la confidencialidad, en donde se cifra con la clave privada del firmante y se comprueba con la clave pública del mismo; y, el intercambio de clave, que permite el intercambio de una clave generándola de forma aleatoria y cifrándola con la clave pública, sin embargo, existen algoritmos que no permiten cifrar ni firmar pero que si dejan

[31] PADRÓN-GODÍNEZ, Alejandro; MELÉNDEZ, R. Prieto; TREVIÑO-PALACIOS, Carlos Gerardo. Lectura de clave óptica bajo el esquema de criptografía asimétrica. En *Memorias: SOMI XXXIV, Congreso de Instrumentación, Morelia, Michoacán-México*. 2019.

[32] BAZURTO, Alicia Andrade. *Características y aplicaciones de las funciones resumen criptográficas en la gestión de contraseñas*. 2019. Tesis Doctoral. Universitat d'Alacant/Universidad de Alicante.: https://rua.ua.es/dspace/bitstream/10045/96849/1/tesis_alicia_andrade.pdf

compartir de forma segura un mismo número en ambos extremos de los cuales se puede derivar una clave para criptográfica simétrica[21].

Al evaluar el rendimiento la criptografía asimétrica es lenta para el cifrado de datos por lo que se debe recurrir a un intercambio de claves y el complemento con criptografía simétrica para el resto de los datos. En el caso de firma digital se debe calcular mediante una función hash para mejorar la eficiencia[4].
Algunos de los algoritmos que usan esta criptografía son:

RSA "*Rivest-Shamir-Adleman*": Posee tres etapas, la primera para generar claves, la segunda para cifrar el mensaje y la tercera para descifrarlo; en la generación de claves el usuario busca dos números primos grandes y fuertes que luego se multiplican, se usa la función de Euler para generar otro número primo denominado e, luego se multiplican los dos números hallados que generan la clave pública y privada, en el cifrado se tiene una lista de números equivalentes al sistema a cifrar, esto hace que el destinatario deba buscar la clave pública en el directorio[33].

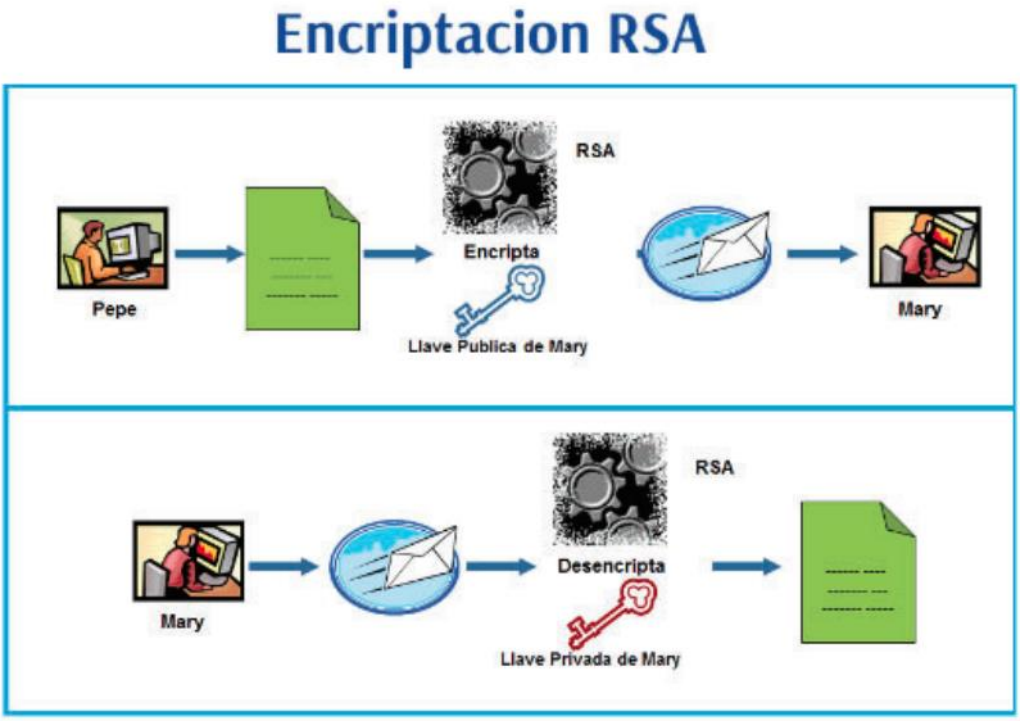
Es un algoritmo muy seguro para enviar información entre personas que no se conocen y quieren comunicarse sin comprometer sus datos personales. Es un algoritmo que se usa en la verificación de firmas digitales, sin embargo, toma mucho tiempo cifrar los datos de esta manera, no es práctico a la hora de usar archivos grandes o numerosos[34]. Es un algoritmo que ha tenido gran expansión y que puede ser utilizado a lo largo de los años en varias plataformas comerciales como Apple, Microsoft, Sun y Novell, es aplicado en

[33] LEYVA BORGES, María Esther. *Creación de un procedimiento para atacar la seguridad del RSA*. 2019. Tesis Doctoral. Universidad Central "Marta Abreu" de Las Villas.: https://dspace.uclv.edu.cu/bitstream/handle/123456789/12056/AAB.%20Tesis.%20Criptoanalisis.pdf?sequence=1&isAllowed=y

[34] HP. ¿Cuáles son los diferentes tipos de cifrado? 2021. https://www.hp.com/co-es/shop/tech-takes/cuales-son-los-diferentes-tipos-de-cifrado#:~:text=Los%20tres%20principales%20tipos%20de,consumidores%20utilizan%20todos%20los%20d%C3%ADas.

organismos estatales, grandes compañías, laboratorios y universidades, incluso en servicios de la nube y conexiones https[35].

Figura 4. Encriptación RSA[36]



Fuente: SÁNCHEZ RODRÍGUEZ (2020)

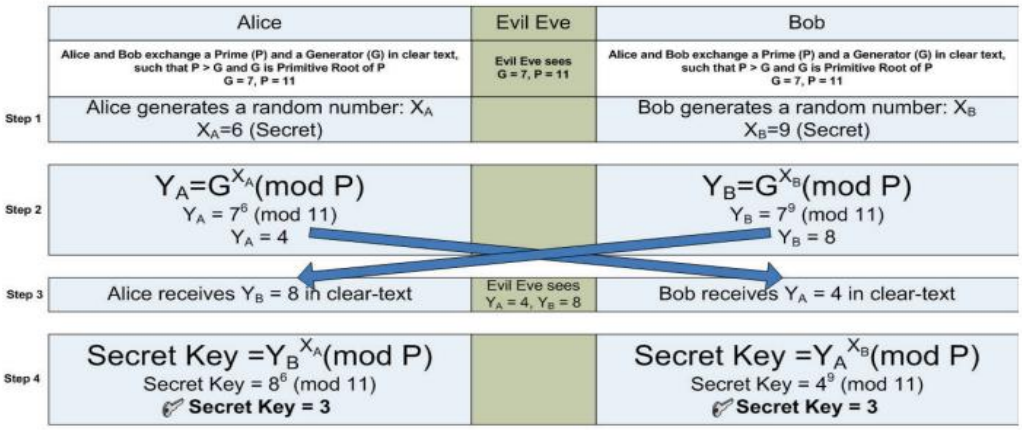
DIFFIE-HELLMAN: Este algoritmo solo permite el intercambio de clave, no sirve para cifrado ni firma digital. Está basado en la dificultad para calcular el algoritmo y permite llegar al mismo número de forma segura; en ocasiones es usado para derivar una clave en criptografía simétrica convencional. Es más rápido que el RSA por lo que es más popular, no está patentado; es usado en protocolos como TSL o cifrado.

[35] LARA PEREZ, Martha Lucia, et al. La computación cuántica y las implicaciones sobre la criptografía moderna. https://repository.unad.edu.co/handle/10596/28230

[36] SÁNCHEZ RODRÍGUEZ, Sofía. Sistema seguro de mensajería instantánea certificada. 2020.. https://oa.upm.es/58165/1/TFG_SOFIA_SANCHEZ_RODRIGUEZ.pdf

Es un algoritmo que permite crear una clave secreta entre dos equipos informáticos que nunca han tenido contacto previo mediante un canal inseguro. Tiene limitaciones como la falta de autenticación, es vulnerable al ataque de hombre en el medio; es recomendable usarlo con otros métodos como la firma digital para verificar identidades; es muy usado en la comunicación de datos, no se recomienda para datos archivados durante largos periodos de tiempo[37].

Figura 5. Encriptación DIFFIE-HELLMAN[38]



Fuente: STATISTA (2022)

ELGAMAL: Desarrollado en 1984 por Taher Elgamal, consta de 3 partes: un generador de claves, el método de cifrado y el de descifrado, cuyo procedimiento se basa en cálculos sobre un grupo cíclico cualquiera. Es muy similar al Diffie Hellman y muy utilizado en la generación de claves digitales. Su seguridad se basa en una función utilizada de un solo sentido y difícil de calcular en sentido contrario.

ElGamal es un algoritmo homomórfico en la multiplicación, combina valores encriptados en otro que corresponde al producto de ellos. Es utilizado en el ámbito de las votaciones

[37] RIQUELME FAÚNDEZ, Edgardo Andrés. Algoritmos genéricos para resolver el logaritmo discreto y sus aplicaciones. 2023.

[38] STATISTA, Available: https://es.statista.com/estadisticas/934626/servicios-de-mensajeria-instantanea-mas-utilizados-por-los-usuarios-de-internet-en-espana/

electrónicas donde se modifica para que tome los votos al exponente, cuando se desencripta se calcula el logaritmo para obtener la suma de los votos, es inconveniente si el número de votos es muy grande pues puede llegar a ser muy costoso[39].

De la criptografía asimétrica los algoritmos más reconocidos son el RSA y ElGamal, el primero basado en la factorización de números enteros y el segundo en un logaritmo discreto. Ambos son computacionalmente intensos por lo que no es recomendable cifrar información muy grande con ellos[40].

6.2 Algoritmos Simétricos

Los algoritmos simétricos son diseñados para cifrar mensajes utilizando una única clave que conoce el emisor y el receptor lo que hace que el documento solo pueda ser descifrado si se conoce esa clave secreta. Algunos de los más usados son AES, BLOWFISH y DES[3].

El algoritmo AES fue desarrollado en 1997 por Vincent Rijeme y Joan Daemen, es muy utilizado en la actualidad y no se conocen ataques eficientes hasta el momento. Tiene como características el procesamiento de bloques completos de texto de 128 bits manejando claves estándar de 128, 192 o 256 bits (Loor Landeta), cuenta con una matriz de ensayos en las que las celdas van cambiando de valor según los procesos ejecutados por medio de la sustitución o la permutación. Consta de 11 rondas, 1 inicial, 9 que pasan por cuatro fases y una final que pasa por tres fases. La clave se da en notación hexadecimal constando de un proceso de cifrado y otro para calcular las subclaves. El único ataque efectivo conocido contra este algoritmo es el de fuerza bruta[1].

[39] ASTUDILLO QUINTERO, Pablo Vicente. Implementación de una red de mezcla utilizando encriptación de Paillier para votaciones electrónicas. 2023.

[40] GARCÍA MARTÍNEZ, Moisés. Estudio de mapeos caóticos discretos y su aplicación en criptografía. 2015. https://repositorio.ipicyt.edu.mx/handle/11627/4030

El algoritmo AES fue evaluado bajo criterios de seguridad, rendimiento de software y hardware, resistencia al análisis de poder, ataques de implementación e idoneidad en entornos cuyo espacio es restringido[1], está probado que es de trabajo rápido en teléfonos y tarjetas inteligentes proporcionando mayor seguridad por su clave más larga, es flexible, veloz y eficiente en la implementación de hardware. Es un algoritmo que realiza en promedio 250000 transformaciones por cada 100 kbytes suficiente para satisfacer los estándares, es usado en productos de hardware y software, estándares de comunicación, redes sociales; en procesadores Xeon y Core, Microsoft lo utiliza en sus productos de software[41].

AES es utilizado en gobiernos y organizaciones de seguridad, empresas privadas para las comunicaciones clasificadas; es usado en la mayoría de herramientas que existen en el mercado y utilizan cifrado es funcional en muchas aplicaciones, es muy seguro y aceptado por su precio[21].

El algoritmo Blowfish, fue utilizado como reemplazo de DES, desarrollado por Bruce Schneider, tiene un cifrado de bloque de 64 bits con una longitud de clave variable de 32 a 448 bits y 18 subclaves, cuenta con 4 casillas de sustitución cada una con 512 entradas de 32 bits[4]. Tiene características de rapidez en microprocesadores de 32 bits, se puede ejecutar en menos de 5 KB de memoria, es muy simple, usa operaciones como la suma XOR y la búsqueda de tablas y es libre. Al ejecutarse se da en dos etapas la generación de las subclaves convirtiendo 448 bits en 7168 bits, y la segunda en el cifrado de datos iterando una función simple 16 veces. La clave de este algoritmo se genera aleatoriamente para cada archivo. Es más rápido que el DES y el IDEA y no requiere licencia para su uso[42]. Posee características como la rapidez en los procesos de encriptación, ocupa un tamaño mínimo de memoria (5Kbyte aproximado), se basa en

[41] RODRÍGUEZ, Ernesto Godínez, et al. AES estándar mundial de encriptado.
[42] RUIZ AZOFRA, Eduardo. Técnicas criptográficas utilizadas en" MALWARE. 2015.

operaciones matemáticas simples, puede aumentar el tamaño de la clave hasta 448 bits[43].

El algoritmo DES (*Data Encryption Standard*), hace uso de la misma clave para el cifrado y descifrado protegiendo así los datos confidenciales comerciales y no clasificados. Es un algoritmo considerado inseguro por su método de cifrado porque ha sido blanco de muchos ataques[44]. Fue desarrollado en 1977 por el Departamento de Comercio de EEUU en colaboración con la empresa IBM, estaba basado en la aplicación de las teorías de criptografía de la época y en las leyes de Estado. Es un algoritmo que consiste en la aplicación sucesiva de permutaciones y sustituciones con un bloque de entrada de 64 bits que se sometía a la función de permutación (8 bits) y la de sustitución (5 bits), constando todo el proceso por 16 etapas de cifrado. De los 64 bits, 56 son utilizados para la encriptación y los restantes son de paridad usados para la detección de errores[45]. En tola el algoritmo llega a una clave efectiva de 56 elevado a la 2 y aunque es computacionalmente seguro, hoy en día con hardware específicos se puede realizar ataques por fuerza bruta descubriendo las claves en solo unos días, es por ello que dejo de ser un algoritmo empleado por el gobierno en 1998, siendo sustituido por el AES[46].

Otro algoritmo simétrico es el IDEA (*International Data Encryption Algorithm*), un cifrador por bloques usado para cifrar textos de un tamaño de 64 bits, con una llave K de 128 bits. Se basa en el uso de desplazamientos circulares ejecutados de manera compleja para generar seis subclaves para cada una de ocho etapas[47]. El algoritmo IDEA fue creado

---

[43] VELASTEGUI, Marco Antonio Yandún, Francisco Joseph Bolaños Burgos, and Jairo Vladimir Hidalgo Guijarro. "Algoritmos simétricos y asimétricos para el encriptado de imágenes Symmetric and asymmetric

[44] RODRÍGUEZ RODRÍGUEZ, Jefferson Stivens, et al. Operadores genéticos aplicados a la criptografía simétrica. https://repository.udistrital.edu.co/handle/11349/28192

[45] HERRAMIENTAS WEB PARA LA ENSEÑANZA. Protocolos de comunicación DES. 2021. https://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

[46] GUEVARA SAMANIEGO, Vanessa Alexandra. *Desarrollo de un algoritmo para romper por fuerza bruta al Simplified Data Encryption Standard (S-DES) mediante el uso de computación paralela*. 2019. Tesis de Licenciatura. Quito, 2019. http://bibdigital.epn.edu.ec/handle/15000/20362

[47] SAMANIEGO ZANABRIA, Ana Liz. Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información. 2018.. De: https://repositorio.urp.edu.pe/bitstream/handle/20.500.14138/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

en los años noventa por Lay y Masey. El algoritmo que se usa en el cifrado es el mismo que en el descifrado. Realiza complejas operaciones matemáticas siendo muy eficiente incluso con procesadores de 16 bits. Según expertos este algoritmo es más recomendable que el DES[48].

La criptografía simétrica es una herramienta básica de cifrado, práctica, rápida y segura; presenta dos tipos de cifrado: En bloque y en flujo, ambos funcionales y de rendimiento muy similar. Los más destacados cifradores en bloque ya se mencionaron en párrafos anteriores y se diferencian porque los de flujo toman el mensaje de elemento a elemento (bit o byte) procesándolo en modo de cadena (letra a letra)[49]; aplican una transformación que varía dependiendo de la clave y de la posición del elemento en el mensaje; todos se basan en el esquema de Vernam[50].

6.3 HASH

El hash es una operación criptográfica que genera identificadores que son únicos y que no se pueden repetir a partir de una información dada, su objetivo es codificar los datos por medio de una cadena de caracteres única, asegurando la autenticidad, el almacenamiento seguro de mensajes y la firma de documentos digitales.

Las funciones se dan por medio de una serie de procesos matemáticos y lógicos complejos realizados por computación con el fin de obtener una cadena de caracteres con una longitud fija y única para los datos que se introducen. Los hashes son un proceso unidireccional lo que lo hace un método más seguro.

---

[48] MAÑAS, José Antonio. GUÍA DE SEGURIDAD (CCN-STIC-401). GLOSARIO Y ABREVIATURAS. 2016.

[49] DAZA, Doris Maritza Ruano, et al. Análisis del rendimiento entre los algoritmos simétricos de Blowfish y AES. *Revista Vínculos: Ciencia, tecnología y sociedad*, 2021, vol. 18, no 2, p. 2. Available from: https://geox.udistrital.edu.co/index.php/vinculos/article/view/17632/18723

[50] Yambay Wilman, Jenny; ARCOS PONCE, Georgina. *IV congreso internacional de ingenierías: La ingeniería como base del desarrollo*. Universidad Politécnica Estatal del Carchi, 2018.

Cada hash tiene un resultado diferente para la misma información, variando sus longitudes entre 224, 256, 384 y 512 bits, todo depende de la función que se elija. Por ejemplo, si un código arroja 256 bits, el código sería 64 caracteres alfanuméricos; es algo complicado, pero es fundamental para mantener la seguridad de la información. Tiene ventajas como que no importa la cantidad de información que se le suministre el resultado siempre tendrá la misma longitud, generalmente 64 caracteres, esto hace que sea más legible; cualquier modificación que se le haga a la entrada resultará en un hash totalmente diferente, lo que hace que ninguno sea igual a otro[51].

Dentro de sus aplicaciones se encuentra la utilización en páginas web para descargar archivos muy pesados protegiendo su confidencialidad y evitar que los documentos sean manipulados. En cuanto a firmas digitales el algoritmo se desarrolla con los datos enviados para luego descifrarlo con una contraseña especial de manera que el que tenga la clave puede comprobar que el documento es auténtico[28].

Algunas funciones que se destacan del Hash son la creación de claves públicas que representan las direcciones de las carteras (Address Wallet), estas acortan la dirección y agregan una capa extra de seguridad. Un ejemplo de utilización es el Bitcoin. Otra es el proceso de minería que calcula SHA-256 de forma distribuida en cada nodo, permitiendo la creación de nuevos bloques[52].

Se usa en aplicaciones como firmas digitales, lectores de huellas digitales, verificación de voz o face ID en teléfonos celulares, en el comercio electrónico garantizando la seguridad y los sistemas de pago en línea y en los bancos, haciendo uso de tokens para confirmar las transacciones[53]

---

[51] SANTOS, Jesús. Que son, como funcionan y para qué sirven los hash. 2022. https://economia3.com/funciones-hash-para-que-sirven/

[52] SAN MIGUEL MARTÍN, Pablo. Diseño y desarrollo de un algoritmo eficiente y seguro de firma digital ECDSA para su uso en protocolos Blockchain. 2023.. Available from: https://oa.upm.es/72880/1/TFG_PABLO_SAN_MIGUEL_MARTIN.pdf

[53] Tejedor Morales, María Yahaira. HASHING. UN CONCEPTO. UNA REALIDAD. De. https://www.laccei.org/LACCEI2018-Lima/student_Papers/SP73.pdf

TABLA 1. COMPARATIVO DE LOS ALGORITMOS SIMÉTRICOS, ASIMÉTRICOS Y HASH

Algoritmos	Características	Ventajas	Desventajas
Asimétricos	• Utiliza dos claves (cifrado, descifrado) • Tamaños de clave 2048 bits o mayores	• Seguridad: Puede comunicar en forma segura claves públicas a terceros • Numero de claves: Un par de claves por usuario • Mejor en el manejo de grandes cantidades de datos	• Velocidad: Lento • Utiliza más recursos • Tiene riesgos si se pierde la clave privada
Simétricos	• Utiliza la misma clave para cifrar y descifrar • Tamaños de clave de 128 o 256 bits	• Velocidad: Rápido • No utiliza muchos recursos • Es mejor en el manejo de grandes cantidades de datos • Presenta riesgos de robo de claves si estás no se gestionan adecuadamente	• Número de claves: A medida que aumentan los usuarios aumenta el número de claves • Seguridad: Alta vulnerabilidad porque pública la clave
HASH	• Longitudes de 224, 256, 384 y 512. • Cualquier modificación que se le haga a la entrada de información dará como resultado un hash completamente diferente	• nivel de seguridad bastante alto • sencillo de usar • Muy legible • permiten descargar archivos muy pesados	• No permite usar registros de longitud variable • No clasifica algunos archivos • No permite repetir la misma llave

Fuente propia

7. COMPARACIÓN DE LAS FORTALEZAS Y DEBILIDADES DE LOS ALGORITMOS SIMÉTRICOS, ASIMÉTRICOS Y HASH A TRAVÉS DE UNA REVISIÓN SISTEMÁTICA DE LITERATURA, IDENTIFICANDO EL NIVEL DE SEGURIDAD Y RENDIMIENTO DE CADA UNO DE MANERA QUE SE PUEDA ESTABLECER CUÁL ES EL MÁS PRÁCTICO

En este capítulo se realiza una revisión de la literatura que compara las fortalezas y debilidades, identificando el nivel de seguridad de los algoritmos simétricos, asimétricos y Hash, estableciendo cuál es el más práctico.

En el 2016, se realizó un análisis y comparación del rendimiento de los algoritmos AES y Blowfish. El proceso fue realizado a través de una simulación con tres máquinas virtuales con los sistemas operativos Windows 7, Windows 8.1 y Windows 10; cada máquina cifrando los mismos tipos de archivo de video, pero con rangos de tamaño diferente. Los resultados de la simulación para el cifrado y descifrado se muestran en la figura 6.

Figura 6. Cifrado y descifrado de archivos de video utilizando AES y Blowfish[54]

Tamaño	AES	Blowfish
11,867	0,22	0,34
51,291	0,97	1,67
103,278	3,44	3,23
512,800	16,2	30,27
1051,988	55,47	33,53

Cifrado en Windows 7

Tamaño	AES W7	Blowfish W7
11,867	0,13	0,22
51,291	0,47	0,73
103,278	1,50	1,45
512,800	4,56	7,42
1051,988	10,97	15,09

Descifrado en Windows 7

Tamaño	AES	Blowfish
11,867	0,67	0,44
51,291	1,53	1,39
103,278	2,08	2,78
512,800	13,58	16,41
1051,988	38,08	40,86

Cifrado en Windows 8.1

Tamaño (KB)	AES (seg.)	Blowfish (seg.)
11,867	0,13	0,20
51,291	0,45	0,73
103,278	1,06	1,64
512,800	6,00	9,03
1051,988	13,22	19,45

Descifrado en Windows 8.1

Tamaño	AES	Blowfish
11,867	0,42	0,20
51,291	1,08	1,64
103,278	3,03	3,78
512,800	16,77	19,97
1051,988	32,02	34,47

Cifrado en Windows 10

Tamaño	AES	Blowfish
11,867	0,13	0,19
51,291	0,50	0,77
103,278	0,91	1,47
512,800	5,08	7,84
1051,988	11,98	15,55

Descifrado en Windows 10

Fuente: Thruman Wladimir (2016)

[54] CARRERA ALBÁN, Thruman Wladimir. Análisis y comparación de dos algoritmos de cifrado simétrico en plataformas Windows. 2016. UEES. De: http://repositorio.uees.edu.ec/bitstream/123456789/1428/1/MATI_PaperFinal_ThrumanCarrera.pdf

En los resultados de la simulación se encontró que el algoritmo AES en términos de tiempo de procesamiento es muy superior al algoritmo Blowfish utilizando cualquiera de los tres sistemas operativos. Blowfish es un algoritmo que requiere más potencia de procesamiento.

En los algoritmos simétricos, en el año 2018, Samaniego Zanabria realizó una evaluación de los algoritmos AES, IDEA y RC5. En el análisis encontró que el algoritmo AES está diseñado bajo 3 criterios: el máximo de resistencia frente a ataques conocidos, sencillez de diseño y una implementación con velocidad y adaptabilidad; es implementado con un mecanismo de protección con una única llave mediante lógica combinacional suplementada con registros, multiplexores y memorias; no cuenta con parámetros en los que se pueda personalizar por parte del usuario, en cuestión de seguridad es resistente a los análisis lineales y diferenciales, no cuenta con parámetros de borrado de emergencia y tiene una capacidad para 80 bits de seguridad (1024 bits de RSA y 163 de ECDSA).

En cuanto al algoritmo IDEA, brinda una seguridad que se deriva del intercalado de operaciones en grupos adición y multiplicación modular y O-exclusivo (XOR) [32], no cuenta con parámetros personalizables por el usuario ni con un borrado de emergencia, tiene una capacidad en la que la llave original se divide en 8 partes de 16 bits cada una, las primeras 6 se dan de izquierda a derecha y son utilizadas en la primera ronda; en la capacidad de cifrado en los mensajes de mayor tamaño se utilizan modos de operación que permiten cifrar archivos de cualquier tamaño con una sola llave y un cifrador determinado[34].

El algoritmo RC5, opera con rotaciones dependientes con operaciones como sumas modulares y operaciones XOR, en cuestión de seguridad utiliza la clave secreta para expandir un arreglo S de claves conteniendo 2(r+1) palabras aleatorias, es un algoritmo que proporciona alta seguridad porque incorpora rotaciones circulares de bits que dependen de los datos introducidos haciéndolo un algoritmo más robusto e irrompible, no

cuenta con parámetros personalizables por el usuario ni con borrado de emergencia, sin embargo, puede ser fácilmente implementado[33].

En la ejecución de los algoritmos AES, IDEA y RC5, se encuentran tiempos de ejecución que corresponden a 1539,7 Mb/s 4174 b/s y 3450 b/s respectivamente, con tiempos de descifrado de 1529 Mb/s, 6452 b/s y 5665 b/s[33]. En las pruebas de criptoanálisis realizadas por Samaniego Zanabria, teniendo en cuenta ataques con texto cifrado, con texto original conocido y texto cifrado, y, con texto cifrado escogido, se dieron los siguientes resultados en los tiempos empleados para descifrar el texto: AES (634 segundos), IDEA (399 segundos), RC5 (538 segundos). En las pruebas de ataques de fuerza bruta encontraron que solo el AES y el RC5 cumplen con el ítem longitud de la clave, y solo el AES cumple con el requisito complejidad de la clave para evitar los ataques de fuerza bruta[55]. Con lo anterior el estudio concluyó que, en fortalezas como la seguridad de la clave, la dificultad para adivinar la clave y la dificultad para invertir el algoritmo cifrado, de los tres algoritmos evaluados solo el AES cumple con la dificultad para invertir el algoritmo cifrado.

Para el año 2019, se realizó un estudio comparativo entre los algoritmos simétricos AES y DES, y el asimétrico RSA utilizando valores como la línea de tiempo del algoritmo, el valor de longitud de clave, el tipo de algoritmo, la cantidad de datos que se van a cifrar, problemas de seguridad, velocidad en los procesos de cifrado y descifrado, tamaño de la clave y variación del tamaño del bloque, usos y utilidades y funcionalidad.
En los resultados del estudio encontraron que de los tres algoritmos el más reciente es el AES, en la cantidad de datos que se van a cifrar el DES es más bajo en comparación con el AES y el RSA, en cuanto a velocidad el RSA es más lento, en la variación del tamaño de la clave o nivel del escalabilidad el único escalable es el DES, los tres

[55] SAMANIEGO ZANABRIA, Ana Liz. Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información. 2018.. De: https://repositorio.urp.edu.pe/bitstream/handle/20.500.14138/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllow

presentan bajos consumos de energía, en el momento de implementarlos en hardware y software el DES es mejor en hardware, el AES es más rápido y eficiente tanto en hardware como en software y el RSA tiene un alto costo computacional. Los tres algoritmos son usados para la confidencialidad e integridad, sin embargo, el RSA sirve para verificar la autenticidad de origen. En la categoría de funcionalidad el DES funciona para cifrado y descifrado de archivos, el AES para Cifrado y descifrado de archivos y cifrado de contraseñas; y el RSA para el cifrado de mensajes, firma digital e intercambio de claves[56].

De este estudio comparativo se puede concluir que el AES tiene fortalezas como la rapidez, seguridad, facilidad de implementación y eficiencia, puede diseñarse de manera que la longitud de clave se pueda adaptar a las necesidades, se puede implementar en software y hardware. Su debilidad radica en la comunicación de la clave. Del algoritmo DES, se pueden mencionar fortalezas como la rapidez, facilidad de implementación y eficiencia, tiene debilidades como la longitud de la clave que es muy corta, es un algoritmo inseguro y obsoleto. Del algoritmo RSA (asimétrico), se pueden mencionar fortalezas como la seguridad, la longitud de clave variable, ventajas como la firma digital, aunque su alto costo llega a ser una debilidad.

Comparando algoritmos asimétricos conocidos como el Diffie-Hellman (DF) y el RSA, así como sus fortalezas se encuentra que en cuestiones de seguridad ambos algoritmos son significativamente seguros, aunque difieran en el tamaño de clave. El Diffie-Hellman, es susceptible a ataques man in the middle (MitM) porque no auténtica a ninguna de las partes involucradas en el intercambio, en estos ataques el tercero se hace pasar por una de las partes creando un par de claves para falsificar mensajes pudiendo así descifrar los

[56] SERRATO LOSADA, Hernán Darío, et al. Comparación de métodos criptográficos para la seguridad informática. 2019. https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

mensajes intercambiados; esta debilidad se corrige con una firma digital, algo que proporcionaría una autenticación adecuada. Otra fortaleza del DF es que proporciona secreto directo perfecto (claves de sesión únicas para cada sesión), algo que no proporciona el RSA[57].

Paguay Cuvi (2015) en su análisis de algoritmos matemáticos relaciona las siguientes fortalezas y debilidades de algunos algoritmos asimétricos: El RSA, posee fortalezas relacionadas con la imposibilidad de factorizar números primos extremadamente grandes actuando de forma similar a una firma digital, pudiendo llegar a ser verificada la autenticidad del archivo o texto cifrado; el Diffie-Hellman tiene la fortaleza de que es capaz de distribuir claves a más de 2 personas mediante sistemas de clave pública, es un algoritmo seguro en el intercambio de claves anónimas, sin embargo, posee la debilidad de que puede ser vulnerado por un ataque de hombre en el medio lo que hace que sea necesario verificar alguna forma de autenticidad del usuario que remite; el algoritmo Gamal, tiene como fortaleza que sirve para generación de cifrados DSS y NIST pero cuenta con la debilidad de que las cadenas de cifrado son más largas, lo que hace que se consuma más recurso computacional, en este sentido es menos eficiente que el RSA, además de que es menos fuerte con respecto al RSA a los ataques por fuerza bruta[58].

En relación con las funciones criptográficas Hash, se mencionan fortalezas como la eficiencia respecto a otros algoritmos implicando un gasto computacional bajo para un equipo de gama baja o media[59], otra de sus fortalezas es que evitan valores duplicados

[57] KRIPTÓN SOLID. Comparación de los algoritmos de intercambio de claves Diffie-Hellman y RSA. De: https://kryptonsolid.com/comparacion-de-los-algoritmos-de-intercambio-de-claves-diffie-hellman-y-rsa/

[58] PAGUAY CUVI, Mario Humberto. Análisis de algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de ingeniería en sistemas de la ESPOCH. 2015.. De: https://core.ac.uk/download/pdf/234590142.pdf

[59] ARIANSEN MONCADA, Renzo Agusto; Rojas Díaz, José Iván. Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016. 2016.. De:

y que son difíciles de encontrar. Los beneficios en su implementación considerados como fortalezas son la capacidad de almacenamiento limitada a 64 caracteres, el procesamiento estándar y encriptación de valores originales[60]. Son funciones muy rápidas que no requieren un almacenamiento de más; como debilidad se encuentra la posibilidad de presentar colisiones, es decir, que se pueden duplicar posiciones de entradas de datos y generar problemas a la hora de la búsqueda y el hecho de no permitir registros de longitud variable[61].

A continuación, en la tabla 2 se relaciona un resumen de las fortalezas, debilidades y niveles de seguridad de los algoritmos simétricos, asimétricos más reconocidos y las funciones hash:

https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/348/TESIS_Ariansen_Rojas%20.pdf?sequence=1&isAllowed=y

[60] GUTIÉRREZ, Yesid Díaz, et al. Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos. *Redes de Ingeniería*, 2018, vol. 9, no 2, p. 82-87. https://revistas.udistrital.edu.co/index.php/REDES/article/view/14383

[61] SÁNCHEZ, Samuel; Domínguez, Pablo; Velásquez, Luis. Hashing: Técnicas y Hash para la Protección de Datos. *Universidad Tecnológica de Panamá, Grupo de Investigación*, 2018.

TABLA 2. COMPARATIVO FORTALEZAS, DEBILIDADES Y NIVELES DE SEGURIDAD DE LOS ALGORITMOS SIMÉTRICOS, ASIMÉTRICOS Y HASH

Algoritmo		**Fortalezas**	**Debilidades**	**Nivel de seguridad**
Simétricos	AES	• Procesamiento superior • Resistente a los análisis lineales y diferenciales • Tiene una capacidad para 80 bits de seguridad • Máximo de resistencia frente a ataques conocidos • Sencillez de diseño • Efectivo en ataques de fuerza bruta • Dificultad para invertir el algoritmo cifrado • Cifrado y descifrado de archivos y cifrado de contraseñas • Rápido y eficiente tanto en hardware como en software	• No cuenta con parámetros de borrado de emergencia • Comunicación de la clave	Alta
	IDEA	• Cifra archivos de cualquier tamaño con una sola llave y un cifrador determinado	• No cuenta con parámetros de borrado de emergencia • No muy efectivo en ataques de fuerza bruta	Medio

Fuente propia

TABLA 3. (CONTINUACIÓN)

Algoritmo		**Fortalezas**	**Debilidades**	**Nivel de seguridad**
	DES	• Cifrado y descifrado de archivos • Es mejor en hardware • Rapidez, facilidad de implementación y eficiencia	• Cifra menor cantidad de datos • Longitud de la clave muy corta • Inseguro y obsoleto	Baja
	RC5	• Algoritmo robusto e irrompible • Puede ser fácilmente implementado	• No muy efectivo en ataques de fuerza bruta • Clave insegura	Medio
Asimétricos	RSA	• Permite verificar la autenticidad del origen • Cifrado de mensajes, firma digital e intercambio de claves • Imposibilidad de factorizar números primos extremadamente grandes • Seguridad, longitud de clave variable • Significativamente seguro	• Alto costo	Alta
	Diffie-Hellman	• Significativamente seguro • Proporciona secreto directo perfecto	• Susceptible a ataques Man in the middle (MitM)	Media

	• Distribuye claves a más de 2 personas mediante sistemas de clave pública • Seguro en el intercambio de claves anónimas	• Necesita la verificación del usuario que remite para disminuir la manera en que puede ser vulnerado	
Hash	• Gasto computacional bajo • Evitan valores duplicados y que son difíciles de encontrar • Capacidad de almacenamiento limitada a 64 caracteres • Procesamiento estándar y encriptación de valores originales	• Posibilidad de presentar colisiones	Media

Fuente propia

Con todo lo anterior se puede concluir que cada uno de los algoritmos tiene cierto nivel de practicidad a la hora de cifrar archivos. Sin embargo, si se habla de algoritmos asimétricos se puede evidenciar que el AES es uno con gran capacidad y velocidad de cifrado y descifrado, siendo garantía de seguridad la longitud de su clave, es un algoritmo que no se puede romper en un tiempo razonable. En los algoritmos asimétricos se establece que el mas práctico es el RSA a pesar de ser más lento que los simétricos, proporciona un alto nivel de seguridad también gracias a la longitud de las claves, es un algoritmo casi imposible de corromper en la actualidad; es muy práctico en el cifrado de archivos y firma digital garantizando la integridad y confidencialidad de la información.

8. ANÁLISIS DE LAS IMPLICACIONES PRÁCTICAS DE LOS RESULTADOS OBTENIDOS EN INVESTIGACIONES ANTERIORES SOBRE LA EFICIENCIA DE LOS DIFERENTES MÉTODOS DE CIFRADO Y PROTECCIÓN DE LA INFORMACIÓN, Y HACER RECOMENDACIONES PARA SU USO EN ENTORNOS REALES

En los procesos de protección de la información, cifrado y autenticación de usuarios se hace un proceso de verificación de la identidad para poder acceder a la información o a la red, esta autenticación puede incluir la verificación de credenciales (usuario y contraseña) y verificación de factores adicionales como la ubicación, huella dactilar o reconocimiento facial. Esta autenticación permite que solo los usuarios autorizados puedan acceder, ayudando a proteger la privacidad y la integridad de los datos. Existen varios métodos de autenticación que dependen de los requisitos específicos de la red: Basado en contraseñas, autenticación de dos factores, biométrica, por token, por correo electrónico o mensaje, de estas las más seguras son las de 2 factores y la biométrica.

Otro elemento que influye es el control de acceso que gestiona los permisos y restricciones que tienen los usuarios para acceder a recursos en concreto, algunos de ellos pueden ser: Parches o actualizaciones de software, mejoramiento en el cifrado, fijación de errores de seguridad, proporcionar nuevas funciones de seguridad, copias de seguridad, protección de información, prevención de interrupciones, protección contra malware, seguridad en la nube y verificación de integridad de los datos.

Los mecanismos para el cifrado y protección de la información son los que se compararán, dentro de estos existen la criptografía de Hash, la firma digital, criptografía simétrica y asimétrica y algoritmos de detección de errores[62].

[62] CANTELI, Ana. Comunicaciones seguras, Técnicas, Cifrado de datos. 2023. De: https://www.openkm.com/es/blog/comunicaciones-seguras.html

8.1 FIRMA DIGITAL

Es una herramienta que se consolida en servicios, plataformas, hardware, software que permiten la autenticación e identificación de los usuarios antes de acceder a determinados recursos o transacciones. Se hace a través de niveles, el primero en el que se identifica mediante una contraseña que la persona misma conoce; el segundo corresponde a algo que se tiene, un objeto que solo la persona posee como una tarjeta de crédito; y el tercero, se hace mediante la verificación de rasgos físicos propios como la biometría, el caso de la huella dactilar es el más frecuente o el reconocimiento facial. Los niveles de seguridad dependen del trámite que se vaya a realizar. Este mecanismo garantiza la autenticidad, integridad y disponibilidad.

En la actualidad, la firma digital se utiliza ampliamente en entornos de Internet para verificar la autenticidad de los datos y garantizar que no hayan sido modificados. La firma digital se crea mediante un proceso criptográfico que establece una conexión única entre la información en cuestión y la persona que la firma. Esto nos permite estar seguros de que los datos provienen de la fuente original y no han sufrido cambios durante su transmisión o almacenamiento[63].

8.2 CRIPTOGRAFÍA SIMÉTRICA:

Algoritmo AES: Se basa en el tamaño de la llave y las rondas que realiza para el cifrado, entre mayor sea el tamaño de las llaves mayor será el número de rondas que debe realizar implicando un mayor número de operaciones. Cuando se llevan a cabo ataques contra este algoritmo, se emplea un método de búsqueda de clave conocida como "fuerza bruta". En este tipo de ataque, se busca exhaustivamente la clave utilizada, realizando repeticiones para cada tamaño de clave y las rondas correspondientes según la longitud

[63] MARTÍNEZ MOLANO, Valeria; RINCÓN CÁRDENAS, Erick. Problemas y desarrollo de la identidad en el mundo digital. *Revista chilena de derecho y tecnología*, 2021, vol. 10, no 2, p. 251-276. https://www.scielo.cl/scielo.php?pid=S0719-25842021000200251&script=sci_arttext

de la clave. Este proceso implica realizar una gran cantidad de operaciones, lo que lo convierte en una tarea que requiere mucho tiempo, especialmente cuando se distribuye entre varias computadoras. Es importante destacar que la fortaleza de este algoritmo se basa en el tamaño de la clave utilizada[64].

Los ataques hacia este algoritmo son computacionalmente imposibles, es por ello que la mayoría de ataques se centran en los dispositivos en los que se implementa AES buscando obtener datos que pueda dejar el algoritmo temporalmente en las memorias y que puedan ser utilizados para romper el algoritmo[39].

Algoritmo DES: Posee una longitud de clave corta (56 bits) considerado bastante inseguro pues facilita el rompimiento de la misma en menos de 24 horas. Es muy vulnerable a ataques de fuerza bruta; no es considerado un algoritmo débil sino con debilidad en la longitud de clave. Como respuesta surgió el 3DES con una longitud de 168 bits y el algoritmo IDEA con una longitud de clave de 128; este último está constituido por bloques de 64 bits en el que se ejecutan rondas de cifrado de 4 sub-bloques de 16 bits[65]

Frente Ataques Cibernéticos

En criptografía simétrica se emplea una única clave tanto para el cifrado como para el descifrado". la clave secreta es compartida tanto por el remitente como por el destinatario. El remitente codifica el mensaje mediante una clave antes de enviarlo al destinatario. la persona que recibe el mensaje utiliza la misma clave para decodificarlo y comprenderlo.

[64] MORI ACERO, Simón Wilmer. Optimización del algoritmo estándar de encriptación avanzada (AES) para la protección de la información. 2019.. De: https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1364/T037_43278620_T.pdf?sequence=1&isAllowed=y

[65] SERRATO LOSADA, Hernán Darío, et al. Comparación de métodos criptográficos para la seguridad informática.2019. https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

La criptografía simétrica tropieza con varios obstáculos a la hora de protegerse contra los ciberataques:

- Intercepción de clave simétrica: Cuando un atacante intercepta la clave simétrica durante la comunicación, puede usarla para descifrar mensajes cifrados y acceder a datos confidenciales.

- En los ataques de fuerza bruta, el proceso de descifrado implica intentar todas las combinaciones de claves imaginables para descifrar un mensaje cifrado. Esto puede suponer una dificultad para la criptografía simétrica si la clave no es lo suficientemente larga o compleja.

- Ataques de diccionario: Algunos ataques intentan adivinar la clave utilizando diccionarios de palabras comunes o combinaciones de caracteres predefinidas. el mensaje se puede descifrar si la clave no es segura y está en el diccionario utilizado por el atacante.

Se aplican varias técnicas de seguridad para mitigar estos riesgos y proteger la criptografía simétrica contra ataques cibernéticos:

- La longitud y complejidad de la clave: Las claves largas y complejas son difíciles de descifrar mediante fuerza bruta o ataques de diccionario.

- Cambios de clave frecuentes: Cambiar las claves con regularidad reduce el tiempo que una clave es vulnerable si se ve comprometida

- Métodos de cifrados sólidos: Emplear algoritmos criptográficos fiables y ampliamente reconocidos, como AES (*Advanced Encryption Standard*), cuya seguridad se ha probado exhaustivamente.

- Para salvaguardar la comunicación, es fundamental emplear protocolos seguros de intercambio de claves como TLS (*Transport Layer Security*) para proteger la clave simétrica compartida entre las partes.

Si bien la criptografía simétrica proporciona una forma eficaz de salvaguardar los datos, es esencial incorporar medidas de seguridad complementarias para hacer frente a las posibles amenazas que plantean los ciberataques.

"AES es actualmente uno de los algoritmos de cifrado simétrico más importantes y utilizados en todo el mundo, sin embargo, el modo de cifrado más recomendable es AES-GCM ya que incorpora AEAD. Cuando nosotros establecemos una conexión TLS 1.2 o TLS 1.3, el canal de datos casi siempre hace uso de AES-128-GCM o AES-256-GCM, ya que son los dos algoritmos de cifrado simétricos más utilizados por las conexiones HTTPS." [66]

Frente Ataques de la IA:

Los algoritmos simétricos, como AES (*Advanced Encryption Standard*), son robustos y eficientes en términos de rendimiento. Para resistir ataques basados en IA, se pueden aplicar las siguientes estrategias:

- Longitud de clave sólida: Aumentar la longitud de la clave puede hacer que sea más difícil para los modelos de IA realizar ataques de fuerza bruta.

- Modos de operación seguros: Utilizar modos de operación seguros y autenticación de mensajes para proteger contra ataques como cifrado elegido y manipulación de mensajes.

[66] LÓPEZ, Alberto. Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. 2024 De: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/#373279-criptografia-simetrica-o-criptografia-de-una-clave

- Actualizaciones periódicas de claves: Cambiar las claves de forma regular puede ser beneficioso para resistir ataques a largo plazo.

- Implementar técnicas de protección de la clave: Como el uso de claves derivadas de contraseña o el almacenamiento seguro de las claves.

"Los ataques por fuerza bruta son el enemigo real de los algoritmos de criptografía simétrica, hay que tener en cuenta que estos algoritmos son públicos y que la fuerza de los mismos depende directamente de lo complejo que sea el algoritmo internamente, y también de la longitud de la clave empleada para evitar estos ataques."[67]

8.3 CRIPTOGRAFÍA ASIMÉTRICA:

RSA: Es el más usado y útil para cifrar datos y firmas digitales, es muy seguro debido a la longitud de las claves que utilizan la factorización de números, su funcionamiento se basa en que cada persona genera su par de claves cuando necesita cifrar algún mensaje. Dentro de los ataques más conocidos contra el algoritmo están los de factorización que encuentra los factores primos que forman el módulo para encontrar el módulo vacío y el inverso de la llave; el ataque por paradoja del cumpleaños, que indica que dos personas de una habitación cumplen años el mismo día, lo que requiere que en la habitación haya un mayor número de personas para que la probabilidad aumente, en este caso el atacante conoce las claves públicas, divide en 2 y forma dos cuerpos, una que se conoce como zona inferior y otra como zona superior, cifra un número y así sucesivamente continúa aumentando en uno hasta encontrar la colisión entre los números de las dos zonas. Otra forma es el cifrado cíclico, que rompe el secreto del mensaje que se cifra aún

[67] LÓPEZ, Alberto. Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. 2024 De: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/#373279-criptografia-simetrica-o-criptografia-de-una-clave

sin tener la clave privada realizando una serie de cifrados utilizando el valor del criptograma, el módulo y la llave pública[68].

La seguridad del algoritmo radica en el problema de la factorización de números enteros, algo que les da ventajas frente a otros sistemas de clave pública en cuestiones de autenticación, es muy utilizado en el mundo real lo que ha hecho que haya sido probada su seguridad. Tiene desventajas en cuanto a la lentitud de cifrado.

Frente Ataques Cibernéticos

En la criptografía asimétrica, también llamada criptografía de clave pública, se utilizan dos claves vinculadas matemáticamente: Una clave pública y una clave privada. Explicaremos el proceso de la criptografía asimétrica en caso de un ciberataque:

- Los mensajes cifrados se crean utilizando la clave pública del destinatario para codificar el mensaje. Esta clave es bien conocida y puede divulgarse libremente. el destinatario sólo puede descifrar el mensaje si tiene la clave privada que le corresponde después de haber sido cifrado.

- La clave privada debe mantenerse confidencial y sólo conocerla su propietario. Cuando una persona no autorizada obtiene la clave privada, puede descifrar todos los mensajes que fueron cifrados con la clave pública correspondiente.

- En criptografía asimétrica, un atacante puede realizar un ataque de intermediario, donde secretamente reemplaza la comunicación entre el remitente y el destinatario con su propio mensaje y pretende ser cualquiera de ellos. Para evitar este tipo de ataque, es esencial que se verifiquen las claves públicas para confirmar que provienen del destinatario previsto.

[68] SOLÍS ORNELAS, Carlos Alejandro. Propuesta de un algoritmo de cifrado híbrido basado en matrices de rotación cuaterniónica y el estándar RSA.

- La gestión de claves es crucial en la criptografía asimétrica. Esto abarca la creación de claves seguras, la custodia de claves privadas y la eliminación de claves comprometidas.

- Para protegerse contra los ataques cibernéticos, es fundamental emplear algoritmos criptográficos sólidos y ampliamente reconocidos, similares a los utilizados en la criptografía simétrica. Uno de los algoritmos asimétricos más utilizados son RSA y ECC (*Elliptic Curve Cryptography*).

La criptografía asimétrica permite una comunicación en línea segura al permitir que las partes intercambien información confidencial sin tener que revelar una clave secreta compartida. Es vital salvaguardar las claves privadas y verificar las claves públicas para evitar ataques cibernéticos.

“Hay que tener en cuenta que la criptografía de clave pública lo cierto es que se suele usar en el tráfico de correo electrónico. Por ejemplo, como en el método de cifrado estándar S/MIME, en las firmas digitales o hasta en los protocolos criptográficos como SSL/TLS, SSH y HTTPS. Además de esto, lo cierto es que también se pueden combinar con métodos simétricos.” [69]

Frente Ataques de la IA:

Los algoritmos asimétricos, como RSA y ECC, son esenciales para la criptografía de clave pública. Para resistir ataques basados en IA:

- Longitudes de clave mayores: Al igual que en los algoritmos simétricos, usar claves más largas aumenta la resistencia a ataques de fuerza bruta.

[69] LÓPEZ, Alberto. Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. 2024 De: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/#373279-criptografia-simetrica-o-criptografia-de-una-clave

- Uso de curvas elípticas seguras: En el caso de ECC, elegir curvas elípticas seguras es fundamental para prevenir ataques criptográficos.

- Protección contra ataques cuánticos: Dado que los algoritmos cuánticos pueden amenazar a los algoritmos asimétricos existentes, es importante considerar algoritmos resistentes a la computación cuántica, como aquellos basados en retículas.

- Implementar técnicas de protección de la clave privada: como el uso de módulos de seguridad de hardware.

"La fortaleza del sistema por el cual es seguro este tipo de algoritmo asimétrico, es que está basado en funciones matemáticas las cuales son fáciles de resolver en un sentido, pero que su resolución en sentido contrario es extremadamente complicada, a menos que se conozca la clave."[70]

8.4 HASH: Se utiliza para proteger contraseñas no guardadas, el algoritmo se aplica a la contraseña que se introduce para compararla con la almacenada, es utilizado en todos los sistemas webs con autenticación y en caso de olvido de la contraseña esta se debe resetear pues no hay forma de que el servicio la proporcione. Este algoritmo también tiene usos para detectar malware en canciones o películas por derechos de autor con bases de datos públicas. Es un algoritmo asegura la integridad de los mensajes, en este caso si los hashes son idénticos significa que la comunicación ha sido segura sin alteración de datos.

[70] LÓPEZ, Alberto. Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. 2024 De: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/#373279-criptografia-simetrica-o-criptografia-de-una-clave

El rendimiento de estos algoritmos depende del tamaño de los datos de entrada y la capacidad de procesamiento del hardware empleado, entre más complejo mayor será el impacto en el rendimiento.

Función unidireccional: “Las funciones hash son funciones unidireccionales, lo que significa que es prácticamente imposible de ingeniería inversa de los datos de entrada del valor hash. Esto los hace ideales para almacenar contraseñas de forma segura. Cuando un usuario crea una contraseña, el valor hash se almacena en lugar de la contraseña real. Cuando el usuario inicia sesión, la contraseña que ingresa se ha puesto y se compara con el valor de hash almacenado. Si coinciden, se le otorga acceso al usuario.”[71]

Frente Ataques Cibernéticos

Un algoritmo hash es una forma de transformar datos en un código corto que no cambia los datos en sí. Estos algoritmos se aplican en numerosas aplicaciones de seguridad, incluida la integridad de datos, la autenticación y la protección con contraseña. Describiré el proceso de un algoritmo hash en el caso de un ciberataque:

- Se emplean algoritmos hash para garantizar la integridad de los datos: El valor hash cambiará si se manipulan los datos, esto permite identificar cualquier manipulación de datos durante la transmisión o el almacenamiento.

- Protección con contraseña: en lugar de almacenar contraseñas en texto plano el sistema verifica la contraseña del usuario mediante un hash y comparándola con el hash almacenado. Las contraseñas están protegidas en caso de una violación de la base de datos, ya que el atacante solo tendría acceso a los valores hash en lugar de las contraseñas reales.

[71] CAPITAL, Faster. Algoritmos de cifrado asegurando datos explorar algoritmos de cifrado. De: https://fastercapital.com/es/contenido/Algoritmos-de-cifrado--asegurando-datos--explorar-algoritmos-de-cifrado.html#hash-funciones

- Cuando dos conjuntos distintos de datos generan el mismo valor hash, se conoce como ataque de colisión: Los algoritmos hash tienen como objetivo reducir la probabilidad de colisiones, pero aun así pueden ocurrir en situaciones excepcionales, los atacantes pueden utilizar ataques de colisión para manipular datos o dañar sistemas.

- Un ataque de preimagen intenta encontrar un conjunto de datos que produzca un valor hash específico, el objetivo de un segundo ataque de preimagen es descubrir un conjunto de datos diferente que genere el mismo valor hash que un conjunto de datos determinado. Los algoritmos de hash criptográfico se crean para resistir este tipo de ataques, pero los avances en la tecnología podrían hacer que estos ataques sean más factibles en el futuro.

Para reducir los peligros de los ciberataques dirigidos a algoritmos hash, es recomendable utilizar algoritmos criptográficos confiables y actualizados, y seguir buenas prácticas de seguridad, como agregar una cadena aleatoria de caracteres a las contraseñas antes de aplicar hash y usar funciones hash iterativas para aumentar la resistencia contra los ataques. Además, es esencial monitorear y actualizar constantemente los sistemas para garantizar la seguridad continua de los datos en medio de amenazas cibernéticas en continua evolución.

“Por otra parte, las funciones criptográficas hash se utilizan también para asegurar la “integridad de los mensajes”. En pocas palabras, para estar seguros de que algunas comunicaciones o archivos no fueron alterados de alguna forma, se pueden examinar los hashes creados antes y después de la transmisión de los datos. Si los dos hashes son idénticos, significa que no ha habido ninguna alteración.” [72]

[72] DONOHUE, Brian. ¿Qué Es Un Hash Y Cómo Funciona? De: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Frente Ataques de la IA:

Las funciones hash, como SHA-256, son cruciales para la integridad de los datos. Para resistir ataques basados en IA:

- Longitudes de hash más largas: Utilizar longitudes de hash más largas puede hacer que sea más difícil para los modelos de IA realizar ataques de colisión.

- Sal y estiramiento de contraseñas: En el contexto de contraseñas, agregar sal a las contraseñas y aplicar funciones de estiramiento puede aumentar la resistencia a los ataques, añadiendo información aleatoria al hash para dificultar los ataques de preimagen.

8.5 INVESTIGACIONES QUE EVALÚAN LOS MÉTODOS DE CIFRADO

Jhonatan Cabrera Jara[73], realizó un estudio comparativo entre los algoritmos AES y Rivest, Shamir & Adleman (RSA), en el que se establecería la diferencia entre ambos, encontrando que ambos algoritmos son eficientes dependiendo de las circunstancias en las que se apliquen, el primero es muy efectivo con archivos pesados algo que no tiene el RSA, mientras que el RSA es computacionalmente más difícil de romper; con el AES se pueden interceptar las claves en el camino, siendo esta su debilidad. Con esto en la investigación específica que los dos algoritmos se complementan llevando a que sea muy efectivo encriptar archivos pesados con AES y cifrar la clave que se debe compartir con RSA, debido a que RSA tiene la dificultad de generar una clave mínima de 1024 bits.

En este sentido al ser dos tipos de cifrado diferentes AEX (simétrico) y RSA (asimétrico), no se puede establecer si uno es mejor que otro pues ambos son óptimos según su

[73] CABRERA JARA, Heber Jhonatan. Estudio comparativo de los algoritmos de encriptación advanced encryption standard (aes) y rivest, shamir & adleman (rsa). 2018. http://redi.unjbg.edu.pe/handle/UNJBG/3193

funcionalidad, que también es dependiente de los tiempos para cifrar o descifrar y del computador que se utilice.

Edisson Esteban Alvarado Prado[74], realizó un estudio de eficiencia de los algoritmos criptográficos RSA, AEX, IDEA y RC4, teniendo en cuenta sus características principales, eficiencia y beneficios frente a amenazas. En la evaluación de fortalezas encontró que tanto el RSA como el AES son muy seguros cuando ocupan más bits, el IDEA es seguro si la clave no es débil y el RC4 es inseguro. En las características de seguridad, el RSA necesita hallar los factores de un número compuesto bastante grande; el AES, necesita un número de intentos que va desde 2^{217} hasta 2^{255} veces; el IDEA tiene 8 vueltas por lo que los ataques de análisis diferencial no se pueden hacer después de la primera vuelta; y el RC4 no tiene ninguna. En la dificultad de adivinar la clave solo el RC4 no presenta ninguna dificultad. En los ataques representativos, el RSA se vulnera con cifrado cíclico y por factorización; el AES por ataques de fuerza bruta y de canal lateral, el IDEA por criptoanálisis diferencial y de fuerza bruta, y el RC4 de fuerza bruta y FMS.

En este estudio se encontró que el algoritmo RSA tiene las mejores características y es muy eficiente contra los ataques; el RC4 es fácil de implementar y requiere un mínimo de espacio, sin embargo, no proporciona la seguridad deseada; el IDEA depende de la clave que se use y el AES es funcional respecto al tamaño del disco y soporta ataques de fuerza bruta. En conclusión, cada algoritmo es funcional de acuerdo a lo que se necesite, pero el RSA es el mejor candidato al cifrar respecto a los demás, aunque ocupa un mayor tamaño de disco.

Denys Ivan Capuñay Puican75, realizó un análisis comparativo de los algoritmos criptográficos usados para redes privadas virtuales teniendo en cuenta que el problema

[74] ALVARADO PRADO, Edisson Esteban. Estudio de eficiencia y eficacia de los algoritmos criptográficos RSA, AES, IDEA y RC4 en la seguridad informática. https://repository.unad.edu.co/handle/10596/35362
[75] CAPUÑAY PUICAN, Denys Ivan. Análisis comparativo de algoritmos criptográficos para redes privadas virtuales. 2016. https://repositorio.uss.edu.pe/handle/20.500.12802/2696

principal radica en asegurar la seguridad e integridad de la información al conectarse a otro equipo de forma remota. Seleccionó los algoritmos AES y DES, evaluando cada uno en una red implementada. En los estudios realizo captura de tráfico en redes privadas virtuales determinando que AES es divide los datos en un mayor número de paquetes en un menor tiempo comparado con el otro; de los paquetes encriptados ambos algoritmos usan igual número, pero AES desencripta mas en menor tiempo, con menos recursos. AES tiene un mejor protocolo de encriptamiento en tiempo, paquetes de envío, paquetes de desencriptación, paquetes de encapsulación y de desencapsulación.

Jhonny Moisés Sánchez Vallejos76, realizó un análisis de técnicas de encriptación de datos a través de un analizador de paquetes en máquinas virtuales bajo la plataforma Linux haciendo pruebas con transferencias de archivos en distintos escenarios. Comparó el algoritmo RSA con 2048 bits de clave con cifrado AES de 256 bits con el algoritmo RSA de 1024 bits de clave con cifrado AES de 128 bits; siendo más efectiva la primera; concluyendo que es necesario adoptar ambas técnicas de encriptación para lograr un alto nivel de eficiencia en velocidad de tiempo de procesamiento de encriptación de los datos transmitidos; es una técnica difícil de vulnerar.

Con las anteriores investigaciones se puede diferir que tanto el algoritmo simétrico AES como el asimétrico RSA, son muy efectivos, ambos tienen limitaciones y ventajas. El primero es más rápido y eficiente en el manejo de grandes cantidades de datos mientras que el segundo es eficaz para comprobar la autenticación de la identidad de las partes o en el cifrado de claves usadas por AES. Es así como se concuerda en que la combinación de AES y RSA crean métodos más completos y robustos, son efectivos y seguros para la protección de la información; si se utilizan ambos aprovechando sus fortalezas se pueden asegurar los datos y hacer una correcta verificación de la identidad y la autorización de cada una de las partes que se involucran.

[76] SÁNCHEZ VALLEJOS, Jhonny Moisés. Técnicas de encriptación para mejorar la seguridad en la transferencia de archivos en un entorno fiable. 2017. https://repositorio.uss.edu.pe/handle/20.500.12802/4060

8.6 RECOMENDACIONES PRÁCTICAS PARA USO EN ENTORNOS REALES

Dimensiones como la seguridad de la información son dependientes de la criptografía que ha ido evolucionando hasta su estado actual dividiéndose en criptografía simétrica y asimétrica, aunque también se pueden mencionar las funciones hash; se han identificado sus características, ventajas y debilidades, estableciendo que han llegado a coexistir y a tener distintos usos y aplicaciones llegando a combinarse dando paso a una criptografía híbrida que se basa en la colaboración de ambos enfoques. Existen variedad de aplicaciones y herramientas que se pueden encontrar para aplicar técnicas criptográficas, algunas de ellas gratuitas basadas en algoritmos no patentados[77].

Los métodos analizados en este trabajo como ya se ha observado proporcionan altos niveles de seguridad, sin embargo, es muy común preguntarse cuál es el mejor y cuándo usarlo. Al respecto, se puede establecer que cada método y algoritmo tiene pros y contras, además de que tienen escenarios adecuados para su uso. En el caso de los algoritmos de intercambio de claves de cifrado la elección depende de las limitaciones de velocidad, costo e interoperabilidad. Algoritmos como el RSA es utilizado, por ejemplo en muchos protocolos, para funciones de cifrado y firma digital, navegadores web para garantizar conexiones seguras a través de redes inseguras, correos electrónicos, VPN, comunicaciones y chat, programas de software y sistemas de TI. Cabe resaltar que es muy recomendable combinar algunos de los métodos, por ejemplo, el RSA es combinado con otros esquemas de cifrado; es muy común utilizarlo para cifrar la clave simétrica de algoritmos de clave simétrica.

El algoritmo RSA con llave de 2048 bits para clave pública es combinado con el algoritmo Hash para proteger la integridad de la información en muchas páginas web, pues

[77] NAVAS DAMAS, Manuel. Criptografía simétrica y asimétrica. 2023. De: https://crea.ujaen.es/bitstream/10953.1/19494/1/NAVAS_DAMAS%2c%20MANUEL_INFORM%c3%81TICA_TFM.pdf

garantiza una negociación cliente – servidor verificando la autenticidad de la llave pública con la que se cifran los datos[78].

Los algoritmos asimétricos tienen el inconveniente de ser computacionalmente menos eficientes que los simétricos porque son muy lentos para cifrar altos volúmenes de datos, lo que requiere que deba utilizarse en ciertos casos los algoritmos simétricos con funciones hash para sacar mayor provecho en cifrado de volúmenes de datos pequeños. De los algoritmos de este tipo más reconocidos el RSA es el más fácil de implementar siendo uno de los más utilizados, el DF es utilizado para proteger conexiones, donde la clave es de un solo uso siendo desechada al desconectarse ambos extremos[79].

[78] ROJAS DÍAZ, José Iván; Ariansen Moncada, Renzo Agusto. Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016. 2016. https://renati.sunedu.gob.pe/handle/sunedu/2816156

[79] JUST CRYPTOGRAPHY. Funcionamiento de los algoritmos asimétricos y la firma digital. https://justcryptography.com/funcionamiento-de-los-algoritmos-asimetricos-y-la-firma-digital/

9. CONCLUSIONES

Durante el desarrollo de esta investigación, me ha permitido adentrarme en el mundo de la criptografía, donde he explorado a fondo el algoritmo simétrico, asimétrico y Hash. A través de la investigación de fuentes especializadas, he identificado y analizado detenidamente sus características distintivas, ventajas y desventajas. Esta base de conocimiento sólido es esencial para el posterior análisis comparativo y la toma de decisiones informadas sobre la elección de algoritmo en situaciones prácticas.

Y este nos ha permitido llevar a cabo una comparación exhaustiva de los algoritmos simétricos, asimétricos y Hash. A través de una revisión sistemática de la literatura, hemos identificado sus fortalezas y debilidades, centrándonos en la seguridad y el rendimiento de cada uno. Este análisis nos ha proporcionado información valiosa para determinar cuál de estos algoritmos es más práctico y adecuado para diversas aplicaciones y entornos.

Así mismo hemos explorado las implicaciones prácticas de los resultados de investigaciones previas relacionadas con la eficiencia de los métodos de cifrado y protección de la información. Basándonos en estos hallazgos y en nuestra comprensión de los algoritmos, hemos formulado recomendaciones concretas para su implementación en situaciones del mundo real. Estas recomendaciones están destinadas a proporcionar directrices sólidas para la selección y aplicación de algoritmos de cifrado en entornos prácticos, con el fin de garantizar la seguridad de la información en un entorno digital en constante evolución.

Esta investigación ha arrojado luz sobre la importancia de la criptografía y ha proporcionado una base sólida para la toma de decisiones informadas en cuanto a la selección de algoritmos criptográficos. Los algoritmos AES y RSA han surgido como destacados en términos de seguridad y eficiencia, y la combinación de ambos puede proporcionar un alto nivel de seguridad en entornos del mundo real. Es esencial

comprender las fortalezas y debilidades de estos algoritmos para garantizar la confidencialidad, integridad y protección de los datos en un entorno digital en constante cambio.

10. RECOMENDACIONES

Al implementar cualquier método de cifrado es importante determinar qué es lo que se quiere lograr con ellos para así mismo evaluar cual puede llegar a ser el más eficaz y que más conviene a lo que se necesita. Todos los métodos de cifrado pueden ser una solución bastante eficiente para la protección de la información y contra el acceso no autorizado y otras amenazas.

Se debe reconocer que los algoritmos analizados en la presente monografía, aunque actúan y se ejecutan de manera distinta, tienen las mismas finalidades y su uso depende de la aplicación o la utilidad que se les quiera dar.

Al hablar de requisitos de seguridad se deben considerar factores como el sector, la estructura, el tamaño, la tecnología en cuanto a software y hardware con la que se opera para garantizar la información confidencial, financiera, los datos sensibles, la restricción y el acceso a sistemas confidenciales.

Se debe considerar que hay condiciones que favorecen la efectividad de los algoritmos que se utilicen, tales como el conocimiento de las políticas de seguridad asegurándose de que todos las comprendan y la capacitación en requisitos y protección de la información.

El uso en entornos reales de los algoritmos criptográficas debe ser analizado desde las herramientas de hardware y software con las que se cuenta y las condiciones de seguridad y rapidez, en este sentido, se recomienda usar RSA para incrementar los niveles de seguridad y AES en el caso de requerir un cifrado y descifrado más rápido.

BIBLIOGRAFÍA

ALMENARES MENDOZA, Florina, and Patricia Arias Cabarcos. *Estudio de la eficiencia de protocolos y algoritmos de seguridad en Android*. BS thesis. 2015.

ALVARADO PRADO, Edisson Esteban. Estudio de eficiencia y eficacia de los algoritmos criptográficos RSA, AES, IDEA y RC4 en la seguridad informática. https://repository.unad.edu.co/handle/10596/35362

ARÉVALO-RODRÍGUEZ, Anderson Smith, Diana Marcela Hurtado-Gómez, and Gilber Jhon Galindo-Sierra. "Algoritmo internacional de cifrado de datos (IDEA) que utiliza la variante de cifrado SHA-256." *Revista Vínculos* 19.2 (2022). De: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/20826/19136

ARIANSEN MONCADA, Renzo Agusto, and José Iván ROJAS DÍAZ. "Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016." (2016)... De: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/348/TESIS_Ariansen_Rojas%20.pdf?sequence=1&isAllowed=y

ASTUDILLO QUINTERO, Pablo Vicente. Implementación de una red de mezcla utilizando encriptación de Paillier para votaciones electrónicas. 2023

BALBÁS GUTIÉRREZ, David. "Ataques al criptosistema RSA." (2019).

BARREIRO MONT, Claudia. *Desarrollo de una plataforma de criptoanálisis basada en medidas de consumo sobre el algoritmo de encriptación DES*. BS thesis. Universitat Politècnica de Catalunya, 2019.

BAZURTO, Alicia Andrade. *Características y aplicaciones de las funciones resumen criptográficas en la gestión de contraseñas*. 2019. Tesis Doctoral. Universitat d'Alacant/Universidad de Alicante.: https://rua.ua.es/dspace/bitstream/10045/96849/1/tesis_alicia_andrade.pdf

CABRERA JARA, Heber Jhonatan. Estudio comparativo de los algoritmos de encriptación advanced encryption standard (aes) y rivest, shamir & adleman (rsa). 2018. http://redi.unjbg.edu.pe/handle/UNJBG/3193

CANTELI, ANA. Comunicaciones seguras, Técnicas, Cifrado de datos. 2023. De: https://www.openkm.com/es/blog/comunicaciones-seguras.html

CAPUÑAY PUICAN, Denys Ivan. Análisis comparativo de algoritmos criptográficos para redes privadas virtuales. 2016. https://repositorio.uss.edu.pe/handle/20.500.12802/2696

CARRERA ALBÁN, Thruman Wladimir. Análisis y comparación de dos algoritmos de cifrado simétrico en plataformas Windows. 2016. UEES. De: http://repositorio.uees.edu.ec/bitstream/123456789/1428/1/MATI_PaperFinal_Thruman Carrera.pdf

CAPITAL, Faster. Algoritmos de cifrado asegurando datos explorar algoritmos de cifrado. 2023 De: https://fastercapital.com/es/contenido/Algoritmos-de-cifrado--asegurando-datos--explorar-algoritmos-de-cifrado.html#hash-funciones

DAZA, Doris Maritza Ruano, et al. Análisis del rendimiento entre los algoritmos simétricos de Blowfish y AES. *Revista Vínculos: Ciencia, tecnología y sociedad*, 2021, vol. 18, no 2, p. 2. Available from: https://geox.udistrital.edu.co/index.php/vinculos/article/view/17632/18723

Donohue, Brian. ¿Qué Es Un Hash Y Cómo Funciona? De: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

FERNANDEZ TOLEDO, Jesús. Criptografia. 2020. <Criptografía simétrica. https://jesusfernandeztoledo.com/criptografia-simetrica/>.

GARCÍA MARTÍNEZ, Moisés. Estudio de mapeos caóticos discretos y su aplicación en criptografía. 2015. https://repositorio.ipicyt.edu.mx/handle/11627/4030

GUEVARA SAMANIEGO, Vanessa Alexandra. *Desarrollo de un algoritmo para romper por fuerza bruta al Simplified Data Encryption Standard (S-DES) mediante el uso de computación*

GUTIÉRREZ, Yesid Díaz, et al. Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos. *Redes de Ingeniería*, 2018, vol. 9, no 2, p. 82-87. https://revistas.udistrital.edu.co/index.php/REDES/article/view/14383

GITLAN, Dionisie. Su guía única de algoritmos de cifrado. 2024 De: https://www.ssldragon.com/es/blog/tipos-algoritmos-cifrado/

GITLAN, Dionisie. Cifrado vs. Hashing: ¿Cuál es la diferencia? 2024 De: https://www.ssldragon.com/es/blog/cifrado-y-hashing/

HERRAMIENTAS WEB PARA LA ENSEÑANZA. Protocolos de comunicación DES. 2021. https://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

HP. ¿Cuáles son los diferentes tipos de cifrado? 2021. https://www.hp.com/co-es/shop/tech-takes/cuales-son-los-diferentes-tipos-de-cifrado#:~:text=Los%20tres%20principales%20tipos%20de,consumidores%20utilizan%20todos%20los%20d%C3%ADas.

HUIDOBRO, José Manuel. Introducción a la protección de la información. “criptografía”.

JUST CRYPTOGRAPHY. Funcionamiento de los algoritmos asimétricos y la firma digital. https://justcryptography.com/funcionamiento-de-los-algoritmos-asimetricos-y-la-firma-digital

JYOTI, Gaba y Kumar, Mukesh. Implementation of Steganography Using CES Technique. (Conference Paper) [En línea]. The Technological Institute of Textile & Sciences, Department of Computer Engineering, IEEE Second International Conference on Image Information Processing (ICIIP), 2013. Págs. 395-399. Disponible en: https://www.researchgate.net/publication/261458593_Implementation_of_steganography_using _CES_technique

KRIPTÓN SOLID. Comparación de los algoritmos de intercambio de claves Diffie-Hellman y RSA. De: https://kryptonsolid.com/comparacion-de-los-algoritmos-de-intercambio-de-claves-diffie-hellman-y-rsa/

LARA PEREZ, Martha Lucia, et al. La computación cuántica y las implicaciones sobre la criptografía moderna. https://repository.unad.edu.co/handle/10596/28230

LEYVA BORGES, Maria Esther. *Creación de un procedimiento para atacar la seguridad del RSA*. 2019. Tesis Doctoral. Universidad Central “Marta Abreu” de Las Villas.: https://dspace.uclv.edu.cu/bitstream/handle/123456789/12056/AAB.%20Tesis.%20Criptoanalisis.pdf?sequence=1&isAllowed=y

LUMBIARRES LÓPEZ, Rubén. "Generación de falsas claves criptográficas como medida de protección frente a ataques por canal lateral." (2015).
Luque Lodeiro, Rubén, et al. Blockchain: Estado del arte, tendencias y retos. 2020.

LÓPEZ, Alberto. Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. 2024 De: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/#373279-criptografia-simetrica-o-criptografia-de-una-clave

MAÑAS, José Antonio. GUÍA DE SEGURIDAD (CCN-STIC-401). GLOSARIO Y ABREVIATURAS. 2016.
MARCOS, Manuel Gavira. "Zygmunt Bauman y David Lyon. Vigilancia líquida 2013. Barcelona: Paidos, 176 pp." *Encrucijadas: Revista Crítica de Ciencias Sociales* 16 (2018): 17

MARÍ SALVADOR, Noelia. *Una propuesta híbrida para el criptoanálisis RSA*. Diss. Universitat Politècnica de València, 2018.

MARTÍNEZ MOLANO, Valeria; RINCÓN CÁRDENAS, Erick. Problemas y desarrollo de la identidad en el mundo digital. *Revista chilena de derecho y tecnología*, 2021, vol. 10, no 2, p. 251-276. https://www.scielo.cl/scielo.php?pid=S0719-25842021000200251&script=sci_arttext

MATTELART, Armand, and André Vitalis. *De Orwell al cibercontrol*. Editorial Gedisa, 2015

Medina Velandia, Lucy Noemy. Criptografía y mecanismos de seguridad. 2017. https://digitk.areandina.edu.co/handle/areandina/1423

MÉNDEZ NARANJO, Pablo Martí. 2015. Nuevo Algoritmo Criptográfico con la Incorporación de la Estenografía en Imágenes. (Tesis)(Maestría). [En línea]. Escuela Superior Politécnica de Chimborazo, Posgrado y Educación Continua. Riobamba. 2015. págs. 13-50Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/4374/1/20T00628.pdf

Mendoza, Julio César. "Demostración de cifrado simétrico y asimétrico." *Ingenius: Revista de Ciencia y Tecnología* 3 (2008): 46-53. https://dialnet.unirioja.es/servlet/articulo?cod

MORI ACERO, Simón Wilmer. Optimización del algoritmo estándar de encriptación avanzada (AES) para la protección de la información. 2019. De: https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1364/T037_43278620_T.pdf?sequence=1&isAllowed=y

MOYA, José Manuel. Introducción a la Protección de la Información. “Criptografía” (Paper). [En línea]. Colegio Oficial de Ingenieros de Telecomunicación, Telecomunicaciones, In Escrituras silenciado: paisaje como cistografía, 2013. págs. 495-513.
http://www.academia.edu/21679789/INTRODUCCION_A_LA_PROTECCIÓN_DE_LA_INF ORMACIÓN._CRIPTOGRAFÍA_

MUNDT BRICEÑO, Carlos André. *Análisis comparativo entre algoritmos simétricos orientados al IOT*. Diss. Universidad Andrés Bello, 2018. http://repositorio.unab.cl/xmlui/handle/ria/13569

MUÑOZ-MENDOZA, Luís D., Jodamia U. MURILLO-ROSADO, and Cristian R. Amen-Chinga. "Algo sobre la firma electrónica en el contexto actual." *Polo del Conocimiento* 2.7 (2017): 1016-1028. http://polodelconocimiento.com/ojs/index.php/es/article/view/322

NAVAS DAMAS, Manuel. Criptografía simétrica y asimétrica. 2023. De: https://crea.ujaen.es/bitstream/10953.1/19494/1/NAVAS_DAMAS%2c%20MANUEL_INFORM%c3%81TICA_TFM.pdf

Oficina de Seguridad del Internauta. Tipos de cifrado para proteger nuestra información en internet. . 2019. <De: https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad>.

PAGUAY CUVI, Mario Humberto. "Análisis de algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de ingeniería en sistemas de la ESPOCH." (2015).

PENAZZI, Daniel. CRIPTOGRAFIA DE CLAVE SIMETRICA: AES (Notas de curso para las Jornadas de Criptografía y Códigos Auto correctores.) [En línea]. Universidad Nacional de Córdoba, Facultad de Matemática, Astronomía y Física. Mar de Plata, 2006. págs. 3-10. Disponible en: http://www.famaf.unc.edu.ar/~penazzi/17NovAESMardePlata.pdf

RÍOS, Lucas Giraldo. Ciberseguridad y redes sociales. *Revista de las Fuerzas Armadas*, 2021, no 257, p. 69-88.

RIQUELME FAÚNDEZ, Edgardo Andrés. Algoritmos genéricos para resolver el logaritmo discreto y sus aplicaciones. 2023

RODRÍGUEZ RODRÍGUEZ, Jefferson Stivens, et al. Operadores genéticos aplicados a la criptografía simétrica. https://repository.udistrital.edu.co/handle/11349/28192

RODRÍGUEZ, Ernesto Godínez, et al. AES estándar mundial de encriptado. https://www.researchgate.net/profile/Ernesto-Godinez/publication/362850594_ARTICULO_NO_78_ARTICULO_XX_CONGRESO_NACIONAL_DE_INGENIERIA_ELECTROMECANICA_Y_DE_SISTEMAS_CNIES_2021_CIUDAD_DE_MEXICO_MEXICO_NOVIEMBRE_2021_1_AES_estandar_mundial_de_encriptado/links/6303d48ceb7b135a0e53d3d4/ARTICULO-NO-78-ARTICULO-XX-CONGRESO-NACIONAL-DE-INGENIERIA-ELECTROMECANICA-Y-DE-SISTEMAS-CNIES-2021-CIUDAD-DE-MEXICO-MEXICO-NOVIEMBRE-2021-1-AES-estandar-mundial-de-encriptado.pdf

ROJAS DÍAZ, José Iván; Ariansen Moncada, Renzo Agusto. Implementación de protocolo de cifrado TLS para mejorar la seguridad de las comunicaciones en la capa de transporte 2016. 2016. https://renati.sunedu.gob.pe/handle/sunedu/2816156

RUIZ AZOFRA, Eduardo. Técnicas criptográficas utilizadas en" MALWARE. 2015.

ROCA, Busó Seguridad Informática: Criptografía. Minubeinformatica.Com. De: http://minubeinformatica.com/cursos/seguridad-informatica/criptografia

SAMANIEGO ZANABRIA, Ana Liz. Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información. 2018. De: https://repositorio.urp.edu.pe/bitstream/handle/20.500.14138/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

SAN MIGUEL MARTÍN, Pablo. Diseño y desarrollo de un algoritmo eficiente y seguro de firma digital ECDSA para su uso en protocolos Blockchain. 2023. Available from: https://oa.upm.es/72880/1/TFG_PABLO_SAN_MIGUEL_MARTIN.pdf

SÁNCHEZ RODRÍGUEZ, Sofía. Sistema seguro de mensajería instantánea certificada. 2020. https://oa.upm.es/58165/1/TFG_SOFIA_SANCHEZ_RODRIGUEZ.pdf

SÁNCHEZ VALLEJOS, Jhonny Moisés. Técnicas de encriptación para mejorar la seguridad en la transferencia de archivos en un entorno fiable. 2017. https://repositorio.uss.edu.pe/handle/20.500.12802/4060

SÁNCHEZ, Samuel; Domínguez, Pablo; Velásquez, Luis. Hashing: Técnicas y Hash para la Protección de Datos. *Universidad Tecnológica de Panamá, Grupo de Investigación*, 2018.

SANCHEZ-RUBIO, Dionisio. "Diseño gráfico en la era post-Snowden. Criptografía tipográfica y otros modos de camuflaje." *INMATERIAL. Diseño, Arte y Sociedad* 1.2 (2016): 33-67.

SANDOVAL, Miguel Morales; De La Fuente, José Antonio Molina; DE LA FUENTE ANAYA, Héctor Alán. Criptografía: una tecnología antigua en aplicaciones modernas de alto impacto. 2022.

SANTOS, Jesús. Que son, como funcionan y para qué sirven los hash. 2022. https://economia3.com/funciones-hash-para-que-sirven/

SERRATO LOSADA, Hernán Darío, et al. Comparación de métodos criptográficos para la seguridad informática. 2019. https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

SOLÍS ORNELAS, Carlos Alejandro. Propuesta de un algoritmo de cifrado híbrido basado en matrices de rotación cuaterniónica y el estándar RSA.

STATISTA, Available: https://es.statista.com/estadisticas/934626/servicios-de-mensajeria-instantanea-mas-utilizados-por-los-usuarios-de-internet-en-espana/

TECNOLOGÍA + INFORMÁTICA. ¿Qué es la criptografía? 2019. <https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad>.

TEJEDOR MORALES, María Yahaira. HASHING. UN CONCEPTO. UNA REALIDAD. De. https://www.laccei.org/LACCEI2018-Lima/student_Papers/SP73.pdf

TORRES CARDONA, Renson. "Criptografía simétrica y asimétrica y su aplicación en medios digitales como las imágenes, video y audio.". https://repository.unad.edu.co/handle/10596/40365

TRAYNO, VLADLENA. "Ataque diferencial mediante inyección de un error en AES-128." (2016).

VELASCO ESCOBAR, Moisés. Seguridad de la información en la red basada en el sistema de criptografía RSA. De: https://tesis.ipn.mx/bitstream/handle/123456789/21731/TESIS.pdf?sequence=1&isAllowed=y

VELASTEGUI, Marco Antonio Yandún, BOLAÑOS BURGOS, Francisco Joseph and HIDALGO GUIJARRO, Jairo Vladimir. "Algoritmos simétricos y asimétricos para el encriptado de imágenes Symmetric and asymmetric

VALDES, G., Domingo y TEJEDOR MORALES, María Yahira. HASHING. UN CONCEPTO. UNA REALIDAD. DE: https://laccei.org/LACCEI2018-Lima/student_Papers/SP73.pdf

YAMBAY WILMAN, Jenny; ARCOS PONCE, Georgina. *IV congreso internacional de ingenierías: La ingeniería como base del desarrollo*. Universidad Politécnica Estatal del Carchi, 2018