CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA Y SU APLICACIÓN EN MEDIOS DIGITALES COMO LAS IMÁGENES, VIDEO Y AUDIO

RENSON TORRES CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2020

CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA Y SU APLICACIÓN EN MEDIOS DIGITALES COMO LAS IMÁGENES, VIDEO Y AUDIO

RENSON TORRES CARDONA

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

Msc. KATERINE MARCELES VILLALBA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este proyecto de grado principalmente a Dios, a mi hijo, esposa, padres, hermana y sobrina.

A Dios por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente. A mi hijo por ser mi motor para ser mejor persona cada día, a mi esposa por su cariño y confianza para poder cumplir mis sueño y metas, a mis padres, hermana y sobrina que sin importar las adversidades siempre han confiado en mi de manera incondicional.

AGRADECIMIENTOS

Agradezco a Dios por darme la sabiduría, valentía y fuerza para culminar este proyecto de grado con éxito.

Gracias a todas las personas que me apoyaron para la ejecución de este proyecto, como fueron los entrevistados, por su respaldo y participación; a mi asesora de proyecto Katerine Márceles Villalba y mis tutores de área Edgar Roberto Dulce y Martin Camilo Cancelado por su dedicación, entusiasmo, y sus aportes para el desarrollo de esta investigación. A mi hijo y esposa por su apoyo incondicional en mi vida que, con su amor y respaldo, me motivan a alcanzar mis objetivos.

CONTENIDO

pág.

LISTA DE FIGURAS

GLOSARIO

Algoritmo: Se puede determinar como una unión ordenada y finita de operaciones que, con el fin de dar la solución de un problema, Forma de plasmar diferentes formas matemáticas.[1]

Algoritmo de Cifrado: Es un método que se utiliza con el fin de proteger la información que viaja a través de la red. Es un procedimiento matemático que transforma la información para que no sea visible ante los usuarios no reconocidos.[2]

Cifrado: es el método que se utiliza con el fin de codificar o encriptar los datos, para que solo puedan ser descifrados por el destinatario final del mensaje y quien debe de saber la forma de descifrarlo[3]

Cifrado Asimétrico: Cifrado asimétrico, o criptografía asimétrica o de clave pública, es un método de protección de información, este es un método que utiliza una llave publica para cifrar la información y una privada para poder acceder a esta.[4]

Cifrado Híbrido: Este método es una combinación entre el cifrado simetrico y el asimétrico, este emplea una clave publica para compartir la clave privada, pero el mensaje va con la clave privada y solo se desencripta con la misma privada, la publica se emplea para enviar la llave privada.[5]

Cifrado Simétrico: Este método de cifrado utiliza la misma clave tanto para encriptar como para desencriptar la información cifrada, Este método es muy efectivo cuando la información se trabaja solo entre dos personas, pero es más inseguro ya que con solo una contraseña es más fácil de vulnerar la información. un hacker, la intercepten. La ventaja es que este método es mucho más ágil que el método asimétrico.[6]

---

[1]ASALE, R. -., & Rae Algoritmo: Diccionario de la lengua española [En linea]. 2019. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://dle.rae.es/diccionario

[2] Ciberseg1922. ¿Qué son los algoritmos de cifrado? Tipos y características [En linea]. 2020. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://ciberseguridad.com/servicios/algoritmos-cifrado/#Definicion_de_algoritmos_de_cifra

[3] ¿Qué es el cifrado? [En linea]. 2019 [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.internetsociety.org/es/encryption/what-is-encryption/

[4] Cifrado asimétrico: Transmisión segura de datos [En linea]. 2020. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.ionos.es/digitalguide/servidores/seguridad/cifrado-asimetrico/

[5] LinkFang. Criptografía híbrida [En linea]. 2020. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://es.linkfang.org/wiki/Criptograf

[6] Kaspersky. ¿Qué es el cifrado de datos? [En linea]. 2018. [Fecha de consulta: 19 octubre de 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

Criptografía: La criptografía se conoce como el arte de escribir de modo secreto con una clave ya predefinida que permite revelar el mensaje verdadero solo a al destinatario final.[7]

Data Encryption Standard: DES (Data Encryption Standard) es el primer método de cifrado de información creado para la información digital, este fue desarrollado en conjunto por IBM y el gobierno de EEUU, este se creó con la idea de que el público en general tuviera acceso a este, para que así pudieran proteger la información que circulaba por las redes de ordenadores.[8]

Metadatos: Los metadatos son un conjunto de información de diferentes características que se almacena dentro de los archivos digitales y sirven para dar una descripción más acertada del formato y estos difieren dependiendo del archivo y del tipo de elemento que lo capturo.[9]

[7] ASALE, R. -., & Rae Criptografía: Diccionario de la lengua española [En linea]. 2019. [Fecha de consulta: 19 de octubre de 2020]. Disponible en: https://dle.rae.es/diccionario

[8]Herramientas web para la enseñanza de protocolos de comuicaion. DES [En linea]. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

[9] Qué son los Metadatos. [En linea]. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.geoidep.gob.pe/conoce-las-ides:/metadatos/que-son-los-metadatos

RESUMEN

Con la realización de la monografía se busca comprender mejor los métodos de cifrado de información Simétrica, Asimétrica e Híbrida y sus diferentes aplicaciones en la protección de la información, buscando entender no solo su forma de operar si no también su parte lógica, entre su manera de programación, algoritmos y fórmulas matemáticas.

La segunda parte del trabajo se basará en entender el tipo de formatos de las imágenes, el audio y el video y el cómo opera la aplicación de la criptografía en este tipo de archivos, en cómo se bloquea la información esencial del archivo y como a la misma vez permita que los usuarios puedan acceder a esta.

También se abordó la parte de los metadatos en las imágenes, los cuales proveen una cantidad de información que no es controlada por las entidades estatales y además de conocer herramientas que tienen la capacidad de borrar esta informacion con el fin de que las personas pueden tener una mayor seguridad en este tipo de formatos.

Igualmente se relacionan las normas, leyes y demás que rigen tanto en Colombia como a nivel internacional con el fin de proteger los derechos de autor y ejercer una seguridad sobre la informacion de las personas; además de las estrategias que se implementan a través de la criptografía, con el fin de avanzar en el proceso de la protección de las imágenes, video y audio.

ABSTRACT

With the completion of the monograph, the aim is to better understand the methods of encrypting Symmetric, Asymmetric and Hybrid information and its different applications in the protection of information, seeking to understand not only its way of operating but also its logical part, among its way of programming, algorithms and mathematical formulas.

The second part of the work will be based on understanding the type of formats of images, audio and video and how the application of cryptography operates in this type of files, how the essential information of the file is blocked and how to At the same time, allow users to access it.

We will also work on the part of the metadata in the images, which provide a quantity of information that is not controlled by state entities and in addition to knowing tools that have the ability to erase this information so that people can have a greater security in these types of formats.

Likewise, the rules and laws and others that govern both in Colombia and internationally will be exposed in order to protect copyright and exercise security over people's information, in addition to the strategies that are implemented through cryptography, in order to advance in the process of protecting images, video and audio.

INTRODUCCIÓN

A medida que pasa el tiempo los avances de la tecnología son cada vez más grandes y evidentes, estando a punto de la llegada de la computación cuántica, algo que promete revolucionar totalmente el mundo de la computación en todos sus aspectos, para de igual manera los delitos informáticos avanzan al mismo paso de la tecnología, entendiendo que entre estos existe una correlaciona muy cercana y hasta muy lógica, entendiendo el límite entre la propiedad privada y la lucha por el libre acceso a la información.

Es aquí donde un sinnúmero de personas lucha por ingresar al mercado de creación de contenido digital como las imágenes, el audio y el video, buscando sacar algún redito de esto, y es aquí donde las personas que al final no hacen parte de esta cadena de producción intentan sacar también su tajada económica, afectando a las personas que en realidad están realizando el trabajo.

Si bien la cantidad de dinero que mueve esta industria es multimillonaria, en donde algunos pocos se quedan con un gran porcentaje y muchos de esos artistas de bajo perfil, solo les llega una pequeña cantidad y estos son los que realmente se ven afectados por el tema de venta ilegal de este tipo de material digital, donde al final lo creadores no están percibiendo los recursos económicos que le permitan seguir realizando sus proyectos.

A nivel mundial se ha implementado diferentes normas y leyes que buscan proteger a estas personas, pero al final esto no se ha logrado, se castigan algunos, pero el problema sigue y este problema lo debe de solucionar la misma tecnología, en donde sí se ha logrado proteger los sistemas financieros a través de la encriptación de los datos también sería posible lograrlo con este tipo de información y es aquí en donde se verán las posibilidades que existen.

En donde también se podrán abordar el tema de los metadatos que este tipo de formatos pueden almacenar y terminar afectando a las personas, que de una manera inconsciente entregan esta información a diestra y siniestra sin precaución alguna y de la cual muchas compañías se están aprovechando.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Se estima que solo en el campo musical las pérdidas económicas que genera la reproducción musical de manera ilegal o lo que se conoce como piratería, asciende aproximadamente a seis mil millones de dólares en el mundo, lo que ocasiona que se estén perdiendo miles de empleos a nivel mundial por causa de este problema, además de la propia afectación que tienen los artistas, ya que muchos no logran tener un punto económico estable que les permita sacar al mercado nuevas creaciones, lo que se convierte en un gran inconveniente.[10]

De igual manera se encuentra relación el tema de la piratería de videos, más enfocado a las producciones cinematográficas, en donde se causa un gran impacto a esta economía, aunque esta genera grandes ganancias a nivel mundial, la piratería también se está llevando una buena parte de esta, en donde de igual manera se termina afectando a los pequeños productores que tienen ganancias limitadas, lo que les impide continuar con procesos de creación de contenido por falta de presupuesto.[11]

En lo relativo a las imágenes, no se afecta tanto económicamente, pero si se puede ver una utilización indiscriminada de diferentes imágenes en internet, en donde muchas veces se termina afectando a las personas, debido al material que estas incluyen y que a la misma vez no tienen una debida protección en cuanto a sus metadatos.

1.2 FORMULACIÓN DEL PROBLEMA

Con el avance constante de la tecnología y las posibilidades de emprendimientos nuevos, los medios audiovisuales se han convertido en una posibilidad muy rentable y de la mano vienen creciendo compañías que ofrecen los servicios de protección de información y no solo en el cifrado para que ésta sea protegida en la internet, si no también ofreciendo seguridad a los productos audiovisuales que se están creando en las empresas.

Es en este caso la investigación se basará en cómo funcionan estas tres ramas de la criptografía y no solo al proceso que está realizando, si no a también a sus tipos

[10] Publimetro. Piratería se come 40% del mercado musical; mata talentos y estrellas [en línea]. 2016. [Fecha de consulta: 14 octubre 2020]. Disponible en: https://www.publimetro.cl/cl/home/2016/11/04/pirateria-se-come-40-mercado-musical-mata-talentos-estrellas.html#:~:text=

[11] ¿Cómo funciona realmente la piratería de películas y series? [en linea]. 2020.[Fecha de consulta: 14 octubre 2020]. Disponible en: https://smartprotection.com/es/media/como-funciona-realmente-pirateria-online-peliculas-series/

de programación, algoritmos y fórmulas matemáticas y además entender cómo funcionan en el mundo de la seguridad informática, enfocados en objetivos ya predefinidos y alcanzables.

Se realizará un estudio de cómo se crean y funcionan de una manera general las imágenes, el audio y el video, además se buscará comprender todas las variaciones que tienen estos, como calidad, medios de trasmisión y otros que puedan afectar la seguridad que estos poseen en los diferentes medios de almacenamiento digital que existen.

El centro de la investigación se basará en cómo funcionan los diferentes métodos de cifrado de información en este tipo de formatos, entendiendo en que esta información debe contener una protección que garantice la integridad del archivo, pero que a su misma vez le debe permitir a los usuarios obtener información de estos sin llegar a ser afectada su originalidad, independientemente de las modificaciones que lleguen a tener. Lo anterior, permite formular la siguiente pregunta problema: ¿Cuán importante es la criptografía simétrica y asimétrica en su aplicación en medios digitales como las imágenes, video y audio?[12]

[12] VENTURINI, G.¿Qué es la Criptografía? [en línea]. 2020 [Fecha de consulta: 14 octubre 2020] Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/#:~:text=Básicamente

2 JUSTIFICACIÓN

Hoy en día los medios digitales se han convertido en un medio de creación de contenido de entretenimiento y educación muy importante para el desarrollo de la humanidad, puede ser de las industrias mundiales que más dinero están generando y esto, está siendo aprovechado por casi todo mundo ya sea como creador o usuarios, sobre todo en el tema del video, que es básicamente una mezcla de audio e imágenes.

En un principio todo este tipo de información era muy costosa, sobre todo en el tema de la música y el video, pero hoy en día con el avance de la tecnología de las telecomunicaciones, llegaron muchas plataformas como, por ejemplo: Netflix, YouTube, Facebook, Instagram, Amazon, Dezzer, Spotify, etc. Ya son una cantidad impresionante que permiten un acceso relativamente económico a todo este contenido, pero en países donde sus habitantes tienen una percepción económica muy baja aún, persiste mucho la piratería sobre todo de música y videos.

Pero siendo un medio que genera tanto dinero en el mundo, muchas personas están aprovechando las falencias de seguridad que se presentan en estos archivos, para poder copiarlos en diferentes dispositivos y distribuirlos a los usuarios de una manera más económica o hasta gratis, evitando que muchos creadores de fotografía, audio y video perciban estas ganancias, lo que ocasiona que pequeñas empresas entren en crisis financieras y terminen cerrando y así evitan que muchos talentos algún día lleguen a ser conocidos.

Es por esto, que se busca entender porque aún el cifrado que se le está aplicando a este tipo de información sigue siendo tan frágil, ya que el intentar copiar este tipo de información, ésta no ofrece ningún tipo de resistencia, y en su mayoría basta con copiar y pegar. En virtud de lo anterior, con el desarrollo de este trabajo se busca conocer las normas que rigen a nivel mundial la protección de la información que este tipo de archivos pueden contener, entendiendo que cada archivo que se genera almacena unos metadatos que pueden llegar a revelar información privada de su creador y que pueden hasta llegar al punto de ponerlos en peligro[13], así como también los mecanismos de protección empleados para garantizar la confidencialidad e integridad de la información a través de los medios digitales de audio, imagen y video.

[13] Entiende el concepto de piratería digital y aprende a protegerte [en línea]. 2019. [Fecha de consulta: 22 octubre 2020]. Disponible en: https://obsbusiness.school/es/blog-investigacion/propiedad-intelectual/obs-presenta-el-informe-de-pirateria-digital

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el funcionamiento del cifrado de información de las imágenes, videos y audios.

3.2 OBJETIVOS ESPECÍFICOS

- Comprender los diferentes métodos de cifrado Simétrico y Asimétrico y su aplicación en el medio.

- Establecer los diferentes métodos de protección de la información en la imagen, el audio y el video.

- Determinar cómo actúa el cifrado de la información de la imagen, el audio y el video.

- Identificar herramientas y o plataformas que permitan el borrado de los metadatos.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Para poder entender la relevancia de la criptografía en los medios digitales es importante conocer su concepto, métodos y orígenes, como también el alcance que ha adquirido en la seguridad informática. Los medios digitales que son el área de enfoque de este proyecto constituyen una serie de tipificaciones a aplicar y relacionar en cuanto a la protección de datos se refiere. Por ende, este marco teórico pretende relacionar estos conceptos con el fin de conseguir el objetivo principal.

Se refiere a cómo la criptografía siendo una técnica que protege la información digital, funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la misma escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

Con la creación y evolución de las computadoras, el cifrado de información fue ampliamente divulgada, empleado y modificado, constituyéndose luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario, así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

También se puede decir, que la criptografía es la ciencia y arte de escribir mensajes en forma cifrada o en código. Es parte de un campo de estudios que trata las comunicaciones secretas, usadas, entre otras finalidades, para:[14]

- Autentificar la identidad de usuarios.
- Autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias.
- Proteger la integridad de transferencias electrónicas de fondos.

[14] Tecnología + informática. ¿Qué es la criptografía? [En línea]. 2020. [Fecha de consulta: 11 dmarzo 2020]. Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/

4.1.1 Criptografía y seguridad informática: La criptografía permite cifrar mensajes por medio de un método de criptografía, el cual permite garantizar la privacidad; o sea, solamente el remitente y el o los destinatarios pueden tener acceso al contenido del mensaje. Además de eso, un mensaje debe poder ser suscrito; es decir, la persona que lo recibe debe poder verificar si el remitente es realmente la persona que dice ser y tener la capacidad de identificar si un mensaje puede haber sido modificado y esta es la tarea primordial de la criptografía, garantizar la integralidad de la información.

Los métodos de criptografía actuales son altamente seguros y eficientes y basan su uso en una o más llaves. La llave es una secuencia de caracteres, que puede contener letras, dígitos y símbolos (como una contraseña), y que es convertida en un número, utilizada por los métodos de criptografía para codificar y decodificar datos y esto es dependiendo de la actividad que se vaya a realizar; ya que, si bien cualquier algoritmo funciona en cualquier operación, siempre habrá uno que se ajuste mejor a la actividad a realizar.[15]

4.1.2 Criptografía simétrica y asimétrica: Simétricas es la utilización de determinados algoritmos para descifrar y encriptar (ocultar) documentos. Son grupos de algoritmos distintos que se relacionan unos con otros para mantener la conexión confidencial de la información, en este caso la contraseña de cifrado es la misma que se utiliza para poder acceder a la información, es un poco más insegura, pero en ciertos casos es muy funcional, aunque este algoritmo también permite la creación de varias llaves, se pude encriptar un archivo con dos contraseñas o más y esto disminuye la probabilidad de perdida de información.

Asimétricas es una fórmula matemática que utiliza dos llaves, una pública y la otra privada. La llave pública es aquella a la que cualquier persona puede tener acceso, mientras que la llave privada es aquella que sólo la persona que la recibe es capaz de descifrar, en este caso solo la persona que tiene la llave de recuperar la información es la única que puede acceder a esta; dado que en este caso ni la persona que realiza el proceso de cifrado, puede volver a acceder a ésta lo que garantiza mayor confiabilidad en los datos.

El cifrado hibrido es una mezcla entre el simétrico y asimétrico, en este caso se usa la clave pública del receptor para realizar el proceso de cifrado, pero una vez realizado el proceso, solo el receptor podrá acceder a este con la clave privada.

Actualmente, los métodos criptográficos pueden ser subdivididos en dos grandes categorías, de acuerdo con el tipo de llave utilizado: criptografía de llave única y la

[15] Ibíd.

criptografía de llave pública y privada, ambos siguen vigentes debido a que sus fortalezas los hacen fuertes en ciertos campos.[16]

4.1.3 Tipos de claves criptográficas: existe la criptografía llave única utiliza la misma llave tanto para codificar como para decodificar mensajes. A pesar de que este método es bastante eficiente en relación con el tiempo de procesamiento, o sea, el tiempo que gasta para codificar y decodificar mensajes, tiene como principal desventaja la necesidad de utilización de un medio seguro para que la llave pueda ser compartida entre personas o entidades que deseen intercambiar información criptografía, pero es muy eficiente para mover información a grandes distancias en casos de emergencias.

Criptografía de llaves pública y privada: La criptografía de llaves pública y privada utiliza dos llaves distintas, una para codificar y otra para decodificar mensajes. Con este método cada persona o entidad mantiene dos llaves: una pública, que puede ser divulgada libremente, y otra privada, que debe ser mantenida en secreto por su dueño. Los mensajes codificados con la llave pública solo pueden ser decodificados con la llave privada correspondiente, el problema es que para este método debe existir un proceso de generar las claves privadas y en casos de que el usuario final no tenga su llave, no va a tener forma de acceder a esta.[17]

4.1.4 ¿Qué es firma digital?: Para comprender la aplicación de la criptografía es importante conocer la importancia de la firma digital, esta consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda verificar si el remitente es quien dice ser e identificar cualquier mensaje que pueda haber sido modificado.", aunque para este caso es necesario una aplicativo especifico tanto para crear el archivo como para acceder a este, toda vez que por ejemplo: el recibir un archivo en formato PDF, JPG o cualquier otro no garantiza la integralidad de la información de un archivo con firma digital.[18]

Para comprender la aplicación de la criptografía es importante conocer la importancia de la firma digital, esta consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda verificar si el remitente es quien dice

[16] Salmocorpblog. Criptografía simétrica y asimétrica [En linea]. 2017. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://salmocorpblog.wordpress.com/2017/01/27/criptografia-simetrica-y-asimetrica/

[17] Tecnología + informática. ¿Qué es la criptografía? [En línea]. 2020. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/.

[18] Todo lo que tiene que saber sobre firma electrónica y firma digital [en línea]. Colombia, 2020. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.portafolio.co/economia/todo-lo-que-tiene-que-saber-sobre-firma-electronica-y-firma-digital-541460

ser e identificar cualquier mensaje que pueda haber sido modificado.", aunque para este caso es necesario una aplicativo especifico tanto para crear el archivo como para acceder a este, toda vez que por ejemplo: el recibir un archivo en formato PDF, JPG o cualquier otro no garantiza la integralidad de la información de un archivo con firma digital.[19]

4.1.5 ¿Qué tamaño de llave criptográfica debe ser utilizado?: Es de gran importancia generar buenos niveles de seguridad al utilizar los métodos de criptografía, enuncia que aquellos niveles de seguridad "son públicamente conocidos y son seguros por la robustez de sus algoritmos y por el tamaño de las llaves que utilizan. Para que alguien descubra una llave necesita utilizar algún método de fuerza bruta; es decir, probar combinaciones de llaves hasta que la correcta sea descubierta. Por lo tanto, cuanto mayor sea la llave criptográfica, mayor será el número de combinaciones a probar, inviabilizando así el descubrimiento de una llave en un tiempo normal. Además de eso, las llaves pueden ser cambiadas regularmente, haciendo los métodos de criptografía aún más seguros.", pero esto obliga a que los usuarios ya sea el emisor o receptor, dependiendo del caso, tengan procesos de creación de contraseñas lo suficientemente seguros, ya que se puede manejar un algoritmo muy seguro, pero si la contraseña es débil un ataque por diccionario no tendrá mucho problema en descubrir la información.

Actualmente, para obtenerse un buen nivel de seguridad en la utilización de un método de criptografía de llave única, es aconsejable utilizar llaves de un mínimo de 128 bits. Y para el método de criptografía de llaves pública y privada es aconsejable utilizar llaves de 2048 bits, siendo el mínimo aceptable de 1024 bits. Dependiendo para los fines para los cuales los métodos criptográficos serán utilizados, se debe considerar la utilización de llaves mayores: 256 o 512 bits para llave única y 4096 o 8192 bits para llaves pública y privada, aunque por ejemplo: el algoritmo AES o el de curva elíptica, son simétricos pero sus procesos de cifrado son altamente seguros y se manejan normalmente a 128 bits y pueden llegar hasta los 256 bits y las probabilidades de que un ataque tenga éxito es demasiado bajo, pero esto de igual manera depende de que la clave de cifrado sea lo suficientemente segura.[20]

4.1.6 La importancia de la criptografía en medios digitales como audio, video e imagen: el cifrado de información a permitido el traslado de imágenes, audio y video que se consideren de alto valor de un punto a otro, ya sea por medios físicos o a través de la internet, de una manera segura, ya que estos métodos de criptografía permiten codificar la informacion y en caso de que esta llega a ser

[19] Ibíd.

[20] MARRERO TRAVIESO, Y. La Criptografía como elemento de la seguridad informática [En linea]. 2003. Ciudad de La Habana. [Fecha de consulta: 8 octubre 2020]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

captura en el camino, no va a ser legible por parte del sustractor ilegal y se mantendrá la confiabilidad en estos datos.

Existe una técnica de cifrado de datos llamada esteganografía, que consiste en el arte de camuflar información dentro de una imagen, entendiendo que la composición de una imagen en bits, maneja una estructura predeterminada y al terminar esta estructura el archivo permite agregar otros archivos en bits y luego sustraerlos y armarlos en un archivo de texto con su extensión original y recuperarlo y es poco probable de ser descubierto en el camino, aunque si hay indicios, no hay forma de agregarle una protección extra, a no ser que la tarea se realiza con algún software especial, pero su camuflaje muy práctico.

Pero esta técnica también es un sistema de hackeo muy efectivo, ya que al poder esconder cualquier tipo de informacion, también cabe agregarle algún tipo de malware con un ejecutable automático y al enviar una imagen llamativa, es muy fácil que las personas se sientan atraídas por estas y las abran y en ese momento abra entrado un virus al equipo anfitrión y dependiendo del malware, los daños pueden variar, en este caso esta técnico es muy útil, pero al igual es muy peligrosa, aunque el arte de ocultar archivos en otros también aplica, a los audios, al video y básicamente a cualquier tipo de formato digital.[21]

[21] Redacción 01/02/2020 11:37, & Redacción, La esteganografía digital, la técnica que oculta información en archivos multimedia [En linea]. 2020. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://www.lavanguardia.com/vida/20200201/473240641630/la-esteganografia-digital-la-tecnica-que-oculta-informacion-en-archivos-multimedia.html

4.2 MARCO CONCEPTUAL

4.2.1 Criptografía: La criptografía se entiende como el Criptografía: arte de escribir con clave secreta o de un modo enigmático, buscando proteger la información.[22]

4.2.2 Cifrado: El adjetivo cifrado hace referencia aquello cuya escritura que se desarrolla con cifras: es decir, con signos que se utilizan para la representación de números o que solamente se pueden comprender cuando se conoce la clave correspondiente.

El cifrado es un método habitual en la criptografía (la técnica que consiste en escribir mensajes de manera secreta). Lo que supone el cifrado, en este caso, es una codificación del contenido del mensaje, protegiéndolo. De este modo, solo pueden comprender el contenido aquellas personas que saben la clave y que tienen la manera de decodificarlo.[23]

4.2.3 Cifrado Simétrico: Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben estar de acuerdo en la clave a usar de antemano. Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave. Como ejemplo: de sistema simétrico está «Enigma»; Éste es un sistema que fue usado por Alemania, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.[24]

4.2.4 Cifrado asimétrico: Este método utiliza dos claves diferentes (pública y privada), que están vinculadas entre sí matemáticamente. Las claves son solo números extensos vinculados entre sí, pero no son idénticos, de ahí el término asimétrico. La clave pública se puede compartir con cualquier persona, mientras que la clave privada debe mantenerse en secreto. Ambas se pueden usar para cifrar un mensaje, y la clave opuesta a la que se emplee para cifrarlo se utiliza luego para descodificarlo.[25]

---

[22] ASALE, R. -., & Rae, Criptografía: Diccionario de la lengua española. [en linea]. 2019. [Fecha de consulta: 23 marzo 2020]. Disponible en: https://dle.rae.es/criptografía

[23] PEREZ PORTO y MERINO. Definición de cifrado. [en linea] 2016, Fecha de consulta: 16 marzo 20] Disponible en: https://definicion.de/cifrado/

[24] Criptografía simétrica y asimétrica [En linea]. 2014. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://infosegur.wordpress.com/unidad-4/criptografia-simetrica-y-asimetrica/

[25] Guía de ``Gnu Privacy Guard''. Capítulo 2: «Sistema de cifrado simetrico» [En linea]. [Fecha de consulta: 27 marzo 2020] Disponible en: https://www.gnupg.org/gph/es/manual/c190.html..

4.2.5 Cifrado híbrido: Un sistema de cifrado híbrido usa tanto el cifrado simétrico como el asimétrico. Funciona mediante el uso de una clave pública para compartir una clave privada para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión. La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.[26]

4.2.6 Firma digital: La Firma Digital es un método de cifrado de información que asocia la identidad de una persona o de un equipo informático a un mensaje o documento. En función del tipo de firma puede, asegurar la integridad del documento o mensaje.[27]

4.2.7 Imagen: Significa figura o representación visual de algo o alguien. Proviene del latín imāgo, imagĭnis, que significa 'retrato'. En este sentido, puede tratarse de una pintura, un dibujo, un retrato, una fotografía o un video. Una imagen puede buscar simplemente representar la realidad; o más bien, tener una función simbólica, con una determinada carga significativa en su contexto cultural. Es el caso de imágenes como las señales de tráfico, las banderas o los signos, relativas a una comunicación que es visual e informativa.[28]

4.2.8 Video: El video es una tecnología utilizada para capturar, grabar, procesar, transmitir y reproducir una secuencia de imágenes representativas de una escena que se encuentra en movimiento, con la posibilidad de incluir sonidos. El término, que proviene del latín "ver", actualmente está asociado a distintos formatos de almacenamiento, ya sean análogos (VHS y Betamax) como digitales (MPEG-4, DVD, Quicktime, Avi, etc). Pero, desde los viejos casetes VHS hasta los masivos videos del YouTube de hoy, o plataformas como Netflix hay un largo trecho, donde lo viejo esta casi extinto.[29]

4.2.9 Audio: Es un término que proviene de la lengua inglesa, aunque su antecedente etimológico más lejano se halla en el latín. El concepto de audio se

[26] Ibíd.
[27]Universidad Politècnica de València. «¿Qué es una firma electrónica?» [en linea]. 2012. [Fecha de consulta: 24 marzo 2020] Disponible en: https://www.upv.es/contenidos/CD/info/711250normalc.html
[28]Significado de Imagen, [en linea]. 2017. [Fecha de consulta: 27 marzo 2020]. Disponible en: https://www.significados.com/imagen/
[29]DUARTE, Gabriel Definición de Video, [En linea]. 2008. [Fecha de consulta: 27 marzo 2020]. Disponible en: https://www.definicionabc.com/tecnologia/video.php

emplea para nombrar a la técnica que permite grabar, transmitir y reproducir sonidos.[30]

4.2.10 Metadatos: Los metadatos son un término que se empezó a utilizar en los años 60 para nombrar un conjunto de datos, este término se siguió utilizando a través de los años, pero fue ya en el 2004 donde el termino empezó a tomar su verdadera relevancia en el mundo de la computación y continuo su evolución hasta el verdadero significado que tiene en el día de hoy.

Los metadatos manejan una informacion muy concreta, pero con el paso del tiempo se le ha empezado a utilizar en diferentes procesos, ya que a través de ellos se puede adquirir información muy relevante de las personas y las grandes plataformas de internet como, por ejemplo: Google, Facebook, Twitter, Instagram y otras más han sabido sacar partida de esta informacion.[31]

[30] DEFINICIÓN DE AUDIO [En linea]. 2016. [Fecha de consulta: 12 abril 2020]. Disponible en: https://definicion.de/audio/

[31] PowerData, G. Metadatos, definición y características [En linea]. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.powerdata.es/metadato

4.3 MARCO HISTÓRICO

Se conoce la existencia de técnicas criptográficas primitivas desde tiempos remotos, en base a esto se realizó un recorrido por toda la historia empezando desde la criptografía clásica, criptografía medieval, la criptografía antes y después de la segunda guerra mundial, la criptografía moderna y los últimos avances de la criptografía.

Criptografía clásica: Según Singh, Simón en su libro The Code Book, el uso conocido más antiguo que se ha logrado encontrar de la criptografía, fueron unos jeroglíficos marcados en diferentes figuras del Antiguo Egipto, esto data de unos 4500 años. Aunque no se sabe a ciencia cierta si la idea era cifrar algún tipo de información, o simplemente buscaban plasmar algún tipo de información propia de su cultura con el fin de transmitir algún tipo de conocimiento, ya que no se sabe exactamente por qué hacían estos jeroglíficos.[32]

Se encuentran varios ejemplos de diferentes usos de lo que se puede considerar criptografía a través del uso de cifrados por sustitución mono alfabéticos (como el cifrado Atbash) que crearon los eruditos hebreos en un tiempo aproximado desde el 600 al 500 a. C, también en los escritos religiosos que podrían insultar a la cultura dominante o a los líderes políticos. Por ejemplo: un tema muy famoso es el así llamado el número de la bestia (666), el cual se menciona en el libro de las revelaciones, es muy posible que esta cifra contenga una información que hasta ahora es secreta, que revele algún mal mayor hasta ahora desconocido, estudiosos del tema tienen teorías que se está haciendo una referencia al imperio Romano y quizás al emperador Neron, que esa época era un señor de la destrucción y solo era entendido por algún grupo de personas que ya poseían un conocimiento previo de estos números, y por eso este libro sigue despertando tanto interés, por la cantidad de escritos enigmáticos que posee y que aún no se han descubierto.[33]

Los espartanos que eran guerreros por naturaleza, hacían uso de una técnica de criptografía para así lograr cifrar de alguna manera sus mensajes; específicamente utilizaban un método conocido como cifrado por transposición, el funcionamiento de este consistía en enrollar el mensaje sobre un utensilio de madera llamado escítala espartana, el cual ordena las letras y permitía poder leer el mensaje. El hecho es que la persona que recibía el mensaje, tenía en su poder una escítala de la misma medida de la que se utilizó para cifrar el mensaje, ya que era la única manera para que el mensaje se ordenara de la forma correcta y poder acceder a esto, de lo contrario era muy complicado. Además, teniendo en cuenta que en esa época no

[32] VELASCO, J. J. Diario Turing. Criptografía: Breve historia de la criptografía [en línea]. 2014. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html

[33] GUTIÉRREZ, P. Tipos de criptografía: Simétrica, asimétrica e hibrida [En linea]. 2017. [Fecha de consulta: 16 abril 2020]. Disponible en: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

se sabía leer muy bien, tampoco se conocía el idioma originario del pergamino y menos la idea de que alguien iba a codificar un mensaje, esto lo hacía muy exitoso y es unas de las primeras formas que se conocen de cifrado exitoso de información.[34]

Uno de los primeros registros que se puede catalogar como criptografía es el cifrado César y el cual proviene del imperio Romano, y la creación de este se le imputa al mismísimo emperador Romano Julio César, es muy probable que haya sido creado por alguno de sus servidores, pero el caso es que los registros pertenecen al él. El funcionamiento de este método se basa en el movimiento de la posición de las letras y por lo cual cada letra del mensaje original se cambia por otra letra que se ubica en un número fijo de posiciones ya sea más adelante o atrás en el alfabeto que utilizaba esta cultura. Según información recopilados por el historiador del antiguo imperio Romano Suetonio, Julio César utilizaba un método de correr tres letras y Augusto, nieto de Julio Cesar y también emperador utilizaba el desplazamiento de una sola letra.[35]

Durante el transcurso de la edad media la criptografía empezó un avance de manera más constante y este se centre en los territorios árabes, ya entrados en el siglo XIX, el matemático, filosofo, criptógrafo, astrónomo, médico, teórico de la música y astrólogo Al-Kindi desarrollaría una de las plataformas vitales en el descifrado de mensajes ocultos, influyendo grandemente sus estudios del Corán y el análisis de las frecuencias, técnica ya conocida en la segunda guerra mundial, su trabajo se basaba en el estudio y análisis de los patrones de los mensajes cifrados y por medio de esto, detectar las repeticiones e investigar la correlación de la probabilidad que existe de que ciertas letras aparezcan con mayor frecuencia que otras en un mensaje dependiendo del idioma.[36]

El criptologo Ibn al-Durayhim acompañado por el matemático Ahmad al-Qalqashandi, realizarían un estudio a profundidad de los análisis de frecuencias y de igual manera trabajaron en el desarrollo de códigos de criptografía más fuertes, al emplear múltiples sustituciones a cada carácter de los mensajes a cifrar (logrando que los patrones fueran inconsistentes y así evitar que la seguridad fuera vulnerable por medio de patrones ya conocidos). Es considerado el avance de criptoanálisis más importante que había ocurrido hasta el inicio de la Segunda Guerra Mundial; además también puede ser reconocida como unas de las primeras técnicas de hackeo al cifrado de información, ya que conociendo un precedente se dedicaron a desencriptar la información y esta parte es muy importante ya que el encontrar las

[34] Binance Academy. Historia de la Criptografía [En linea]. 2020. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://academy.binance.com/es/articles/history-of-cryptography

[35] Rome and Art. EL CIFRADO DE JULIO CÉSAR [En linea]. 2016. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://www.romeandart.eu/es/arte-cifrado-cesar.html#:~:text=Julio

[36] VELASCO, J. J. Diario Turing. Criptografía: Breve historia de la criptografía [en línea]. 2014. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html

vulnerabilidades en los sistemas es lo que obliga a que éstos evolucionen a algo mejor.[37]

Ya en el siglo XV es inventado un sistema de sustitución polialfabética por León Battista Alberti. Este sistema es conocido como cifrado Vigenere, al haber sido atribuido por error a Blaise de Vigeniere, lo que tenía este sistema de especial es que cada letra tiene una correspondencia única, haciendo que descifrarlo fuera mucho más complicado, toda vez que estas correspondencias eran únicas, pero dependían del generador.[38]

El avance de la criptografía en el Medio Oriente y Europa se mantuvo subdesarrollada en el transcurso de bastante tiempo. Mientras que en Japón no se hallaron registros de su utilización hasta 1510, y sus métodos avanzados no se dieron a conocer hasta que este país abrió sus puertas hacia el resto del mundo en los años de 1860, no existen cantidad de registros y si bien ésta no avanzaba si se puede intuir que se seguía utilizando, método muy eficaz en las estrategias militares, ya que los medios de transporte por lo general eran a caballo y si el mensajero caía en manos enemigas, estos no podrían acceder a la información ya que ni el mensajero podría descifrarlo.[39]

Avance de la criptografía desde los años de 1800 hasta la culminación de la segunda guerra mundial: Aunque la historia de la criptografía es extensa y ésta es muy compleja, debido a toda la información inconclusa que existe, en todo el tiempo que ha pasado hasta el siglo XIX, solo se crearon métodos criptográficos ad hoc para ejecutar procesos de cifrado de información y el criptoanálisis respectivamente, que es el método encargado de buscar los puntos frágiles de los algoritmos de criptografía, por ejemplo: Charles Babbage trabajo, en la época de la Guerra de Crimea, sobre el funcionamiento matemático de los cifrados polialfabéticos, el cual fue descubierto nuevamente y publicado años después por el prusiano Fiedrich Kasiski.

En estos tiempos el discernimiento existente de la criptografía en ese tiempo solo se basaba regularmente en norma generales averiguadas con gran apuro; como, los textos del doctor en letras Auguste Kerckhoffs sobre la criptografía a finales del siglo XIX. Edgar Allan Poe también logro desarrollar diferentes métodos secuenciales para intentar resolver algoritmos de cifrados de información, aproximadamente en los años de 1840. Más concretamente, publico un anuncio de sus conocimientos de criptoanálisis en el periódico de Filadelfia Alexander's Weekly, intentando que personas interesadas en el tema, realizaran el envío de cifrados,

[37] Ibíd.
[38] Ibíd.
[39] BRAINSHIT. Departamento de Matemática Aplicada de la Facultad de Informática (U.P.M.). Introducción a la criptografía [En linea]. [Fecha de consulta: 15 octubre 2020]. Disponible en: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html

para así aplicar sus conocimientos de resolución de métodos de cifrado. Su victoria creó gran entusiasmo entre las personas durante varios meses, pero luego ésto deja de ser algo novedoso y va desapareciendo. Transcurrido unos años, redacto un ensayo sobre los métodos criptográficos que utilizó y que le fueron de gran ayuda para desencriptar los códigos alemanes que estaban empleando en el cifrado de la información durante la Primera Guerra Mundial. Entre los algoritmos de cifrado se hallaban las cifras de Cuatro Cuadros, Doble Cuadro, ADFGX y ADFGVX. No obstante, la introducción de nuevas cifras y códigos solo supuso un breve intermedio antes de que estos fueran descifrados por los nuevos modelos de criptoanalistas que se crearon en la época.[40]

Ya con el avance del tiempo la criptografía se convirtió en un medio muy útil para diferentes tareas, pero fue en la segunda guerra mundial que las máquinas de cifrado de información se empezaron a utilizar extensamente, aunque en los campos de batalla éstas eran poco prácticas, por sus tamaños, por lo que el formato manual era más practico en estos momentos de guerra; en cambio algo que avanzo notablemente en estos tiempo fue el criptoanálisis, ya que se convirtió en algo necesario poder descifrar los mensajes del enemigo y descubrir sus estrategias de guerra y fue así que la criptografía y el criptoanálisis se convirtieron en parte fundamental de la guerra, las estrategias recorrían países, continentes y el que lograra conocer la movida del enemigo tomaría ventaja en esta partida que se jugaba el destino de toda la humanidad.[41]

Desde los años 20 de mil novecientos existía la máquina de cifrado enigma, ya ésta era muy utilizada en toda Europa por su cifrado rotatorio que permitía encriptar y desencriptar información y fue así como los alemanes decidieron usar este elemento en su guerra, ya que era muy fácil de usar, además que se suponía para la fecha que ésta era inviolable. El enigma era muy seguro, dado que resistía a las rupturas de código por estudios de frecuencia y era mejor que utilizar claves polinómicas y con este sistema los alemanes avanzaron por toda Europa dejando a su paso destrucción y desolación en cada batalla, con la tranquilidad de poder enviar sus mensajes de guerra de un lugar a otro sin perder su confidencialidad.[42]

Fue así como Alan Mathison Turing, un gran científico de la época y considerado unos de los padres de la computación, fue reclutado por ¡ aliados que buscaban una forma de poder derrotar al ejército Alemán que avanzaba sin resistencia alguna por toda Europa y es así como Turning utilizando sus conocimientos logro descubrir el método de cifrado de la máquina enigma, basado en unos estudios que habían realizado los polacos, intentado descifrar la información de estas máquinas, fue

[40] Ibíd.
[41] GUTIERREZ, Ángel. Criptografía y criptoanálisis en las dos guerras mundiales [En linea]. [Fecha de consulta: 15 octubre 2020]. Disponible en: https://www.acta.es/medios/articulos/comunicacion_e_informacion/052063.pdf
[42] Ibíd.

como así se creó la famosa máquina de Turing que es más bien un modelo matemático, un autómata con la capacidad de implementar cualquier problema matemático expresado a través de un algoritmo, con ésta solución los países aliados lograron empezar a descifrar la información secreta de las alemanes y sus aliados y empezar a dar vuelta a una guerra que llevaban algo perdida, el aporte de Turing fue fundamental para ganar la guerra, ya que las estadísticas dicen que gracias este autómata la guerra termino dos años antes de lo previsto, lo que ayudo a salvar miles de vidas, además de que para este momento los Alemanes avanzaban victoriosos.[43]

Criptografía moderna: “Después de la Segunda Guerra Mundial y del papel fundamental que jugó la criptografía y el criptoanálisis esta dio un gran salto gracias a Claude Elwood Shannon, matemático, ingeniero eléctrico y criptógrafo, conocido como el padre de la teoría de la comunicación. En 1948, Shannon, que trabajaba en los Laboratorios Bell, publicó "A Communications Theory of Secrecy Systems"; Una teoría secreta de los sistemas de las comunicaciones, un artículo fundamental en el que se modernizaron las técnicas de codificación para transformarlas en procesos matemáticos avanzados. Si bien es cierto que el análisis de frecuencia se basaba en la estadística, Shannon demostró matemáticamente este hecho e introdujo el concepto de "distancia de unicidad" que marcaba la longitud de un texto cifrado, y lo que se necesita para poder descifrarlo.[44]

La explosión de la computación, y su desarrollo tras la Segunda Guerra Mundial, convirtió a los computadores en un instrumento clave dentro del cifrado y descifrado de mensajes; por tanto, por seguridad, la mayoría de los países consideraron la criptografía como algo secreto y vinculado a tareas de inteligencia y espionaje. Hasta el 17 de marzo de 1975 no llegaría el primer "avance público" vinculado al mundo de la criptografía. IBM desarrolló el algoritmo de cifrado Data Encryption Standard (DES) que, dos años más tarde, se convertiría en un Federal Information Processing Standard (FIPS 46-3) y se extendería su uso por todo el mundo.[45]

En el año 2001, DES cedería su puesto a Advanced Encryption Standard (AES) que, tras 5 años de revisión, se convirtió en un estándar. El segundo de los grandes avances públicos también tuvo su origen en los años 70. Prácticamente, todos los sistemas de los que han hablado son simétricos; tanto emisor como receptor deben manejar el mismo código y estar informados mutuamente del código que van a usar a la hora de intercambiar información. Sin embargo, Whitfield Diffie y Martin Hellman sentaron las bases de la criptografía asimétrica (clave pública y clave privada) en el artículo "New Directions in Cryptography" publicado en 1976. La criptografía

[43] Ibíd.
[44] VELASCO, J. J. Diario Turing. Criptografía: Breve historia de la criptografía [en línea]. 2014. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html
[45] Ibíd.

asimétrica hoy es fundamental para transacciones realizadas a través de Internet, por ejemplo: en páginas que usan el protocolo HTTPS o para cifrar nuestros mensajes usando PGP, (que combina tanto criptografía asimétrica como criptografía asimétrica).[46]

Como se ha podido ver, la criptografía ha jugado un papel relevante en la historia de la humanidad y su importancia ha ido aumentando conforme ha aumentado el volumen de información que se ha ido generando o intercambiando. Las revelaciones de Edward Snowden sobre PRISM y el resto de los programas de espionaje en Internet de la NSA han hecho que las personas piensen en la criptografía, pero, en realidad, siempre ha estado presente y ahí, cuando se realiza una llamada telefónica con un dispositivo móvil, cuando se envía un Telegrama o se realiza una compra por Internet, el cifrado de la información no es algo de lo que se hable mucho en el mundo común, pero ha sido parte vital en el avance de los sistemas de comunicaciones, es lo que brinda esa seguridad en que las operaciones que se realizan por internet o las llamadas que se hacen estén protegidas hasta cierto punto.[47]

[46] Boxcryptor. Cifrado AES y RSA [En linea]. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://www.boxcryptor.com/es/encryption/

[47] VELASCO, J. J. Diario Turing. Criptografía: Breve historia de la criptografía [en línea]. 2014. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html

4.4 ANTECDENTES O ESTADO ACTUAL

Existen diferentes investigaciones en cuanto a la encriptación de información en medios digitales, en donde se expondrán como referentes tres artículos diferentes que tratan directamente sobre el tema a desarrollar, el cual aportaron para la fundamentación de éste.

- En el artículo “A New Image Encryption Algorithm Using Homogenized Chebyshev-Arnold Map” se propone un Mapa Chebyshev-Arnold homogeneizado (HCAM) homogeneizando el acoplamiento lineal del mapa Chebyshev y el mapa Arnold. El HCAM propuesto puede evitar dos problemas de origen del mapa de Chebyshev que conducen a un riesgo potencial de seguridad en el algoritmo de cifrado de imagen: Uno es la elección discontinua de valores iniciales para la propiedad caótica, el otro es la distribución de valores no uniformes de las secuencias generadas. Luego, basado en el HCAM, se propone un nuevo algoritmo de encriptación de imágenes que consta de dos partes: confusión y difusión. Para la parte de confusión, se mejoró la transformación mágica caótica (CMT) para ajustar los tiempos de desplazamiento de los píxeles seleccionados con respecto a las diferentes imágenes de texto sin formato, para un mayor nivel de seguridad sin costo de tiempo adicional. Para la parte de difusión, para mantener el bajo tiempo de ejecución del algoritmo, se presenta un esquema de sustitución de píxeles basado en la operación de bits. En consecuencia, la selección de píxeles y ciertos valores para la sustitución en estas dos partes son decididos por el HCAM. Los resultados de la simulación y el análisis de seguridad se han llevado a cabo y demuestran la seguridad y la eficiencia del algoritmo propuesto en comparación con los esquemas anteriores.[48]

El articulo ya mencionado dio bases concretas en cuanto a estudios realizados del cifrado de información, en este caso un algoritmo dedicado a la protección de las imágenes, si bien en este caso en específico se centra en un algoritmo que presenta ciertas fallas de seguridad y de igual manera se presenta uno nuevo que resuelve estos inconvenientes, pero en el desarrollo de la investigación, se muestran diferentes facetas del cifrado de imágenes y en la velocidad que estos pueden realizar los cálculos del proceso y reconociendo éste como uno de los fuerte de ciertos algoritmos, en cuanto al tiempo que tardan en realizar la tarea.

[48] LUO, X. et al. A New Image Encryption Algorithm Using Homogenized Chebyshev-Arnold Map [en linea].2018. [Fecha de consulta: 25 marzo 2020]. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edseee&AN=edseee.8652390&lang=es&site=eds-live&scope=site

- En el artículo Audio Encryption Algorithm Using Hyperchaotic Systems of Different Dimensions. Se ha presentado el cifrado de datos de audio con diferentes sistemas hipercaóticos dimensionales. Los sistemas hipercaóticos propuestos exhiben un excelente comportamiento caótico. Para demostrar su aplicación al procesamiento del cifrado multimedia, los tres sistemas se aplican con un algoritmo basado en la generación de llaves a partir de las condiciones iniciales para el proceso de cifrado y descifrado. Los resultados del cifrado, descifrado y análisis estadístico de los datos de audio muestran que el sistema de cifrado propuesto tiene un excelente rendimiento de cifrado, alta sensibilidad a las claves de seguridad y puede aplicarse para un cifrado seguro en tiempo real.[49]

Reconocer en este artículo un excelente estudio sobre un modelo en particular de cifrado de datos, dirigido a los formatos de audio, este artículo ayudo en la construcción de la monografía, en ofrecer una guía de posibles aplicaciones de la criptografía enfocadas a este tipo de formatos y en cómo operan las fórmulas matemáticas en estos procedimientos y en el planteamiento de un sistema hipercaótico para desarrollar un sistema de cifrado lo suficientemente seguro, basado en unos parámetros estables e incomprensibles.

- Dual-Layer Video Encryption using RSA Algorithm. En este artículo se propone un algoritmo de encriptación de video que utiliza la secuencia RSA y Pseudo Noise (PN), dirigido a aplicaciones que requieren transferencias de información de video que se consideran de alto valor. El sistema se encuentra diseñado principalmente para trabajar con archivos codificados utilizando el códec Audio Video Intercalado (AVI), aunque puede portarse fácilmente para su uso con archivos codificados con el grupo de expertos en imágenes en movimiento (MPEG). Los componentes de audio y video de la fuente se someten por separado a dos capas diferentes de cifrado, para garantizar un nivel alto de seguridad. El cifrado del componente de video implica la aplicación del algoritmo RSA seguido del cifrado basado en PN. Del mismo modo, el componente de audio se encripta primero con PN y luego se somete a encriptación con la Transformación discreta de coseno. Combinando éstas dos técnicas, se convierte en un sistema muy eficiente, en un sistema muy resistente a infiltraciones de seguridad y ataques con valores favorables de parámetros tales como: velocidad de cifrado / descifrado, relación de cifrado / descifrado y degradación visual; ha sido presentado. Para las aplicaciones que requieren cifrado de datos confidenciales en los que los requisitos de seguridad estrictos son la principal preocupación de los usuarios, se

[49] LAGMIRI; BAKHOUS. Audio Encryption Algorithm Using Hyperchaotic Systems of Different Dimensions. [en linea], 2018. [Fecha de consulta: 27 marzo 2020]Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.FE29FFEC&lang=es&site=eds-live&scope=site

> encuentra que el sistema produce similitudes insignificantes en la percepción visual entre la secuencia de video original y la secuencia cifrada. Para las aplicaciones en las que la similitud visual no es motivo de gran preocupación, limitamos la tarea de cifrado a un solo nivel de cifrado que se logra mediante el uso de RSA, lo que acelera el proceso de cifrado. Aunque en este caso se observa cierta similitud entre el video original y el encriptado, no es suficiente comprender los acontecimientos en el video.[50]

Este sistema brindo el conocimiento en cuanto a la utilización de algoritmos de cifrado más comunes, enfocados a un tipo de formato de videos. Este estudio brinda el conocimiento suficiente para entender que cualquier algoritmo de cifrado de información se puede utilizar para encriptar ya sean imágenes, audios y videos y si bien existen algoritmos enfocados en algún tipo de datos, con el debido proceso cualquiera de estos puede ser redireccionados hacia la aplicación que se quiera obtener de estos.

[50] CHADHA Aman, SUSHMIT Mallik, CHADHA Ankit, RAVDEEP Johar y M. ROJA Mani. Dual-Layer. Video Encryption using RSA Algorithm, Referencia de la revista: International Journal of Computer Applications [en linea]. 2015. [Fecha de consulta: 28 marzo 2020] Disponible en: https://arxiv.org/abs/1509.04387

4.5 MARCO LEGAL

En Colombia y el mundo existen un sin número de leyes y normas que buscan proteger los derechos de autor y la información personal de cada individuo y aunque se cuenta con este tipo de reglamento, el tema de la piratería de medios digitales y robo de informacion personal sigue en aumento; en virtud de que en este tipo de actividades se ha visto la capacidad de generar ingresos de manera relativamente sencilla para la delincuencia; además de la incapacidad y poca interés de las fuerzas de seguridad de los estados para perseguir este tipo de delincuencia que deja grandes pérdidas económicas tanto a los creadores, como a las finanzas de los mismos países.

Es así como en Colombia se creó la ley 23 de 1982, a la cual se le han realizado adiciones, siendo la ultima la ley 1915 del 12 de julio de 2018, estas se han implementado con el fin de garantizar los derechos y proteger a las personas que crean algún tipo de contenido digital, en donde se imponen castigos a los sujetos que de alguna u otra manera se aprovechen de este tipo de material para sacar algún beneficio económico, sin los permisos correspondientes del dueño original y además evadiendo impuestos.[51]

Existe la ley 1273 del 2009 "de la protección de la información y de los datos", la cual tipifica las conductas punibles que afectan la información digital de las personas, si bien no se especifica en ningún momento la protección a los derechos de autor ni a la protección de los datos, en ejemplo de esto se tiene el artículo 269J, donde menciona que el hecho de que realizar transferencia no consentida de activos en busca de un beneficio económico acarreará una sanción privativa de la libertad, pero en concreto no existe algo referente a la protección de las personas que crean contenido o de sus metadatos.[52]

En Colombia existen diferentes normas y leyes en busca de la protección de la información, datos personas y derechos de autor, sin embargo, estas se encuentran más enfocadas en la protección de las empresas y del estado que en la persona como tal y estos temas afectan a todos por igual y el hecho de entablar procesos en una demanda, por lo general son costos y complicados para que cualquier persona entable esta pelea que al final de alguna manera lo va a dejar perdiendo.

Por el lado de los metadatos estos si están totalmente desprotegidos, si bien a las compañías que recolectan esta información se les solicita que mantengan una debida protección de la información que recolectan, pero en el fondo ellos le pueden

[51] LEY 1915 DEL 12 DE JULIO DE 2018. [En linea]. Colombia: Presidencia de la Republica. 2018. [Fecha de consulta: 15 octubre 2020]. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201915%20DEL%2012%20DE%20JULIO%20DE%202018.pdf

[52] MINTIC. Ley 1273 de 2009 [En linea]. 2009 [Fecha de consulta: 23 abril 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

dar el manejo que deseen, ya que esta información les pertenece, desde el momento en el que el usuario hizo uso de sus plataformas.

No existen políticas a nivel mundial en busca de la protección de derechos de autor y tampoco en la protección de los metadatos, ya que estas leyes son implantadas en cada nación, de acuerdo a sus sistemas políticos, aunque básicamente en cualquier parte del mundo el copyright es un delito, controlarlo en particulares es algo muy complejo, dado que la piratería sigue siendo un gran negocio y acabarlo es una tarea complicada y más cuando muchos entes del estado se benefician de éste.

En busca de controlar copyright grandes plataformas web como YouTube, Facebook, Instagram, Twitter, Google y otras más que hacen parte de conglomerados empresariales que funcionan a nivel mundial, han implementado políticas de seguridad internas en busca de la protección de los derechos de autor, las cuales hasta el momento han tenido cierto punto de efectividad, ya que si una persona intenta sacar provecho de la creación de otra, lo que hacen éstas plataformas es trasmitirle las ganancias económicas al creador original, sin embargo una plataforma como: YouTube, sigue siendo una fuente de descarga ilegal de contenido digital.

Mientras por otro lado las plataformas sociales lo que están haciendo con los metadatos es darle un uso económico, pero a la misma ves indiscriminado, las personas no tienen la precaución con esta información y las redes sociales en sus políticas de seguridad información, cuál es su procedimiento frente a esta informacion, pero la mayoría de las personas no le prestan atención a esto.

5 DESARROLLO DE LOS OBJETIVOS

5.1 COMPRENDER LOS DIFERENTES MÉTODOS DE CIFRADO SIMÉTRICO, ASIMÉTRICO Y SU APLICACIÓN EN EL MEDIO.

El cifrado de la información se entiende como la forma en que un mensaje se codifica para que otras personas en sus capacidades normales no lo puedan entender, lo que hacen es tomar información y desarmarla y convertirla en otra cosa, en el mundo de los sistemas lo que hace es convertirla en números, esta tarea obligatoriamente la debe de realizar algún tipo de software, ya que va ser el único en desarmarla y volverla armar.

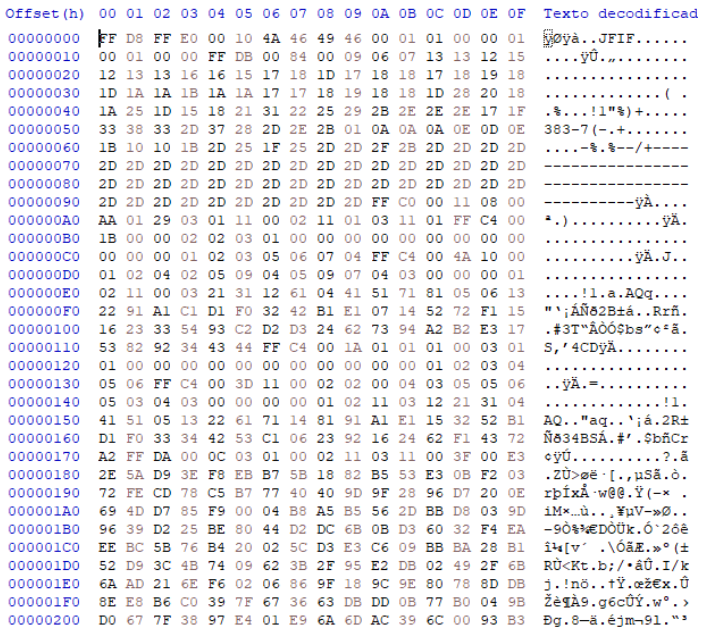
El software a través de un algoritmo lo que va es a transformar la informacion en dígitos, toda la información posee una cara visible, ejemplo: una imagen, una canción, una película, un texto y cada una posee un rasgo particular, pero detrás existe una serie de codificación en binario que es lo que componen cada dato y cada una maneja una estructura, esto es lo que en realidad interpreta cada computador para luego arrojar un mensaje.

A continuación, se muestra una imagen de dos maneras, una es la que puede percibir cualquier dispositivo con visor de imágenes, ya sea un computador, una Tablet, un celular u otro dispositivo, en la segunda imagen se muestra una parte del código binario de la primera imagen, ya que son más de mil líneas la que la componen, esto es lo que interpreta cualquier dispositivo para mostrar la imagen, como se ilustra en las figuras siguientes.

Figura 1. Parte visible de una imagen

Fuente: Synergy. ¿Qué es la criptografía post-cuántica? [En linea]. 2019.(Recuperado en 27 de marzo de 2020) Disponible en: https://nemespanol.io/que-es-la-criptografia-post-cuantica/

Figura 2. Los bits que componen una imagen



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texto decodificad
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	84	00	09	06	07	13	13	12	15	....ÿÛ.„.....
00000020	12	13	13	16	16	15	17	18	1D	17	18	18	17	18	19	18	.....
00000030	1D	1A	1A	1B	1A	1A	17	17	18	19	18	18	1D	28	20	18	.....(.
00000040	1A	25	1D	15	18	21	31	22	25	29	2B	2E	2E	2E	17	1F	.%...!1"%)+.....
00000050	33	38	33	2D	37	28	2D	2E	2B	01	0A	0A	0A	0E	0D	0E	383-7(-.+.....
00000060	1B	10	10	1B	2D	25	1F	25	2D	2D	2F	2B	2D	2D	2D	2D	....-%.%--/+----
00000070	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	----------------
00000080	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	----------------
00000090	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	FF	C0	00	11	08	00	----------ÿÀ....
000000A0	AA	01	29	03	01	11	00	02	11	01	03	11	01	FF	C4	00	ª.).........ÿÄ.
000000B0	1B	00	00	02	02	03	01	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	01	02	03	05	06	07	04	FF	C4	00	4A	10	00	.....ÿÄ.J..
000000D0	01	02	04	02	05	09	04	05	09	07	04	03	00	00	00	01	.....
000000E0	02	11	00	03	21	31	12	61	04	41	51	71	81	05	06	13	....!1.a.AQq....
000000F0	22	91	A1	C1	D1	F0	32	42	B1	E1	07	14	52	72	F1	15	"'¡ÁÑð2B±á..Rrñ.
00000100	16	23	33	54	93	C2	D2	D3	24	62	73	94	A2	B2	E3	17	.#3T"ÂÒÓ$bs"¢²ã.
00000110	53	82	92	34	43	44	FF	C4	00	1A	01	01	01	00	03	01	S,'4CDÿÄ.....
00000120	01	00	00	00	00	00	00	00	00	00	00	00	01	02	03	04	.....
00000130	05	06	FF	C4	00	3D	11	00	02	02	00	04	03	05	05	06	..ÿÄ.=.....
00000140	05	03	04	03	00	00	00	00	01	02	11	03	12	21	31	04	.....!1.
00000150	41	51	05	13	22	61	71	14	81	91	A1	E1	15	32	52	B1	AQ.."aq..'¡á.2R±
00000160	D1	F0	33	34	42	53	C1	06	23	92	16	24	62	F1	43	72	Ñð34BSÁ.#'.$bñCr
00000170	A2	FF	DA	00	0C	03	01	00	02	11	03	11	00	3F	00	E3	¢ÿÚ.........?.ã
00000180	2E	5A	D9	3E	F8	EB	B7	5B	18	82	B5	53	E3	0B	F2	03	.ZÙ>øë·[.‚µSã.ò.
00000190	72	FE	CD	78	C5	B7	77	40	40	9D	9F	28	96	D7	20	0E	rþÍxÅ·w@@.Ÿ(–× .
000001A0	69	4D	D7	85	F9	00	04	B8	A5	B5	56	2D	BB	D8	03	9D	iM×…ù..¸¥µV-»Ø..
000001B0	96	39	D2	25	BE	80	44	D2	DC	6B	0B	D3	60	32	F4	EA	–9Ò%¾€DÒÜk.Ó`2ôê
000001C0	EE	BC	5B	76	B4	20	02	5C	D3	E3	C6	09	BB	BA	28	B1	î¼[v´ .\Óãƒ.»º(±
000001D0	52	D9	3C	4B	74	09	62	3B	2F	95	E2	DB	02	49	2F	6B	RÙ<Kt.b;/•âÛ.I/k
000001E0	6A	AD	21	6E	F6	02	06	86	9F	18	9C	9E	80	78	8D	DB	j.!nö..†Ÿ.œž€x.Û
000001F0	8E	E8	B6	C0	39	7F	67	36	63	DB	DD	0B	77	B0	04	9B	Žè¶À9.g6cÛÝ.w°.›
00000200	D0	67	7F	38	97	E4	01	E9	6A	6D	AC	39	6C	00	93	B3	Ðg.8—ä.éjm¬9l.“³

Fuente: Propia del autor. (Recuperado en 27 de marzo de 2020)

Es ahí donde un software de cifrado de información actúa, él va a tomar cada bit y lo va a transformar en otro bit que va ser ilegible para cualquier dispositivo electrónico en su estado natural y además se le agrega una contraseña, esto es debido a que cualquiera que tenga este software podría acceder a la información y es ahí donde entra a operar la contraseña, impide que el software vuelva a rearmar la estructura original del archivo; por eso, hacer un proceso de desencriptado a mano es básicamente imposible, cada tipo de formato maneja una estructura, pero de igual manera al ser tantos datos es imposible descifrarlo sin la contraseña.

En la misma forma se encuentran estructurados los audios, los videos y cualquier tipo de información que sea digital, éste código binario además guarda mucha más información de la que simplemente se ve, por ejemplo: en una fotografía puede almacenar información en caso que el GPS esté activo en el dispositivo que se toma, informa del lugar exacto donde se toma la fotografía incluyendo la referencia Norte, Sur, puede informar las características del dispositivo y muchas cosas más, es lo que se conoce como metadatos, pero todo esto se almacena en los bits.

En estos momentos cualquier tipo de información digital se puede cifrar, dependiendo del tipo de información y de los parámetros requeridos existen software de uso libre y otros pagos y ya sean free o no, manejan algoritmos muy eficientes, en lo único que existen imposibilidades de cifrar la información es en las llamadas telefónicas, no es que no sea posible, solo que estos son métodos

especiales que requieren de pagos altos y no está disponible para todas las personas.

Aunque si bien el cifrado de información es una técnica utilizada con el fin de proteger información, éstos métodos también han sido utilizados mezclados con malware para realizar ataques cibernéticos y quizás el más famoso de ellos es el Ransomware, que lo que hace es encriptar la información de sus víctimas y obligaban a los usuarios que querían recuperarla pagar para que les entregaran las claves y se llegaba a un punto de impotencia, dado que se tenía la información en el computador pero no se podía acceder a ella, aunque muchos de los softwares utilizados tenían grietas y era posible recuperarla sin pagarle al atacante pero de igual manera necesitan de alguien que supiera realizar el proceso y es donde se ve que todo lo bueno también puede ser utilizado para lo malo.

Un algoritmo de cifrado es simplemente un modelo matemático que brinda la posibilidad de cambiar la estructura de los datos y volverlos a dejar en su manera original, además crea las estructuras de las contraseñas y dependiendo del algoritmo estas serán más fuertes o débiles, estos algoritmos se usan hace mucho tiempo inclusive mucho antes de la entrada de los computadores se usaban para realizar procesos de cifrado de informacion y en el criptoanálisis, aunque eran mucho más básicos.[53]

5.1.1 Criptografía simétrica: Este es el modelo de algoritmo de cifrado de información más antiguo existente, existen vestigios del uso de este modelo por parte del antiguo Egipto y del imperio Romano, pero de una manera muy básica, ya fue en la segunda guerra mundial donde éste empezó a mejorar de una manera muy notable, debido a que los ejércitos de ambos bandos empezaron a implementar máquinas que realizaban el proceso de cifrado y ya se consideraba mucho más complejo y esto ha evolucionado constantemente desde aquella época.

Ya en el uso de los sistemas el primero en usar un algoritmo simétrico sistematizado fue IBM en los años de 1970, Este algoritmo se llamaba Algoritmo Lucifer y fue creado por Horst Feistel, cuando este trabajaba para IBM era un algoritmo DES, si bien este tipo ya casi no se usan por ser debilidad en la época fue algo de gran impacto en la protección de información.

La forma de operar de los algoritmos simétricos es a través de una sola contraseña tanto para cifrar como para recuperar la informacion, un ejemplo muy básico de este nivel de encriptación es el compresor de información WinRAR, este programa tiene una opción de comprimir información con una contraseña y sin ésta no se puede recuperar, éste utiliza un método de cifrado simétrico y es muy complejo de romper si no se conoce la contraseña y es muy utilizado para compartir archivos por internet,

[53] Kaspersky. ¿Qué es el cifrado de datos? [En linea]. 2018. [Fecha de consulta: 15 abril 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

aunque hay aplicativos que permiten la creación de más de una clave y al mayor número de claves crea más complicación en un ataque de fuerza bruta.[54]

Los diferentes métodos de cifrado simétricos:

- Método de cifrado DES (Data Encryption Standard): Este sistema de cifrado de informacion fue desarrollado en los años de 1970 por el gobierno de EEUU en colaboración con IBM con la idea de brindarle a la gente un algoritmo de cifrado estandarizado para las redes de ordenadores y se encuentra basado en todas las teorías criptográficas que se conocían en el momento.

  Esta basa su funcionamiento en un sistema monoalfabético con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado, aunque este sistema de cifrado ya no se usa debido a que es muy débil, debido a que en un ataque de fuerza bruta en unas cuantas horas se puede decodificar. [55]

- Método de cifrado TDES: Conocido también como 3DES o triple DES, éste de igual manera se encuentra basado en el algoritmo, es más como una versión mejorada de éste, ya que el proceso de cifrado consiste en aplicar tres veces el proceso del DES, entonces lo que hace es que logre una encriptación de hasta 192 bits, aunque su eficacia real es de 112 bits que es lo que utiliza para encriptar la información y llegar a ser un poco más seguro, de igual manera no es recomendable usar software que utilice este algoritmo de encriptación, ya que de igual manera es muy factible romperlo con un ataque por diccionario.[56]

- Algoritmo RC2 o también conocido como ARC2: Es un método de cifrado de 64 bits, emplea la función de Feistel, división en bloque y aplicación en cajas, este algoritmo era mucho más práctico, debido a su velocidad de encriptado ya que llega a completar el proceso hasta en un tercio de tiempo de lo que

---

[54] GUTIÉRREZ, P. Tipos de criptografía: Simétrica, asimétrica e hibrida [En linea]. 2017. [Fecha de consulta: 16 abril 2020]. Disponible en: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

[55] GARCIA LARRAGAN. Aplicaciones, C. E., Criptografía, Etiquetas: Criptografía [En linea], 2017. [Fecha de consulta: 16 abril 2020]. Disponible en: http://mikelgarcialarragan.blogspot.com/2017/02/criptografia-xlix-el-algoritmo-des-i.html

[56] DEVNULL. ALGORITMOS DE CIFRADO I [En linea]. 2016. [Fecha de consulta: 16 abril 2020] Disponible en: https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/

demora el DES, de igual manera éste ya no se usa por el tema de que es muy débil.[57]

- Algoritmo ICE, es un método de cifrado de clave simétrica, este cifra la información, pero conservando su estructura de formato, utiliza la forma de cifrado en bloque, su generación de claves llega hasta los 64 bits, la estructura de este algoritmo ha mejorado y aún se utiliza, si bien no es el método más seguro; se sigue trabajando en mejoras lo que la ha llevado a tener una estructura más eficiente en frente al criptoanálisis, éste a diferencia del DES utiliza los 64 bits en cifrado lo que mejora su seguridad.[58]

- Algoritmo IDEA (International Data Encriptión Algorithm): Es un método que utiliza una clave de 128 bits sin paridad de bloques de datos de 64 bits, éste funciona tanto para cifrar como para recuperar la informacion, éste se considera bastante seguro y se encuentra en uso actualmente, este método fue creado en el año 1991, es de uso libre no comercial y es bastante seguro.[59]

- Algoritmo GOST: Es un método de cifrado de información, con origen en rusia que podría ser considerado la versión rusa del AES, ésta emplea bloques de 64 bits y claves de 256 bits y no ha podido y hasta el momento no hay resultados positivos en pruebas de vulnerabilidad, a pesar de que ha sido objeto de numerosas pruebas de criptoanálisis y demás estudios. El mensaje de entrada se divide en partes de bloques de 256 bits (ocho de 32 bits enteros) y el mensaje se completa añadiendo una cantidad de ceros como se requiere para completar la longitud del mensaje hasta que llega a los 256 bits. También funciona como función hash.[60]

- Algoritmo AES: Es un método de cifrado simétrico más utilizado hoy en día. La longitud de ser clave puede ser de 128 bits, 192 bits o 256 bits, este algoritmo es el que ha venido a remplazar el DES, está basado en sustituciones, permutaciones y transformaciones lineales, estas se ejecutan varias veces en bloques de datos de 16 bytes. Su forma de operar que cuando se cambia un solo bit, ya sea en la contraseña, o en los bloques de

---

[57]Sistemasumma. Algoritmo RC2. [En linea]. 2015. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://sistemasumma.com/2010/09/25/algoritmo-rc2/

[58] GOYOS MARTINEZ, V; HERNANDES ENCINAS L M DE FUENTES, J; GONZALEZ MANZANO, L; MUÑOZ, Martin. Cifrado de datos con preservación del formato [En linea]. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://www.tic.itefi.csic.es/CIBERDINE/Documetos/Cifrado%20de%20datos%20con%20preservaci%C3%B3n%20del%20formato.pdf.

[59] DEVNULL. ALGORITMOS DE CIFRADO I [En linea]. 2016. [Fecha de consulta: 16 abril 2020] Disponible en: https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/.

[60] Algoritmo de cifrado GOST 28147 89 c. Notas de arquitectura GOST (n.d.). [En linea]. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://newtravelers.ru/es/nastrojjka/algoritm-shifrovaniya-gost-28147-89-c-zamechaniya-po-arhitekture.html.

texto simple y claro, éste da como resultado un bloque de texto cifrado completamente nuevo, lo que lo hace muy complicado de descifrar. En los diferentes estudios realizados existen preocupaciones debido a las pocas rondas especificadas en el cifrado y además porque su forma matemática es muy ordenada.

Este algoritmo vio la luz del mundo en el año 1997, debido a la necesidad de remplazar el DES, que ya era muy débil, este fue creado en Bélgica y hoy en día es el más usado y por su seguridad no hay que preocuparse ya que estudios que realizaron ingenieros de Microsoft, mencionan que para romper este algoritmo se necesitarían "un billón de ordenadores que pudieran cada uno probar mil millones de claves por segundo, tardarían más de 2.000 millones de años en dar con una del sistema AES-128, y hay que tener en cuenta que las máquinas actuales sólo pueden probar 10 millones de claves por segundo.

Un caso de uso práctico hoy en día es que las transacciones bancarias que realizan las personas, cuando se realiza una compra de algún producto por internet o cualquier tipo de transacción monetaria se encuentra encriptada bajo este método, lo que lo convierte en el más usado y si bien en muchas ocasiones a personas les roban dinero por internet el problema nunca ha sido el algoritmo, es más bien que la gente es poco precavida.[61]

- Algoritmo Serpent: Es un método de cifrado de informacion simétrico que funciona a través de bloques, es considerado uno de los rivales más directos que tiene el AES, usa un tamaño de bloque de 128 bits y puede soportar una clave de tamaños de 128, 192 y 256 bits de longitud. El cifrado de éste consiste en 32 rondas de substitución y permutación obrando sobre cuatro bloques de 32 bits cada uno. En cada ronda éste usa 32 copias de la misma S-Box de 4-bit a 4-bit, es de igual manera muy seguro, hasta ahora por intermedio del criptoanálisis no ha sido posible vulnerarlo, pero llegara el momento en que las máquinas logren hacer estas operaciones, pero para entonces estos ya deben de haber evolucionado.[62]

5.1.2 Criptografía Asimétrica: Este tipo de cifrado maneja los métodos más potentes de criptografía existentes y su primer algoritmo data del año creada por Ralph Merkle, Whitfield Diffie y Martin Hellman, garantiza una comunicación totalmente segura entre el emisor y el receptor del mensaje y puede llegar a manejar llaves de hasta 4096 bits, superando de lejos al cifrado simétrico.

---

[61] Federal Information. ADVANCED ENCRYPTION STANDARD (AES) [En linea]. 2001. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

[62] DEVNULL. ALGORITMOS DE CIFRADO I [En linea]. 2016. [Fecha de consulta: 16 abril 2020] Disponible en: https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/.

Este algoritmo funciona de una manera diferente al simétrico, maneja un clave pública y una privada para realizar el cifrado de la información, en este caso la clave pública la tienen varias personas y esta es la que pide el software para realizar el encriptado de la información, después de realizar el proceso la única forma de acceder la información es con la clave privada, pero el proceso se puede de igual manera realizar a la inversa, que la información se cifre con la clave privada y se recupere con la pública, el hecho es que el proceso requiere de dos llaves y depende del usuario cual será la pública y cual la privada y cómo van a realizar el proceso.

Un ejemplo es que ambas claves sean privadas y que una la maneje el gerente de una compañía y la otra solo la tenga en el subgerente y las utilicen para compartir información entre ambos, en este caso no se definiría cual es la pública, ya que ambos podrían cifrar información y ambos acceder a esta y la privada y la pública cambiarían dependiendo quien realice la operación, pero el caso más común es que el gerente tenga la privada y el resto del personal la pública para que le envíen siempre la información a éste, aunque la idea también es que estas claves roten ya que al mantener siempre la misma contraseña aumento las posibilidades de fuga de informacion, por lo tanto la idea es que se genere una vez y al siguiente proceso estas cambien.

Este método es más utilizado para garantizar la veracidad de la información, ya que esto siempre va a generar un registro de donde salió la información y quien la recibe, además no van a existir excusas por parte del emisor ni del receptor, ya que proceso no va a permitir que en el transcurso del viaje de la información desde su creador hasta su receptor sea modificada, así que tanto el emisor como el receptor podrán negar la veracidad de esta.[63]

[63] Qué es la criptografía asimétrica [En linea]. 2020.[Fecha de consulta: 15 de octubre de 2020] Disponible en: https://academy.bit2me.com/que-es-criptografia-asimetrica/

Figura 3. Funcionamiento de la criptografía asimétrica

Fuente: GUEDEZ, A. Criptografía y seguridad informática: El ciclo de vida de claves y contraseñas y su relación con tus entornos digitales [En liena]. 2019. (Recuperado en 9 abril 2020) Disponible en: https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

Tipos de algoritmos de cifrado asimétricos:

- Algoritmo Diffie-Hellman: Bautizado así debido a sus creadores, esta basa su seguridad en la dificultad que existe en realizar cálculos de logaritmos discretos en un espacio finito y se emplea para crear la clave pública y la privada y este fue el pionero del método de cifrado asimétrico.[64]

  A este método se le ha descubierto una debilidad y es que es susceptible a ataques (MitM) de hombre en medio, donde el atacante se sitúa entre la máquina emisora y la receptora y concuerda una clave simétrica entre ambas partes, básicamente la clave pública y la privada van a ser la misma, el atacante suplanta el host a y el host B para que las máquinas creen la confianza y una vez así éste podrá acceder a la información, aunque este problema se puede solucionar por ejemplo: con un IDS, un EDR o Firewall dedicados a proteger de intentos de suplantación.[65]

- Algoritmo RSA (Rivest Shamir Adleman): Este método de cifrado fue desarrollado en los EEUU en el año 1997 por Ron Rivest, Adi Shamir y Leonard Adleman y de allí su nombre, probablemente es el algoritmo de cifrado asimétrico más famoso, este maneja igual una clave pública y una privada, pero además una es complemento de la otra, así que para recuperar

[64] DE LUZ, Sergio. Criptografía, Algoritmos de cifrado de clave asimétrica [En linea]. 2020 [Fecha de consulta: 23 abril 2020]. Disponible en: https://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/
[65] Ibíd.

la información es necesario tener la privada que corresponde a la pública, este sistema puede manejar claves de cifrado desde los 128 hasta los 4096 bits, por lo tanto se puede considerar el más potente que se utilice.

Básicamente con la tecnología existente en estos momentos es casi imposible romper este algoritmo, hasta ahora no existen pruebas exitosas en encriptados altos, se estima que en unos 25 años haya computadores lo suficientemente potentes que logren accederlo en un tiempo récord, pero en estos momentos se puede considerar el más seguro.[66]

- Algoritmo ElGamal: Este algoritmo está basado en los estudios realizados por el método Diffie-Hellman de logaritmos discretos, este fue creado en los años 80 con la idea de cifrado de información y firma digital, la metodología es similar a su antecesor factorizar números primos muy grandes de igual manera es un algoritmo muy potente y eficaz en su tarea.[67]

- Algoritmo DSA (Digital Signature Algorithm): Este algoritmo tiene como objetivo facilitar la firma de documentos digitales de una manera segura, no fue hecho con la finalidad de cifrar información; por lo tanto, esta tarea no la puede realizar, por lo que continúa mejorando debido a que éste se encuentra financiado por entidades gubernamentales, es prácticamente igual de seguro que el RSA, maneja claves desde los 1024 bits hasta los 3072, pero sus usos tienen enfoques muy diferentes.[68]

- Algoritmo de curva elíptica: Es un método de cifrado de información que se encuentra en desarrollo y tiende a ser el remplazo del RSA, debido a su algoritmo que no se basa en la factorización de números primos muy grandes que contienen una frecuencia ya predefinida, este al basarse en la fórmula de una curva elíptica puede tener diferentes variaciones en su proceso lo que dificulta mucho más la obtención de las contraseñas; además este método hace que la clave pública no se encuentre ligada directamente con la privada, entonces el que desee desencriptarlo no tendrá por dónde empezar, si bien este sistema no es 100% seguro con la tecnología actual no es posible descifrarlo.

  Este es el método de encriptado que utilizan las criptomonedas, es el estándar por ejemplo del Bitcoin, moneda digital que mueve cantidad de millones de dólares y hasta ahora su seguridad no ha sido vulnerada, si bien

---

[66] Ibíd.

[67] BRONCANO TORRES, Juan Carlos. Criptosistema ELGAMAL [En linea]. 2015. [Fecha de consulta: 23 abril 2020]. Disponible en: https://es.slideshare.net/juancarlosbroncanotorres/criptosistema-elgamal

[68] SHARMA, Monika, Digital Signature Algorithm (DSA) in Cryptography [En linea]. 2020. [Fecha de consulta: 23 abril 2020]. Disponible en: https://www.includehelp.com/cryptography/digital-signature-algorithm-dsa.aspx

han existido perdidas de esta moneda los problemas existieron por fracturas existentes en la codificación de sus plataformas más no por el método de cifrado.[69]

Criptografía Cuántica: Es un sistema más moderno del criptosistema de Vernam y no está incluido en un cifrado simétrico ni asimétrico, si bien existen procesos de encriptado de información, aún está el gran problema en todos estos y es tener una forma segura de hacer llegar la llave de un punto a un punto b sin que esta se pierda en el camino y la criptografía cuántica busca solucionar este que sería el último eslabón por superar en el tema de seguridad, ya que el medio utilizado para trasmitir la llave sería una trasmisión fotónica a través de fibra óptica, la informacion se trasmitirá a través de la luz, ya en este caso no habrían paquetes de información legibles, por lo tanto seria indescifrable, a esto apunta la tecnología de cifrado de información, pero aún es un método que va en progreso y que muy posiblemente termine por desarrollarse con la invención de las computadoras cuánticas, las cuales aún se encuentran en desarrollo y se estiman unos 20 años para que estas se encuentren en el mercado.[70]

En si todos los métodos de cifrado se aplican a la protección de la información y no tienen un objetivo específico a parte del algoritmo DSA que está dirigido estrictamente a la firma de documentos digitales y que está siendo impulsado por los gobiernos de varios países, el resto de algoritmos aplican a cualquier tipo de información, ya sea un documento de Word, una Imagen JPG, un archivo de audio MP3 o cualquier medio digital, entendiendo que todos estos tienen una estructura en bits y es esto lo que realmente se cifra, por lo tanto los algoritmos no reconocen de extensiones si no de la estructura invisible de los datos.

[69] M, Josep; MIRET; VALERA, Javier y VALLS, Magda - Grupo de Investigación Cryptography & Graphs [En liena]. 2015. [Fecha de consulta: 23 abril 2020]. Disponible en: http://www.criptored.upm.es/crypt4you/temas/ECC/leccion1/leccion1.html

[70] ¿Qué es la criptografía cuántica y cómo afectará al entorno empresarial? [En linea]. 2017. [Fecha de consulta: 23 abril 2020]. Disponible en: https://es.dynabook.com/generic/toshibytes-blogpost12-quantum-cryptography/

5.2 ESTABLECER LOS DIFERENTES MÉTODOS DE PROTECCIÓN DE LA INFORMACIÓN EN LA IMAGEN, EL AUDIO Y EL VIDEO.

El audio, el video y las imágenes se han convertido en medio de expresión mundial del arte, a través del talento de un sinnúmero de personas y a la misma vez se ha vuelto un medio laboral de manera directa o indirecta para muchísimas personas en el mundo generando grandes movimientos económicos de los cuales dependen muchas personas, algunas ganando grandes cantidades de dinero, otras obteniendo lo suficiente para sobrevivir y quizás aspirar a realizar otro proyecto más.

Es así como con el avance de la tecnología este negocio no solo se ha hecho rentable para los que lo trabajan de una manera legal, ya sea el que crea el contenido, el que lo distribuye y aun así hasta lo mismo estados que se benefician de los impuestos que estos generan, sino que también detrás de esto se ha creado un negocio paralelo e ilegal, que son los que se aprovechan de este tipo de material para poder sacar alguna ganancia sin reconocer los derechos de autor ni pagar impuestos. En este caso la tecnología está implicada directamente con la piratería o distribución ilegal ya sea de audio, imágenes o videos, dado que es muy evidente el avance tecnológico de la internet, quien es la plataforma que permite el intercambio de cualquier tipo de archivos entre personas, lo que ha facilitado la infiltración ilegal de este tipo de contenido, ya que la misma red no tiene la capacidad de entender que es correcto o incorrecto y de esto se aprovechan las personas.[71]

La informática hoy en el mundo, el cifrado de datos es la conversión de la información de un formato legible a uno codificado y solo se puede acceder a esta información descifrándolo, el cifrado es el elemento central de la seguridad de los datos y es la manera más sencilla de mantener los datos protegidos de las personas que no son el cliente final, este sistema es utilizado tanto por personas individuales, como por grandes corporaciones y este se utiliza en muchas actividades diarias que realizan los usuarios del computadores sin ni siquiera notarlos, como por ejemplo: enviar un correo electrónico, el cual va codificado y para las personas esta actividad es transparente.[72]

Básicamente cuando cualquier tipo de archivo sin importar su formato llega a la internet, este se vuelve de dominio público y así este tenga derechos de autor, los usuarios de la red los pueden utilizar de la manera en que les parezca y si bien existen unas normas y leyes que protegen al creador, por lo general las fuerzas del estado no le dedican tiempo a la piratería de información en pequeñas cantidades,

[71] CHÁVEZ ÁNGELES y SÁNCHEZ MEDINA. Industria de la información y piratería digital en México. Análisis económico de la protección de los derechos de autor [En linea]. 2017. [Fecha de consulta: 16 octubre 2020]. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2017000100053

[72] Kaspersky. ¿Qué es el cifrado de datos? [En linea]. 2018. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

que por lo general son para uso personal y para generar algún tipo de redito económico, aunque si se suman cada una de estas estas la cantidad llega a ser exagerada, pero es muy difícil de evitar este tema, en cambio los gobiernos dedican el tiempo a los grandes piratas, quienes pueden mover grandes cantidades de información y que si ganan dinero con esto.

Un tema muy común es que los piratas informáticos utilizan la información personal de los usuarios de las redes sociales, con el fin de crear cuentas falsas y estafar a las personas, ya sea ejerciendo algún tipo de presión o esparciendo malware a través de links, los usuarios ven estas cuentas y creen que es la persona con la que normalmente tratan y ahí caen en sus trampas y es en éste caso que existen herramientas que protegen esta información, más específicamente las imágenes que se agregan a estas páginas web, como es el caso de McAfee Social Protection, el cual impide que las personas puedan descargar o realizar capturas de pantalla de estos formatos, lo cual crea un perímetro de protección y evita el uso incorrecto de esta información personal.[73]

Otras maneras que se recomiendan con el fin de proteger las imágenes es aprovechar las ventajas que ofrecen las cámaras fotográficas que permiten agregar los derechos de autor, aunque esto solo deja un registro del dueño, mas no impide su utilización, otra forma que también es muy funcional es agregarles a este tipo de formatos una marca de agua para evitar el copyright, esto si bien no impide que sea utilizada si deja un rastro muy evidente, que conllevara a que desconocidos tiendan a dejarlas de lado y buscar otros elementos que se adapten más a lo que están buscando.[74]

Los correos electrónicos también ofrecen la posibilidad de encriptar las imágenes, los audios, videos y otros tipos de información si así lo requiere el usuario, por ejemplo: Microsoft Outlook utiliza un sistema de cifrado S/MIME (Secure Multipurpose Internet Mail Extensions), es un modelo de cifrado asimétrico que funciona con una clave publica y una privada; además permite agregar una firma con el fin de certificar el remitente, este sistema esta específicamente direccionado a la protección de los datos que se trasmiten por correo electrónico.[75]

Por otro lado, se encuentra la música y los videos que son básicamente una mezcla entre imágenes y audio, si bien la idea de utilizar el internet es que las personas que crean este tipo de contenido se den a conocer, pero de igual manera esperan tener

[73] Protecting Your Privacy on Social Media [En linea]. 2017. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://www.mcafee.com/blogs/consumer/consumer-threat-notices/protecting-privacy-social-media/

[74] SKAF, Eugenia. Redactora en Postcron.com, & Skaf, E. Marca de Agua: Qué es, por qué y cómo utilizarla. [En linea]. 2018. [Fecha de consulta: 18 noviembre 2020]. Disponible en: //postcron.com/es/blog/marca-agua-facebook/

[75] Admin. ¿Qué es S/MIME y cómo funciona? [En linea]. 2020. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://www.globalsign.com/es/blog/what-is-s-mime

algún tipo de redito económico por este material que es el fruto de su trabajo y es aquí donde se generan las perdidas ,ya que la mayoría de estas plataformas no han logrado controlar la descarga masiva de este tipo de contenido, si bien ahora se controla más y existen más leyes de derechos de autor, al mismo tiempo se ha creado más mecanismos con el fin de violar estos filtros que impiden sus descargas, a sabiendas que si se descarga una canción, unos videos o algunas películas, las fuerzas del estado no van a venir a detenerle, aunque técnicamente podrían hacerlo.

Uno de los grandes negocios que se mueven hoy en día es la creación de contenido para diferentes plataformas como YouTube, Facebook, Instagram, Twitter, Twitch y otras más, en donde el creador genera unas ganancias económicas por el material agregado, pero si la persona hizo uso de alguna canción, video o material creado por otra persona, inmediatamente el dinero que genere este producto ira a manos del dueños original y no del creador como tal, por hacer un uso deshonesto, esto es una parte como estas plataformas protegen los derechos de autor.[76]

En internet, puede ser YouTube la plataforma más grande del mundo en manejo de contenido digital de tipo musical y video y a su vez es la plataforma que permite el mayor número de descargas ilegales de este contenido, si bien estos han creado métodos para evitar el copyrigth entre los videos que se agregan, ya que si el software no lo detecta, el dueño original del producto puede hacer llamados de atención y si un canal obtiene más de tres llamados de atención, este se bloquea, esta es la forma que utilizan para evitar el plagio entre el contenido agregado, ya se de audio o de videos.[77]

Pero también está la parte de descargas, ya que hay una cantidad de programas y páginas web que descargan el tipo de contenido que hay en YouTube, si el usuario desea alguna canción, simplemente la busca y la descarga en su formato preferido o si hay algún video o película, ocurre de la misma manera y la plataforma no tiene restricciones, teniendo la capacidad de hacerla y este es un método de piratería muy eficaz y fácil de operar, existe de igual manera software que impide estas descargas, el cual se utiliza normalmente en cibercafés o sitios que ofrezcan el servicio de internet, con el fin de evitarse problemas legales, pero esto solo funciona a nivel local.

En el tema del audio, más específicamente la música, que es a la que se le puede sacar una ganancia económica, ocurre que evitar que le den un mal uso a esta, también es muy complejo, ya que existe mucha cantidad de software que permite la descarga ilegal de esta, desde diferentes plataformas, ahora existen plataformas

[76] ¿Qué es la creación de contenidos? [En linea]. [Fecha de consulta: 18 noviembre 020]. Disponible en: https://www.workana.com/i/glosario/creacion-de-contenidos/#:~:text=“Creación de contenidos” es un,tráfico web y clientes potenciales.

[77] WikiHow. Cómo desbloquear la infracción de copyright en YouTube. [En linea]. 2019. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://es.wikihow.com/desbloquear-la-infracción-de-copyright-en-YouTube

como: MUSO o AudioLock que ayudan a proteger este tipo de contenido, por ejemplo: AudioLock lo que hace es realizar una búsqueda en los buscadores más importantes de toda la música que se esté ofreciendo en sitios no permitidos y los inhabilita, evitando así que los creadores pierdan por este lado, pero este servicio cuesta y no todas los músicos tienen la posibilidad de pagarlos o quizás ni saben de su existencia, pero es una forma muy práctica de evitar este tipo de descargas ilegales de música.[78]

En si existen diferentes softwares y procedimientos que evitan el uso ilegal tanto de las imágenes, el audio y el video, cada herramienta tiene una forma de operar diferente, ya sea desde el punto de bloquearla totalmente el contenido, protegerla en su viaje por el internet o simplemente realizando un rastreo en los lugares donde reposan de manera ilegal y eliminando dese allí y el punto álgido es que la mayoría de este software tiene un costo y corre directamente por parte del interesado, además del desconocimiento que aún existe en esta área, donde la piratería genera millones de dólares en pérdidas alrededor del mundo y solo los artistas y productores más grandes, son los que soportan los embates de la ilegalidad.

[78] AudioLock.net. Music Anti-Piracy Content Protection. [En linea]. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://audiolock.net/

5.3 DETERMINAR CÓMO ACTÚA EL CIFRADO DE LA INFORMACIÓN EN LA IMAGEN, EL AUDIO Y EL VIDEO.

En el mundo de la informática existen una cantidad diferente de archivos de datos los cuales se clasifican según se extensión y reflejan la informacion que contienen de maneras diferentes, ya sea en forma de audio, en imagen, en audio y video, texto u otras formas existentes, pero en el fondo todos los archivos están compuestos en bits, y dependiente la extensión tienen una forma de acomodarse y esto seguirá siendo así, hasta tanto llegue de lleno la computación cuántica.

5.3.1 Para qué sirve el cifrado de información: El cifrado de las imágenes el audio y el video, sirve para hacer estos medios de informacion más seguros, esta técnica se aplica con el fin de que, en el momento de mover este tipo de formatos de un punto a otro, ya sea por internet o por algún dispositivo de almacenamiento de datos como una USB, un disco duro portátil, un CD u otro medio, no se pierda la confiabilidad y la integralidad de estos.

También hay algoritmos de encriptación de informacion que además de crear una protección sobre las imágenes, el audio el video, solicitan verificar la identidad del usuario final, antes de mostrar los datos que se contiene y para esto existen varios medios, como comprobación por huella dactilar, asociación por medio de la dirección MAC del equipo o de una IP, con el fin de garantizar siempre la integralidad de los archivos.

5.3.2 Como funciona el cifrado de la información: En el mundo de los sistemas las imágenes, el audio el video están compuestos por bits, datos que le dan la estructura a cada archivo, este tipo de formatos tienen una estructura definida, ya que siempre el inicio y el final van a ser el mismo y esto es lo que identifica el medio lector, para mostrar el contenido, al encriptar un archivo lo que hace el algoritmo es modificar el código binario que compone el archivo, lo que va ser que el elemento lector no pueda mostrar la información que este contiene, pero el algoritmo de igual manera tiene la capacidad de recuperar el orden del formato y estos procesos se pueden hacer a través de un software o modificando directamente el archivo.

En ejemplo: cualquier audio en formato Mp3 siempre va a iniciar con la siguiente firma, 49 44 33 04 00 00 00 , el de un archivo JPG inicia FF D8 FF y esta estructura nunca cambia, es lo que permite que el medio lector lo identifique, el truco del cifrado de la informacion es ocultar esta estructura y/o firma, para que el medio no lo entienda y tener la capacidad de revertirla, pero este proceso solo lo puede realizar el usuario final, que es el que conoce la contraseña de recuperación del archivo,

aunque también hay métodos de cifrado de informacion que no operan con una contraseña, simplemente ocultan los datos, esperando que no sean descubiertos.[79]

En el siguiente ejemplo se explicará cómo funciona el algoritmo Advanced Encryption Standard (AES), el cual es de clave simétrica y es uno de los más utilizados, debido a su confidencialidad en la realización de esta tarea y de lo complejo que es descifrarlo sin las contraseñas de acceso, su confidencialidad llega al punto que es el método utilizado por las entidades financieras para realizar sus operaciones en la red, pero también es compatible con imágenes, audio y video.

La operación de este algoritmo de clave simétrica es a través de operaciones en bloque y puede variar entre 128, 192 o 256 bits y en cada nivel lo que hace es aumentar el número de rondas, buscando aumentar la seguridad pero de igual manera aumenta el tiempo de la realización de la actividad y las posibilidades de hackearlo hasta ahora son casi imposibles y se prevé que este caiga cuando llegue la computación cuántica y el único hueco hasta ahora descubierto es con un ataque Meet-in-the-middle, pero este se centra más en capturar las contraseñas, haciéndose pasar por el receptor de la información, mas no atacando directamente el proceso de encriptado.

5.3.3 Como funciona el proceso de un algoritmo de cifrado en una imagen, audio o video: En este punto se explicará el proceso matemático del cifrado del algoritmo AES.

Como ya se ha explicado este funciona a través de rondas y dependiendo el nivel maneja una cantidad de rondas.

Tamaño de la clave	Número de rondas
128 bits	10
192 bits	12
256 bits	14

Este algoritmo ha sido aprobado por la nasa con el fin de cifrar la información confidencial del gobierno de los Estados Unidos de América.

El AES opera por rondas y dentro de cada ronda la entrada es un bloque de 128 bits y de igual manera la salida es de 128 bits, a estos 128 bits que durante la ejecución de cada ronda van cambiando se les llama estado.

La matriz de estado contiene 16 bytes acomodados en columnas de 2.
128 bits

[79] MAC, P. E., & MAC, E. ¿Qué es el código binario? [En linea]. [Fecha de consulta: 18 de noviembre 2020]. Disponible en: https://techlandia.com/codigo-binario-info_292179/

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

16 Bytes

Matriz de estado

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

De la misma manera que los estados, la clave y la subclave pueden estar compuestas en forma de matriz y trabajar de esta forma con ellas.
Estructura que utiliza AES para realizar el proceso de encriptado de información. Como ya se había explicado, este algoritmo utiliza rondas de 10,12 o 14, dependiendo el nivel de encriptado y por cada ronda se aplican unas etapas que hacen parte del proceso.

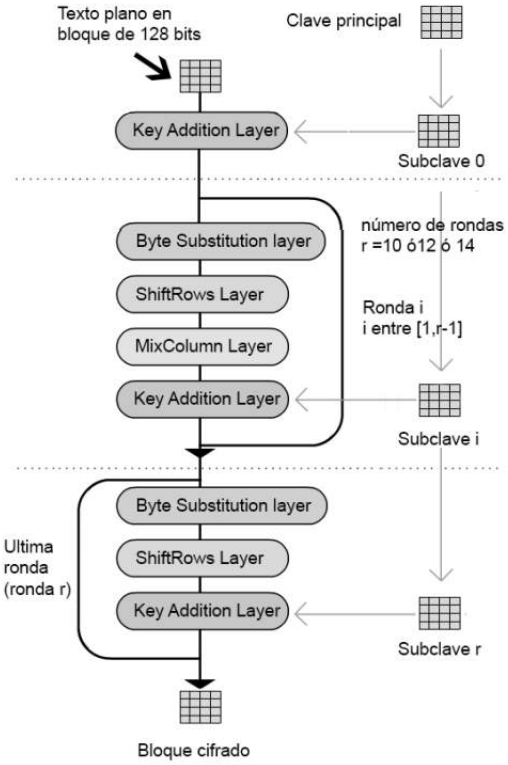
- Byte substitution layer: esta etapa sirve para añadir confusión al proceso y lo que hace es realizar una transformación no lineal en cada uno de los elementos del estado.
- ShiftRows layer: lo que hace es permutar los elementos del estado en diferentes posiciones.
- MixColumn layer: realiza operaciones con una matriz constante y la de estado.
- Key addition layer: esta etapa hace un XOR de la subclave y del estado actual, en esta etapa se generan las subclaves a partir de la clave principal y estas se crean en un proceso llamado key Schedule, la creación de subclaves depende de la cantidad de rondas del encriptado.[80]

[80] MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. [Fecha de consulta: 5 diciembre 2020]. Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Número de subclaves dependiendo en nivel de cifrado, existen un número igual de subclaves más uno por cada ronda.

Tamaño de la clave	Número de rondas	Número de subclaves
128	10	11
192	12	13
256	14	15

Figura 4. Proceso de encriptado AES



Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Byte Substitution layer:

Esta es la primera etapa de cada ronda y se repite el número de rondas que existen en el proceso, en esta etapa se sustituye cada byte por el valor asignado en las s-cajas, este valor asignado también sería de 8 bits.
Estas s-cajas son unas tablas en las que se encuentra el valor inverso de cada elemento de $GF(2^8)$ en valor hexadecimal multiplicado por una matriz constante y

sumado un vector constante, cada byte al tratarse de 8 elementos que pueden ser 0 o 1 entonces se tratan de elementos de $GF(2^8)$.

A cada uno de los bytes A_i de los 16 del estado se le asigna un byte B_i a través de las s-cajas.

$S(A_i) = B_i$

Para ubicar el valor en la tabla, lo que se hace transformar en hexadecimal los bytes y de acuerdo a esto de cada byte salen dos valores hexadecimales y se utiliza el primer valor para localizar la fila que se quiere en la tabla y el segundo para localizar la columna.[81]

Figura 5. S-Caja

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	3B	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	F7	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	2D
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1E	9E
E	E1	F8	98	11	69	D9	E8	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Ejemplo de cómo opera la S-Caja para ubicar los siguientes valores 01101011, entonces esto es igual a $6B_{hex}$

$S(6B_{hex}) = F7_{hex}$

Entonces en este caso ésta operación se realiza sobre los 16 bytes de la matriz del estado y se repite por cada ronda.

[81] MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. [Fecha de consulta: 5 diciembre 2020]. Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Ahora los valores de la S-Caja procede a encontrar la inversa del elemento $GF(2^8)$ y luego procede a multiplicarlo por una matriz constante y le adiciona un vector constante.

Sea A_i = { $a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7$ } un elemento de $GF(2^8)$ entonces B'_i = { $b'_1 + b'_2 + b'_3 + b'_4 + b'_5 + b'_6 + b'_7$ }, esta sería la inversa del cuerpo finito $GF(2^8)$[82]

En este caso al resolver la operación entre A_i y $B'_i = B_i$

B_i = { $b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7$ }

Figura 6. Ecuación de operación AES

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} mod 2$$

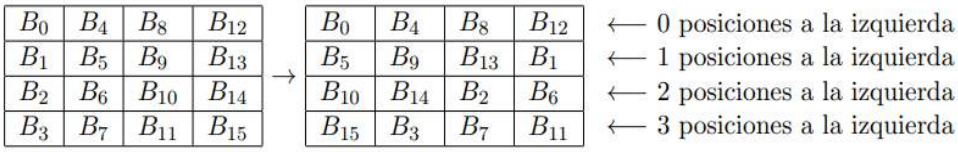
Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

ShiftRows Layer:

En esta etapa se realiza una transformación en ciclo sobre la matriz de estado. Sobre la segunda fila se realiza un desplazamiento de una posición a la izquierda, sobre la tercera fila se realiza un desplazamiento de dos posiciones a la izquierda y sobre la cuarta fila se realiza un desplazamiento de 4 posiciones a la izquierda. Entonces sobre la matriz de estado obtenida de la etapa anterior, B_i = { $b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7$ } se realiza esta trasformación.[83]

[82] Ibíd.
[83] Ibíd.

Figura 7. Operación de conversión



Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

MixColumn:

En este punto cada columna de la matriz de estado que se obtiene en el proceso ShiftRows, se opera por una matriz constante.

Figura 8. Matriz de estados

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_4 \\ B_9 \\ B_{14} \\ B_3 \end{pmatrix}$$

$$\begin{pmatrix} C_8 \\ C_9 \\ C_{10} \\ C_{11} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_8 \\ B_{13} \\ B_2 \\ B_7 \end{pmatrix}$$

$$\begin{pmatrix} C_{12} \\ C_{13} \\ C_{14} \\ C_{15} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_{12} \\ B_1 \\ B_6 \\ B_{11} \end{pmatrix}$$

Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Respecto a la matriz constante, los valores ”02”, ”03” y ”01” se refieren a valores hexadecimales, como elementos que hacen parte de $GF(2^8)$ serian ”0000 0010”, ”0000 0011” y ”0000 0001” respectivamente y se pueden expresar en forma polinómica con el fin de realizar las multiplicaciones.

$P(x) = x^8 + x^4 + x^3 + x + 1.$

Ejemplo:

Supongamos que $B_0 = 23_{hex} = 00100011 = x^5 + x + 1$ entonces al multiplicarlo por $02_{hex} = 00000010 = x$ quedaría:

$x \cdot (x^5 + x + 1)\ mod\ P(x) = x^6 + x^2 + x$

Key addition layer:

Key Schedule: Este proceso se realiza para generar las diferentes subclaves necesarias para las rondas, el proceso sería distinto dependiendo del tamaño de la clave principal y del número de rondas.

Key Schedule para claves de 128 bits: se parte desde la primera subclave que sería 0 SK, es la clave original de AES, y a partir de ella se obtienen el resto, por eso la cantidad de subclaves son igual al número de rondas más uno.[84]

Figura 9. Generación de subclaves

Sea $SK = \{sk_1, sk_2, sk_3, sk_4\}$ donde sk_i son cada una de las columnas con $i \in [1, 4]$.

$$SK = \begin{array}{|c|c|c|c|} \hline B_0 & B_2 & B_8 & B_{12} \\ \hline B_1 & B_5 & B_9 & B_{13} \\ \hline B_2 & B_6 & B_{10} & B_{14} \\ \hline B_3 & B_7 & B_{11} & B_{15} \\ \hline \end{array}$$

entonces

$sk_1 = \{B_0, B_1, B_2, B_3\}$
$sk_2 = \{B_4, B_5, B_6, B_7\}$
$sk_3 = \{B_8, B_9, B_{10}, B_{11}\}$
$sk_4 = \{B_{12}, B_{13}, B_{14}, B_{15}\}$

Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

[84] Ibíd.

Para obtener la siguiente subclave vuelve y se repite el proceso ya predefinido con los valores ya obtenidos y así se va hasta realizar todas las rondas, estos coeficientes son valores que pertenecen a $GF(2^8)$ y se denotan como RC [1] y avanza sucesivamente por cada ronda.[85]

Figura 10. Proceso para obtener la siguiente subclave

$$
\begin{aligned}
RC[1] &= x^0 = (00000001)_2 = 01_{hex} \\
RC[2] &= x^1 = (00000010)_2 = 02_{hex} \\
RC[3] &= x^2 = (00000100)_2 = 04_{hex} \\
RC[4] &= x^3 = (00001000)_2 = 08_{hex} \\
RC[5] &= x^4 = (00010000)_2 = 10_{hex} \\
RC[6] &= x^5 = (00100000)_2 = 20_{hex} \\
RC[7] &= x^6 = (01000000)_2 = 40_{hex} \\
RC[8] &= x^7 = (10000000)_2 = 80_{hex} \\
RC[9] &= x^8 = (00011011)_2 = 1b_{hex} \\
RC[10] &= x^9 = (00110110)_2 = 36_{hex}
\end{aligned}
$$

Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Ahora ya definido como opera el algoritmo en cada una de las rondas, se pasa a ver como se obtiene la columna de la subclave siguiente, partiendo de la clave presente para buscar la siguiente.

Figura 11. Ejecución del algoritmo en cada una de las rondas

$$
SK[4] = \begin{array}{|c|}\hline B_{12} \\ \hline B_{13} \\ \hline B_{14} \\ \hline B_{15} \\ \hline \end{array} \rightarrow \text{Posiciones 1 hacia arriba} \begin{array}{|c|}\hline B_{13} \\ \hline B_{14} \\ \hline B_{15} \\ \hline B_{12} \\ \hline \end{array}
$$

$$
\text{Se pasa por la S-caja} \rightarrow \begin{array}{|c|}\hline S(B_{13}) \\ \hline S(B_{14}) \\ \hline S(B_{15}) \\ \hline S(B_{12}) \\ \hline \end{array}
$$

Primera columna de la subclave

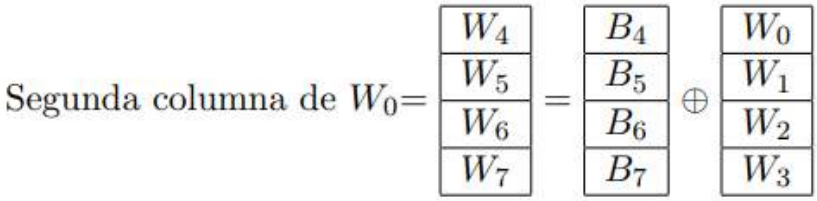
$$
W_0 = \begin{array}{|c|}\hline W_0 \\ \hline W_1 \\ \hline W_2 \\ \hline W_3 \\ \hline \end{array} = \begin{array}{|c|}\hline B_0 \\ \hline B_1 \\ \hline B_2 \\ \hline B_3 \\ \hline \end{array} \oplus \begin{array}{|c|}\hline S(B_{13}) \\ \hline S(B_{14}) \\ \hline S(B_{15}) \\ \hline S(B_{12}) \\ \hline \end{array} \oplus \begin{array}{|c|}\hline RC[1] \\ \hline 00 \\ \hline 00 \\ \hline 00 \\ \hline \end{array}
$$

Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

[85] Ibíd.

El resto de columnas de la siguiente subclave se genera realizando un XOR de la columna anterior y la columna de la misma posición, pero de la subclave anterior.

Figura 12. Obtención de la segunda columna



Fuente: MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. (Recuperado 5 diciembre 2020). Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Y de esta manera se obtienen todas las subclaves, ya que el proceso se repite de igual manera por cada ronda hasta cumplir todo el ciclo, el cual depende de la seguridad que se vaya a implementar.

Existen diferentes algoritmos de cifrado de imágenes, audio y video y esto no es algo muy común para la mayoría de personas, pero en el mundo de la seguridad informática estas herramientas son de vital importancia y poder conocer su funcionamiento matemático revela la verdadera complejidad de estos métodos tan exitosos y de igual manera es en los cálculos donde se han hallado muchas debilidades que permiten ser corregidas, con el fin de ir cerrando puertas que permitan las fracturas del cifrado de información.

5.4 IDENTIFICAR HERRAMIENTAS Y O PLATAFORMAS QUE PERMITAN EL BORRADO DE LOS METADATOS.

5.4.1 Qué son los metadatos, el manejo que le dan las plataformas sociales y herramientas que permitan el borrado de estos: Lo primero es entender que son los metadatos, este es un término creado en los años 60 para dar nombre a un conjunto de datos, pero su evolución real y toma de importancia en el mundo digital se dio a partir del año 2004 hasta la fecha. La palabra proviene de la mezcla de una palabra griega “Meta” que traducida quiere decir después de o más allá de, y del vocablo latino “Datum” que significa dato, de ahí lo que quiere decir la palabra más allá de los datos, es lo que describe la información que contiene un recurso, es como la información que describe otros datos.[86]

El uso del concepto de metadatos es conocido en el mundo de la informática, pero este es anterior al mundo de la internet, pero ahora ha tomado una mayor relevancia ya que las grandes compañías utilizan esta información con el fin de gestionar sus grandes cantidades de datos, dado que con esta información es más fácil organizarla y crear una gestión más eficiente.[87]

Los metadatos tienen muchos usos hoy en día, en virtud de que son un tipo de información muy flexible que se puede ajustar a varias tareas, tales como: facilitar búsquedas y análisis, mejorar el manejo de los datos, ayuda en la integración, facilita la estandarización, ayuda a generar informes de una manera más eficiente, generan mayor confiabilidad y seguridad en la información y otras ventajas de más.[88]

Los metadatos fotográficos o datos EXIF, es una serie de información que se almacenan en todas las fotografías, sin importar el dispositivo que se utilice para captar ésta, ya sea un celular, una cámara fotográfica, una Tablet u otro; los metadatos almacenan datos del dispositivo que se utilizó, parámetros del disparo, datos propios de la imagen y si el dispositivo tiene la función de GPS este va informar del lugar y posición en que fue realizada la fotografía.

Como se puede denotar, en la imagen Figura 4. Guitarras acústicas, se le puede extraer mucha más información de la que se puede ver y el gran problema es que la mayoría de las personas no son conscientes de la información que estas poseen, ya que llega al punto de que una imagen puede tener acceso a un servidor, a una

---

[86] PowerData, Metadatos, definición y características [En linea]. [Fecha de consulta: 29 noviembre 2020]. Disponible en: https://www.powerdata.es/metadatos

[87] Ibíd.

[88] Qué son los Metadatos [En linea]. [Fecha de consulta: 29 noviembre 2020]. Disponible en: https://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos

cuenta bancaria y mucha información muy importante, pero mirando lo común que hacen las personas es tomar fotos con sus dispositivos móviles y subirlas a las redes sociales y esto lo hacen si verificar sus metadatos y si esta información se conserva se prestaría para realizar diferentes delitos informáticos o hasta más graves, porque si bien muchas personas ignoran esta información hay otras que si las conocen y la pueden aprovechar, por ejemplo: un delincuente por medio de una fotografía podría identificar el lugar de vivienda de su víctima, donde trabaja a dando sale y eso es un peligro.[89]

Figura 13. Guitarras acústicas

Fuente: Propia.2019. (Recuperado 27 marzo 2020)

Figura 14. Metadatos de la Imagen Anterior.

EXIF

Make	Canon
Model	Canon EOS Rebel SL3
Orientation	Horizontal (normal)
XResolution	72
YResolution	72
ResolutionUnit	inches
ModifyDate	2019:08:02 18:36:48
Artist	
YCbCrPositioning	Co-sited

Copyright	
ExposureTime	1/20
FNumber	7.1
ExposureProgram	Manual
ISO	800
SensitivityType	Recommended Exposure Index
RecommendedExposureIndex	800
ExifVersion	0231
DateTimeOriginal	2019:08:02 18:36:48
CreateDate	2019:08:02 18:36:48
ComponentsConfiguration	Y, Cb, Cr, -
ShutterSpeedValue	1/21

Fuente: Propia. 2020. (Recuperado 27 marzo 2020)

[89] Ibíd.

5.4.2 Leyes que protegen la información personal en las plataformas sociales en Colombia: En Colombia existen normas de protección de la información, pero como tal no existe ninguna ley por parte del congreso de la república, ni normas ni nada por el estilo emanada por algún órgano de control del país, que regule las plataformas de redes sociales tales como: Facebook, Instagram, Twitter, Telegram, Tinder y otras más que existen, por lo tanto cuando un usuario residente del país accede a estas plataformas está aceptando el contrato que esta página establece y no existe una norma que lo proteja ante la información que se pueda filtrar desde allí, si bien se están implementando proyectos que impidan ciertas libertades en estas plataformas, va más dirigido a información que publiquen las personas que afecten a otras, más la plataforma como tal la puede conservar si es su deseo.

Aunque en Colombia existe la ley 1273 del 2009 referente a los delitos informáticos, que protegen a las personas contra cualquier delito, por ejemplo: un delito muy común en una relación de pareja, ocurre que termina la relación y una de ellas guardo fotos intimas de la otra y por rencor las sube a una plataforma de estas(redes sociales), lo que hace la persona afectada es poner la respectiva denuncia ante la Policía Nacional o la Fiscalía General de la Nación, lo que hace la plataforma es retirar el material por contenido no apropiado, pero tanto la Policía como la Fiscalía no pueden tomar ninguna acción contra la plataforma, en este caso lo que se hace es que el órgano investigador se contacta con los representantes de estas plataformas para que por intermedio de ellos, envíen la informacion de la persona que agrego estos datos, la plataforma envía el perfil del usuario, la Mac del equipo y lo que le hayan solicitado o lo que ellos quieran enviar, ya que como se menciona no existe una norma que los obligue por lo menos en Colombia.[90]

En Colombia ya en algún momento la corte constitucional citó a los representantes de Facebook y Google en el país con el fin de evaluar las políticas que estaban siguiendo ante las repetitivas conductas insultantes de muchos usuarios ante otros, además de amenazas que estaban surgiendo a través de estos medios y que no estaban siendo filtrados de una manera adecuada y ante esto el país expidió la resolución 4885 del 13 de febrero del 2020, donde se llega a la conclusión que Facebook Colombia S.A realiza una actividad que involucra el tratamiento de datos privados de personas, en el desarrollo de su actividad comercial que es la de servicios publicitarios, y a la cual le exigen que cumpla con la protección debida de la informacion y le dan un plazo hasta el 14 de junio del presente año para que imponga estas medidas, esto se puede considerar un gran avance que hace el país con el fin de establecer un control contra estas grandes plataformas mundiales de redes sociales que de cierta manera actúan a su acomodo.[91]

---

[90] Jur, LEY 1273 DE 2009 [En linea]. 2009. LEY 1273 DE 2009. [Fecha de consulta: 19 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[91] Superindustria ratifica que Facebook Colombia debe fortalecer medidas de seguridad para proteger datos personales de más de 31 millones de colombianos: Superintendencia de Industria y Comercio. [En linea]. 2020. [Fecha de consulta: 13 diciembre 2020]. Disponible en:

En el país la entidad encargada de regular las actividades de las plataformas de redes sociales es la superintendencia de industria y comercio (SIC), hasta la fecha solo se han pronunciado con la resolución antes mencionada en contra de una de estas plataformas, buscando que estos implementen mayores medidas de seguridad para así mantener protegidas alrededor de treinta y un millones de cuentas que se encuentran vigentes en el país y lo que puede ocurrir es que si no cumplen, esta plataforma podría salir del mercado Colombiano, pero es muy poco probable que esto ocurra, independientemente que acaten o no las solicitudes del gobierno nacional y hasta la fecha ha sido la única solicitud formal ante estos grandes emporios.

En Colombia también existe la ley 1581 del año 2012 para la protección de datos personales, en esta ley si se establece que las empresas que recolecten información de sus usuarios son los responsables de su protección, pero no se especifica nada con los metadatos de las imágenes, el hecho es que cuando una persona accede a estas plataformas como ya se mencionaba anteriormente, estos ponen una cláusulas que normalmente las personas no leen y lo que allí se menciona es que la personas son responsables del material que comparten y que además le otorgan el permiso de que esta plataforma trate esta información de la manera que más le convenga y mientras no exista alguna fuga no pasara nada.[92]

Realizando una investigación en diferentes sitios de internet no se encontró ningún tipo de informacion que evidencie leyes que protejan los metadatos de las imágenes, si bien en el año 2019 la unión europea impuso una multa de más de cinco millones de dólares a Facebook por fuga de información privada que afecto a más de ochenta y siete millones de personas, esto debido a su incumplimiento de políticas de seguridad, dado a que esta empresa se encuentra registrada legalmente en EEUU, la demanda se trasladó hasta allí y la justicia fallo a favor de la multa impuesta por la EU.

A nivel mundial la mayoría de países han establecido al igual que Colombia unas políticas y leyes de protección de información, pero esto ha sido a nivel general, no solo para las redes sociales que funcionen en su país, sino también para las entidades bancarias, entidades del estado y cualquiera que tenga a su cargo el resguardo de datos personales, más la ley recae es cuando se permiten fuga de ésta al exterior, pero al interior la pueden usar para lo que necesiten, e increíblemente el país más atrasado en este tipo de leyes son los EEUU, debido a

https://www.sic.gov.co/slider/superindustria-ratifica-que-facebook-colombia-debe-fortalecer-medidas-de-seguridad-para-proteger-datos-personales-de-más-de-31-millones-de-colombianos#:~:text=Mediante la resolución 4885 del,otras, se concluyó lo siguiente:&text=•-,Facebook Colombia S.A.S.,el Tratamiento de Datos personales.&text=Sin esta información, esa sociedad colombiana no podría prestar sus servicios.

[92] Jur, LEY ESTATUTARIA 1581 DE 2012 [En linea].2012. [Fecha de consulta: 19 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

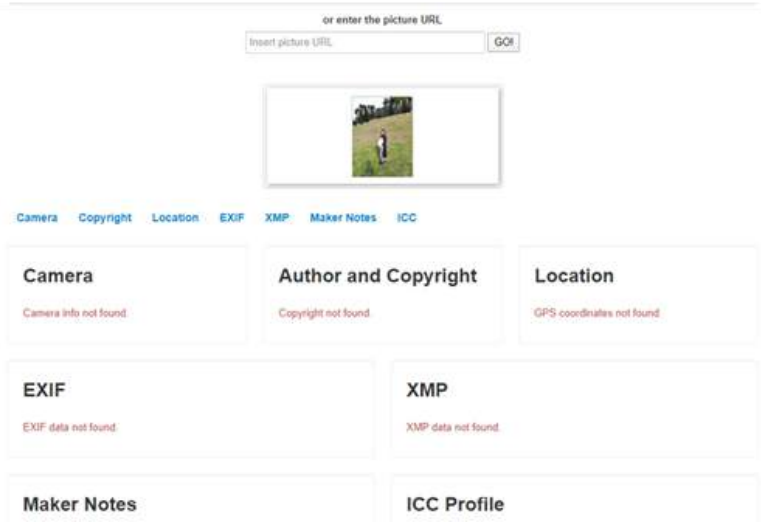
que la regulación se hace por estados y hasta el momento muy pocos estados las han reglamentado y en este caso debería ser el país que regule a esta plataformas en cuanto al uso de la información y de los metadatos, ya que todas estas se encuentran registradas allí y se rigen bajo estas normas.

Aunque no existen leyes directamente contra la protección de los metadatos, hasta cierto punto las de protección de datos influyen un poco, entendiendo que esta información que se almacena en una foto es propiedad del usuario y al subirla a una plataforma de estas pasa a ser responsabilidad de estos, por lo tanto ellos se encargan de borrar los metadatos de las imágenes que quedan publicadas y si alguien las llega a descargar no va poder acceder a esta, pero no como se menciona no hay una ley que los obligue y en las políticas de privacidad que se establece con los usuarios no se menciona esto.

Lo otro que ocurre es que no existe restricciones para la descarga de las imágenes, entonces de una manera muy simple se sustrajo una imagen de Facebook y se le realizo un escaneo simple de metadatos y no se detectó nada, aunque no se sabe si realizando un escaneo a mayor profundidad se logre hallar algo, aunque lo más posible es que no, esto se hace debido a las leyes de protección de datos, pero de igual manera ellos almacenan registro de los metadatos y demás información de los usuarios y aunque es muy poco posible que alguien acceda a estos servidores y la sustraiga, sigue siendo una posibilidad, este mismo año se realizó un informe en donde se afirmaba que la página de citas Tinder tubo una nueva fuga de información, más precisamente se dice de unas siete mil fotografías que incluían sus metadatos, ya que muchas de estas se habían filtrado por internet con la información de la personas y como ocurrió con esta plataforma, puede ocurrir con cualquiera, por lo tanto la ley debería obligarlos es a borrarlos definitivamente y no simplemente a que traten de protegerlos, porque en algún momento fallan sus protocolos de seguridad.

Cabe recalcar que la imagen utilizada a continuación fue sustraída de Facebook con el debido permiso de la persona que aparece en la imagen y es utilizada solo con fines educativos.

Figura 15. Extracción de metadatos de una imagen descargada de Facebook



Fuente: Imagen escaneada de Facebook, Renson Torres Cardona, Online metadata and exif viewer. [Recuperado 10 abril 2020]. Disponible en: http://metapicz.com/#landing

En este caso plataformas como Facebook e Instagram tienen políticas internas del manejo de la información que recolectan de sus usuarios.

Facebook explica en sus políticas de seguridad que recolecta mucha más información de la que las personas digitan en su portal, por ejemplo: si una persona descarga una foto de esta plataforma, ya no va a encontrar los metadatos de ésta, aunque eso no quiere decir que los borraron, en este caso ellos toman toda es información y la procesan para entender más las personas.

Igualmente estos puede extraer muchas más información que los metadatos que tienen las imágenes, aparte generan registros de la posición del GPS del celular, a las páginas que entran, a que le da me gusta, quienes son sus amigos, donde los etiquetan, muy seguramente poseen más información de los usuarios que las mismas centrales de inteligencia y todo esto lo utilizan para crear perfiles de consumo de sus usuarios y así poder enviarles publicidad de su gusto, pero lo realmente preocupante es toda la información personal que poseen de las personas y lo que pueden llegar hacer esta, teniendo en cuenta que esta plataforma ya fue multada por precisamente permitir fuga de información y que al final los perjudicados no recibieron un solo peso como reparación, unos cometen el error y otros sacan provecho, pero los afectados se quedan así y éste no es un solo inconveniente de Facebook, es de todas las plataformas que de una u otro manera almacenan información de las personas.[93]

[93] Política de datos. [En linea]. 2020. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://es-es.facebook.com/about/privacy

Lo que se explica es que ellos recogen todos los metadatos de las imágenes que se le suministran, además acceden a los dispositivos desde donde se acceden a las plataformas, le hacen un seguimiento a las personas, esto con el fin de poder enviarle publicidad de los productos que pautan con ellos, ya que esta plataforma y general obtienen sus ganancias de la publicidad, pero le especifican a las personas que ellas se quedan con toda esta información y al observar las políticas de protección de información de otras plataformas como Instagram, Twitter, Tinder y otra cantidad más es prácticamente lo mismo, básicamente cualquier plataforma de esta puede ubicar a cualquier persona en el mundo.[94]

Esto hace notar que las personas ya han perdido toda su libertad y privacidad, porque cualquier actividad que se realice desde un dispositivo móvil, computador u otro está siendo registrado y no precisamente por DIOS; además hay que entender que eso que se cree tan seguro en realidad no lo es, ya que si empresas como Facebook que son tan poderosas han permitido la fuga de información, que se puede esperar de las demás, por eso es mejor crear protocolos de seguridad propios y no esperar a que otros lo hagan.

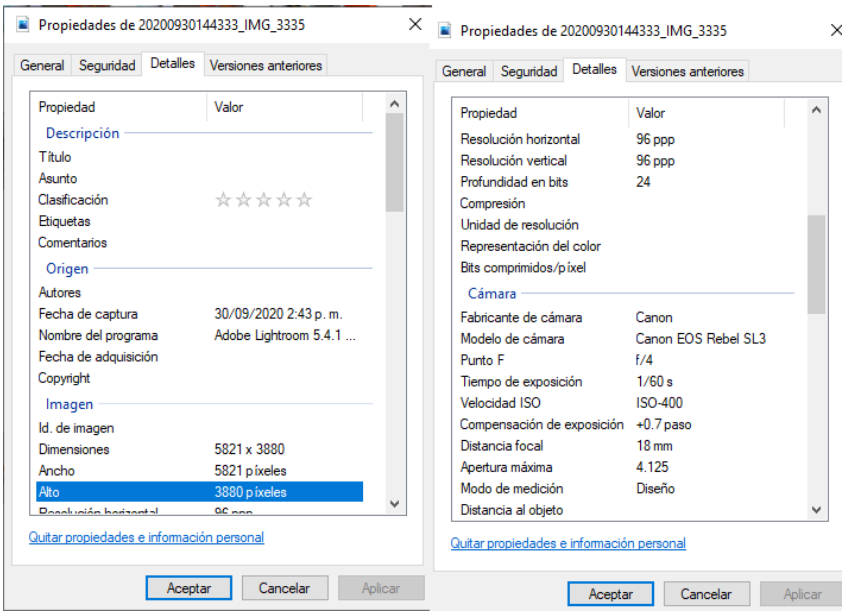
Al final se puede denotar que las organizaciones gubernamentales de los países están tomando acciones con el fin de proteger la información de las personas y esto se ha visto con grandes multas impuestas a las plataformas de redes sociales y a su vez estas mismas también han tomado sus acciones, pero si éste tipo de información es la que mueve estas compañías, solo se podrá llegar al punto de que estas no filtren y que la mantengan protegida y darle vía libre a la que si bien es confidencial, no pone en riesgo a las personas.

5.4.3 herramientas que permiten el borrado de los metadatos: este punto es muy importante de realizar, ya que las imágenes y otros tipos de formatos pueden almacenar diferente información personal, que se puede prestar para cometer ilícitos por parte de personas inescrupulosas que se aprovechan de estas fallas, como saber en donde vive la persona, sitios que frecuenta, el equipo con que capto la imagen y otro tipo de datos, que no deberían estar al acceso de cualquier persona y es por eso que se debe tratar de eliminar esta información antes de que otras personas las accedan.

Existen una cantidad diferente de plataformas que permiten el borrado de estos datos, inclusive los mismos elementos con que se toman las fotos dan la opción de deshacerse de la informacion que se considera privada y solo dejar la que es informativa, pero existe un método manual para hacer esta tarea, la cual es abrir las propiedades de la imagen e ir a detalles y borrar lo que la persona dueña de esta desee, aunque en ocasiones el borrado no es de fondo, solo se lleva lo visible.

[94] Ibíd.

Figura 16. Metadatos de una imagen



Fuente: GUEVARA RODRIGUEZ Karen Ximena, 2020 (Recuperado 13 de diciembre 2020)

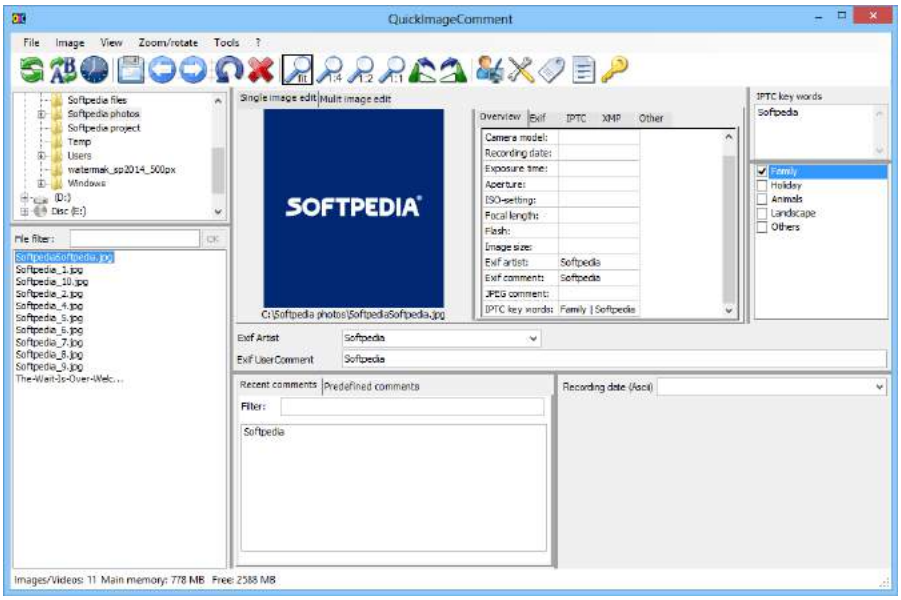
En la imagen de “Metadatos de una imagen” se puede observar una variedad de información, que para la mayoría de las personas es irrelevante, pero por ejemplo se pude conocer la fecha en que esta fue tomada, también se encuentra el tipo de cámara con que fue capturada y este ya puede ser un objetivo de un delincuente, por eso se recomienda borrar estos datos y en este caso solo es seleccionar el ítem requerido y eliminar, no es de mayor complejidad el procedimiento.[95]

Pero si se quiere llegar a profundizar un poco más se puede hacer uso de herramientas como: QuickImageComment, la cual esta diseñada para verificar todos los metadatos que posee una imagen y hacerlos visibles para sus usuarios y de una manera gráfica e ingresar a ellos y eliminar todos los que no son necesarios por una u otra razón.[96]

[95] Cómo borrar los metadatos de las fotos [En linea]. 2020. [Fecha de consulta: 13 diciembre de 2020]. Disponible en: https://www.ionos.es/digitalguide/paginas-web/diseno-web/borrar-los-metadatos-de-las-fotos/

[96] ONIEVA, David. Edita y elimina los metadatos de tus fotos para evitar peligros. [En linea]. 2020. [Fecha de consulta: 13 diciembre 2020]. Disponible en: https://www.softzone.es/programas/imagen/edita-elimina-metadatos-fotos-peligros/

Figura 17. Metadatos mostrados por QuickImageComment

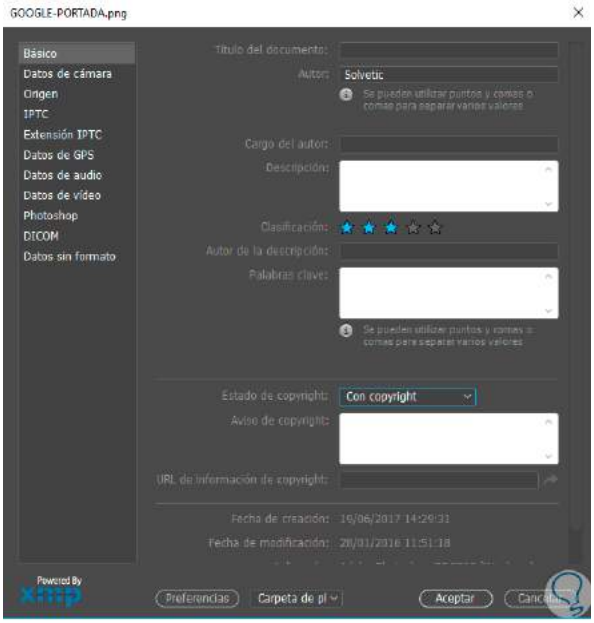


Fuente: Download QuickImageComment 4.37 [En linea]. 2020. (Recuperado 13 diciembre 2020]. Disponible en: https://www.softpedia.com/get/Multimedia/Graphic/Digital-Photo-Tools/QuickImageComment.shtml

En el mercado hay diferentes aplicaciones direccionadas al trabajo de fotografía, las cuales permiten realizar diferentes modificaciones a estas, como en ejemplo: la más famosa de todas adobe Photoshop, la cual no solo cumple funciones de interferir en la parte visual de la imagen, sino que también tiene la capacidad borrar los metadatos que puede almacenar una imagen, esta labor se puede realizar de dos formas, una es al estar trabajando en la imagen se va a la pestaña de file y luego en file info y se desplegaran los metadatos y la otra manera es al momento de guardar la imagen, se da la opción de guardado para web y en la lista desplegable de metadatos se selecciona ninguno.[97]

[97] DISEÑO, Solvetic. Añadir y editar metadatos EXIF de imagen o foto en Photoshop [En linea]. 2017. [Fecha de consulta: 13 diciembre 2020]. Disponible en: https://www.solvetic.com/tutoriales/article/4007-anadir-editar-metadatos-exif-imagen-foto-photoshop/

Figura 18. Metadatos en Adobe Photoshop



Fuente: DISEÑO, Solvetic. Añadir y editar metadatos EXIF de imagen o foto en Photoshop [En linea]. 2017. (Recuperado 13 diciembre 2020]. Disponible en: https://www.solvetic.com/tutoriales/article/4007-anadir-editar-metadatos-exif-imagen-foto-photoshop/

Otra manera que se puede aplicar para el borrado de metadatos es abrir la imagen con un editor como Paint, esta herramienta que se ve tan ineficaz y solo para diversión, posee una cantidad de ventajas y acciones que permiten la realización de un sin número de trabajos, lo que es agregar cualquier edición a la imagen imperceptible y luego se guarda y en este punto se pierden una cantidad de metadatos, al igual que si la imagen va agregada por ejemplo: en un archivo de Word, Power Point o algún programa similar.

Las plataformas de redes sociales en donde se puede compartir imágenes, pero de donde también se pueden sustraer, manejan procesos internos de borrado de metadatos, aunque si se va a las políticas de seguridad de estas compañías no mencionan que estos datos serán borrados, aunque si se descarga una imagen de cualquiera de estos sitios, la información valiosa ha sido borrada, aunque lo que realmente hacen es sustraerla, aprovechar lo importante para lanzarle publicidad de los productos que le puedan interesar y la almacenan en sus bases de datos y la foto que queda publicada, ya no va a tener estos datos que ellos aprovechan de manera comercial.[98]

[98] Política de datos. [En linea]. 2020. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://es-es.facebook.com/about/privacy

Existen diferentes métodos para poder borrar los metadatos de las imágenes y algunos de esto son de un uso muy sencillo y accesible para cualquier persona del común, pero el desconocimiento hace que la población en general comparta información privada que en muchas ocasiones termina siendo utilizada de manera fraudulenta por personas inescrupulosas que se aprovechan de los errores que comenten otros.

6 CONCLUSIONES

La existencia de la criptografía de datos, data de hace muchos años atrás en donde hombres estudiosos de diferentes ciencias hallaron maneras diferentes de esconder información que se debía de mover de un lugar o que simplemente debía de estar resguardada, entendiendo que esta poseía un alto valor para diferentes partes interesadas y que por tal motivo empezó a cifrarse, pero fue ya en épocas modernas que se le dio el nombre de criptografía o cifrado a estos métodos de proteger la información.

Con al avance de la tecnología y el paso del tiempo se han ido implementando diferentes métodos matemáticos para lograr el cifrado de la información de una manera más eficiente y segura, entendiendo que los primeros modelos matemáticos se fueron haciendo débiles a medida que las computadoras se hicieron más potentes y aumentaron su capacidad de procesar mayor cantidad de datos en menos tiempo, esto obligo a que los algoritmos para encriptar informacion fueran evolucionando para cumplir la demanda de seguridad del mercado.

El cifrado de datos es un método utilizado para el transporte de información digital de un punto A, a un punto B, y si bien existen métodos de cifrado que son extremadamente fuertes, no siempre estos se adaptan a las necesidades de las personas, por eso en estos casos se usa el que brinda una buena seguridad y que funcione de una manera eficiente, ya que estos procesos pueden tardar bastante tiempo dependiendo de la forma de operar del algoritmo.

Hoy en día dependiendo de la tarea a realizar se aplica un cierto modelo matemático de cifrado de información, ya sea para enviar un correo electrónico, un mensaje a través del celular, realizar una transferencia electrónica o cualquier actividad en la red, aunque para la mayoría de las personas esta actividad es imperceptible, es de vital importancia en muchos procesos, mantiene la confiabilidad de las personas en las diferentes plataformas que de manera transparente protegen los datos a través de diferentes métodos de encriptado.

Aunque existen una cantidad de formatos diferentes que poseen un sinnúmero de datos que proporcionan informacion a los usuarios y parte de estos son las imágenes, el audio y el video que aparte de ser información digital, hacen parte de unas de las industrias que mueven más dinero en el mundo y la que beneficia a muchas personas que se encuentran inmersas en este negocio, ya sea de una manera legal o ilegal, reconociendo que esta problemática afecta mayormente a países tercermundistas en donde las pocas posibilidades económicas de las personas crean un mercado y otras se benefician de este mismo.

Aparte del gran negocio que manejan este tipo de informacion, también está la parte personal de las personas que poseen datos privados ya sea en imágenes, audio o video y esta se mantiene algún riesgo latente de ser robada o que sea utilizada de maneras inadecuadas por personas inescrupulosas, y para esto existen diferentes métodos de proteger este tipo de información, por ejemplo en el tema de las fotografías, las cámaras tienen la opción de agregar los derechos de autor, que si bien no protegen, si dejan el rastro del propietario. Además existen softwares que permiten proteger todo tipo de informacion, ya sea de manera local o en plataformas sociales, pero aunque esta tecnología haya avanzado bastante, aún existe un gran problema en este punto, sin que el cifrado de informacion, haya logrado dar un solución definitiva a la infiltración de este tipo de formatos.

De igual manera los estados a través de sus gobiernos han creado diferentes leyes con el fin de proteger los derechos de autor, pero la eficacia de estas aún son muy débiles, debido que la mayoría de piratería de las imágenes, los audios y videos se manejan en cantidades pequeñas y los entes policiales enfocan sus esfuerzos en atacar a grandes estructuras que generan una mayor visibilidad, pero que al final no disminuye en mucho el problema, ya que la ley se encuentra mal estructura, debido a que estas deberían enfocarse más en el mundo digital y no como se lleva ahora en un mundo físico, porque ahí la guerra está perdida.

Por otro lado, tenemos los metadatos en las imágenes, estos pueden capturar una cantidad de información que llega al punto de resultar peligrosa si las fotografías digitales llegan a caer en manos equivocadas, ya estas pueden inclusive ofrecer la ubicación casi exacta de su creador, además que los metadatos tienen muchos más usos que el de solo proporcionar información.

Reconociendo que las leyes de protección de información privada se encuentran muy atrasadas al avance en la tecnología y que este no solo es un problema de Colombia, sino que también es de otros países, incluso estos que son considerados del primer mundo con tecnologías de punta, aún no han logrado entender el poder que tienen los metadatos de los archivos, no solo de las fotografías sino de toda la informacion digital.

Ver el verdadero poder de las grandes plataformas de internet como: Facebook, Google, Instagram, Twitter, YouTube y otras grandes redes sociales, que se han convertido en emporios, compañías que son casi intocables, y aunque algunos países han logrado avanzar en algo, para estas son minucias, se considera que el sector financiero tiene un gran poder tanto económico, como de influencia, pero estas plataformas web se pueden dar el lujo de pagar millonarias multas y seguir funcionando como si nada.

Entender también que los mayores protocolos de protección de información se lo han impuesto las mismas plataformas de internet, que ellos son los que han decidido que hacer y que no hacer con la información, ya que los gobiernos de los países

han sido incompetentes para crear verdaderas leyes que protejan la información privada de las personas, ya que si bien las redes sociales y otras páginas web no obligan a las personas a que se suscriban a estos sitios, estos si terminan abusando de toda la información que poseen de las personas, estas plataformas manejan muchas más información de una persona de la que maneja el propio estado, en este punto existe un diferencia abismal.

En conclusión, existen diferentes métodos de cifrado de las imágenes, el audio y el video, pero estos métodos están direccionados más a la protección de información relevante y no se ha trabajado en el problema de la piratería y se está quedando más relegada las leyes de cada país en los cuales existen delitos que generan mayor afectación a la población y sus fuerzas de seguridad se dedican a perseguir este tipo de delitos, ya que el robo de una canción, una imagen o un video no genera mayor afectación y si en cambio alguna familia subsiste a través de estas operaciones ilegales y más bien se busca a los grandes piratas, pero el mayor problema está en los pequeños que de uno en uno suma el mayor porcentaje de este delito que se convirtió en una fuente de generar recursos para la subsistencia de personas menos favorecidas.

7 RECOMENDACIONES

En la realización del estudio del presente trabajo se considera que el cifrado de información no es una fuente de solución muy eficaz para el problema de la comercialización ilegal del audio y el video, pero si es muy útil en el proceso de trasmitir esta información a través de dispositivos digitales o a través de la red, cuando se busca que ésta vaya de punto a punto.

En este caso una de las opciones más viables para solucionar el problema de la piratería por parte de los países, es que sus gobernantes incentiven la creación de empresas legales que mejoren los ingresos de toda la población en general y con esto lograr desmotivar la adquisición de este tipo de entretenimiento de una manera ilegal y además que las personas que subsisten de este negocio, tengan otras posibilidades de ingresos acordes a la ley, sin depender de estas actividades ilegales.

Es muy importante también realizar campañas a través de los ministerios de telecomunicaciones de los países acerca del manejo del cifrado de la información y en cómo se pueden aplicar estos procedimientos, para que las personas empiecen hacer uso de éstos, entendiendo que cada día están más y más sumergidos en un mundo cibernético que avanza a pasos agigantados, pero que andan en este sin manejar las precauciones necesarias y debido a ésto se presenta el crecimiento descontrolado de los delitos informáticos, habiendo maneras tan sencillas de protegerse.

También a través de estos ministerios se deben de manejar campañas de sensibilización de los metadatos, algo desconocido para la mayoría de la población e ignorado por otros y aprovechado por otros, ya que esta información no debería ser de manejo público, pero en eso se ha convertido y a las personas se les puede delegar la responsabilidad de esta, pero no sin antes enseñarles que es y es de competencia de los ministerios de tecnologías por lo menos informar de su existencia.

De igual manera se deben de implementar normas y leyes que permitan el control de las diferentes plataformas de redes sociales, financieras y demás, que las obliguen a darles un manejo adecuado y confidencial a los datos privados de las personas, ya que es evidente que estas bases de datos se convirtieron en un negocio y la información privada de los usuarios van de compañía en compañía sin ningún tipo de restricción y es importante que lo gobiernos intervengan y detengan este tráfico de datos que aparenta ser legal.

8 BIBLIOGRAFÍA

Abc.es. (2012, November 07). Cinco consejos para proteger tu imagen en internet. Retrieved from https://www.abc.es/tecnologia/abci-consejos-proteger-imagen-201210270000_noticia.html

Admin.¿Qué es S/MIME y cómo funciona? [En linea]. 2020. [Fecha de consulta 18 de noviembre de 2020]. Disponible en: https://www.globalsign.com/es/blog/what-is-s-mime

Algoritmo de cifrado GOST 28147 89 c. Notas de arquitectura GOST (n.d.). [En linea]. [Fecha de consulta 15 de noviembre de 2020]. Disponible en: https://newtravelers.ru/es/nastrojjka/algoritm-shifrovaniya-gost-28147-89-c-zamechaniya-po-arhitekture.html

ASALE, R. -., & Rae Algoritmo: Diccionario de la lengua española [En linea]. 2019. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://dle.rae.es/diccionario

Binance Academy. Historia de la Criptografía [En linea]. 2020. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://academy.binance.com/es/articles/history-of-cryptography

Boxcryptor. Cifrado AES y RSA [En linea]. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://www.boxcryptor.com/es/encryption/

CHADHA, Aman; SUSHMIT, Mallik; CHADHA, Ankit; RAVDEEP, Johar y M. Roja, Mani. Dual-Layer. Video Encryption using RSA Algorithm, Referencia de la revista: International Journal of Computer Applications [en linea]. 2015. [Fecha de consulta: 28 marzo 2020]. Disponible en: https://arxiv.org/abs/1509.04387

CHÁVEZ ÁNGELES y SÁNCHEZ MEDINA. Industria de la información y piratería digital en México. Análisis económico de la protección de los derechos de autor [En linea]. 2017. [Fecha de consulta: 16 octubre 2020]. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2017000100053

Ciberseg1922. ¿Qué son los algoritmos de cifrado? Tipos y características [En linea]. 2020. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://ciberseguridad.com/servicios/algoritmos-cifrado/#Definicion_de_algoritmos_de_cifra

Cifrado asimétrico: Transmisión segura de datos [En linea]. 2020. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.ionos.es/digitalguide/servidores/seguridad/cifrado-asimetrico/

Cifrar mensajes de correo. [En linea]. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://support.microsoft.com/es-es/office/cifrar-mensajes-de-correo-373339cb-bf1a-4509-b296-802a39d801dc

Cómo borrar los metadatos de las fotos [En linea]. 2020. [Fecha de consulta: 13 diciembre 2020]. Disponible en: https://www.ionos.es/digitalguide/paginas-web/diseno-web/borrar-los-metadatos-de-las-fotos/

¿Cómo funciona realmente la piratería de películas y series? [en linea]. 2020.[Fecha de consulta: 14 octubre 2020]. Disponible en: https://smartprotection.com/es/media/como-funciona-realmente-pirateria-online-peliculas-series/

Criptografía simétrica y asimétrica [En linea]. 2014. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://infosegur.wordpress.com/unidad-4/criptografia-simetrica-y-asimetrica/

DEFINICIÓN DE AUDIO [En linea]. 2016. [Fecha de consulta: 12 abril 2020]. Disponible en: https://definicion.de/audio/

DISEÑO, Solvetic. Añadir y editar metadatos EXIF de imagen o foto en Photoshop [En linea]. 2017. [Fecha de consulta: 13 diciembre 2020]. Disponible en: https://www.solvetic.com/tutoriales/article/4007-anadir-editar-metadatos-exif-imagen-foto-photoshop/

Download QuickImageComment 4.37 [En linea]. 2020. [Fecha de consulta: 13 diciembre 2020]. Disponible en: https://www.softpedia.com/get/Multimedia/Graphic/Digital-Photo-Tools/QuickImageComment.shtml

Entiende el concepto de piratería digital y aprende a protegerte [en línea]. 2019. [Fecha de consulta: 14 octubre 2020]. Disponible en: https://obsbusiness.school/es/blog-investigacion/propiedad-intelectual/obs-presenta-el-informe-de-pirateria-digital

Federal Information. ADVANCED ENCRYPTION STANDARD (AES) [En linea]. 2001. [Fecha de consulta: 15 de noviembre de 2020]. Disponible en: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

DUARTE, Gabriel. Definición de Video, [En linea]. 2008. [Fecha de consulta: 27 marzo 2020]. Disponible en: https://www.definicionabc.com/tecnologia/video.php

GARCIA LARRAGAN. Aplicaciones, C. E., Criptografía, Etiquetas: Criptografía [En linea], 2017. [Fecha de consulta: 16 abril 2020]. Disponible en:

http://mikelgarcialarragan.blogspot.com/2017/02/criptografia-xlix-el-algoritmo-des-i.html

Gbadvisors, G. E., & Gbadvisors, V. E. Criptografía y seguridad informática: El ciclo de vida de claves y contraseñas y su relación con tus entornos digitales. [En linea]. 2020. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

GOYOS MARTINEZ V, HERNANDES ENCINAS L M DE FUENTES J, GONZALEZ MANZANO L, MUÑOZ Martin, Cifrado de datos con preservación del formato [En linea]. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://www.tic.itefi.csic.es/CIBERDINE/Documetos/Cifrado%20de%20datos%20con%20preservaci%C3%B3n%20del%20formato.pdf

Guía de ``Gnu Privacy Guard''. Capítulo 2: «Sistema de cifrado simetrico» [En linea]. [Fecha de consulta: 27 marzo 2020] Disponible en: https://www.gnupg.org/gph/es/manual/c190.html.

GUTIERREZ Ángel. Criptografía y criptoanálisis en las dos guerras mundiales [En linea]. [Fecha de consulta: 15 octubre 2020]. Disponible en: https://www.acta.es/medios/articulos/comunicacion_e_informacion/052063.pdf

GUTIÉRREZ, P. Tipos de criptografía: Simétrica, asimétrica e hibrida [En linea]. 2017. [Fecha de consulta: 16 abril 2020]. Disponible en: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Herramientas web para la enseñanza de protocolos de comuicaion. DES [En linea]. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

M Josep; Miret; VALERA, Javier y VALLS Magda. Grupo de Investigación Cryptography & Graphs [En liena]. 2015. [Fecha de consulta: 23 abril 2020]. Disponible en: http://www.criptored.upm.es/crypt4you/temas/ECC/leccion1/leccion1.html

BRONCANO TORRES, Juan Carlos. Seguir, Criptosistema ELGAMAL [En linea]. 2015. [Fecha de consulta: 23 abril 2020]. Disponible en: https://es.slideshare.net/juancarlosbroncanotorres/criptosistema-elgamal

Jur, LEY 1273 DE 2009 [En linea]. 2009. LEY 1273 DE 2009. [Fecha de consulta: 19 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Jur, LEY ESTATUTARIA 1581 DE 2012 [En linea].2012. [Fecha de consulta: 19 octubre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Kaspersky. ¿Qué es el cifrado de datos? [En linea]. 2018. [Fecha de consulta: 15 abril 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

LAGMIRI; BAKHOUS. Audio Encryption Algorithm Using Hyperchaotic Systems of Different Dimensions. [en linea], 2018. [Fecha de consulta: 27 marzo 2020]Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.FE29FFEC&lang=es&site=eds-live&scope=site

LEY 1915 DEL 12 DE JULIO DE 2018. [En linea]. Colombia: Presidencia de la Republica. 2018. [Fecha de consulta: 15 octubre 2020]. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201915%20DEL%2012%20DE%20JULIO%20DE%202018.pdf

LinkFang. Criptografía híbrida [En linea]. 2020. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://es.linkfang.org/wiki/Criptograf

LUO, X. et al. A New Image Encryption Algorithm Using Homogenized Chebyshev-Arnold Map [en linea].2018. [Fecha de consulta: 25 marzo 2020]. Disponible en: http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edseee&AN=edseee.8652390&lang=es&site=eds-live&scope=site

DE LUZ, Sergio. Criptografía, Algoritmos de cifrado de clave asimétrica [En linea]. 2020 [Fecha de consulta: 23 abril 2020]. Disponible en: https://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/

Mac, P. E., & Mac, E. ¿Qué es el código binario? [En linea]. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://techlandia.com/codigo-binario-info_292179/

MANTILLA, S y VÁSQUEZ, G. Conocimiento, metodología e investigación contable. 2a. edición, Editorial Horizontes. Universidad Nacional de Colombia. Seminario de Investigación (Metodología de la Investigación), 1997, Pag 243.

MARRERO TRAVIESO. La Criptografía como elemento de la seguridad informática [En linea]. 2003. Ciudad de La Habana. [Fecha de consulta: 8 octubre 2020]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

MARTINEZ DE LA TORRE J. Cifrado de clave privada: AES [En linea]. 2016. [Fecha de consulta: 5 diciembre 2020]. Disponible en:http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

MINTIC. Ley 1273 de 2009 [En linea]. 2009 [Fecha de consulta: 23 abril 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

ONIEVA, David. Edita y elimina los metadatos de tus fotos para evitar peligros. [En linea]. 2020. [Fecha de consulta 13 de diciembre de 2020]. Disponible en: https://www.softzone.es/programas/imagen/edita-elimina-metadatos-fotos-peligros/

PÉREZ PORTO y MERINO. Definición de cifrado. [en linea] 2016, [Fecha de consulta: 16 marzo 2020] Disponible en: https://definicion.de/cifrado/

Política de datos. [En linea]. 2020. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://es-es.facebook.com/about/privacy

PowerData, G. Metadatos, definición y características [En linea]. [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.powerdata.es/metadato

Protecting Your Privacy on Social Media [En linea]. 2017. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://www.mcafee.com/blogs/consumer/consumer-threat-notices/protecting-privacy-social-media/

Publimetro. Piratería se come 40% del mercado musical; mata talentos y estrellas [en línea]. 2016. [Fecha de consulta: 14 octubre 2020]. Disponible en: https://www.publimetro.cl/cl/home/2016/11/04/pirateria-se-come-40-mercado-musical-mata-talentos-estrellas.html#:~:text=

¿Qué es el cifrado? [En linea]. 2019 [Fecha de consulta: 19 octubre 2020]. Disponible en: https://www.internetsociety.org/es/encryption/what-is-encryption/

Qué es la criptografía asimétrica [En linea]. 2020 [Fecha de consulta: 23 abril 2020]. Disponible en: https://academy.bit2me.com/que-es-criptografia-asimetrica/

¿Qué es la criptografía cuántica y cómo afectará al entorno empresarial? [En linea]. 2017. [Fecha de consulta: 23 abril 2020]. Disponible en: https://es.dynabook.com/generic/toshibytes-blogpost12-quantum-cryptography/

Qué son los Metadatos [En linea]. [Fecha de consulta: 29 noviembre 2020]. Disponible en: https://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos

Redacción 01/02/2020 11:37, & Redacción, La esteganografía digital, la técnica que oculta información en archivos multimedia [En linea]. 2020. [Fecha de consulta: 18 noviembre 2020]. Disponible en: https://www.lavanguardia.com/vida/20200201/473240641630/la-esteganografia-digital-la-tecnica-que-oculta-informacion-en-archivos-multimedia.html

Rome and Art. EL CIFRADO DE JULIO CÉSAR [En linea]. 2016. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://www.romeandart.eu/es/arte-cifrado-cesar.html#:~:text=Julio

Salmocorpblog. Criptografía simétrica y asimétrica [En linea]. 2017. [Fecha de consulta: 9 octubre 2020]. Disponible en: https://salmocorpblog.wordpress.com/2017/01/27/criptografia-simetrica-y-asimetrica/

SHARMA, Monika. Digital Signature Algorithm (DSA) in Cryptography [En linea]. 2020. [Fecha de consulta: 23 abril 2020]. Disponible en: https://www.includehelp.com/cryptography/digital-signature-algorithm-dsa.aspx

Significado de Imagen, [en linea]. 2017. [Fecha de consulta: 27 marzo 2020]. Disponible en: https://www.significados.com/imagen/

Sistemasumma. Algoritmo RC2. [En linea]. 2015. [Fecha de consulta: 15 noviembre 2020]. Disponible en: https://sistemasumma.com/2010/09/25/algoritmo-rc2/

SKAF Eugenia. Redactora en Postcron.com, & Skaf, E. Marca de Agua: Qué es, por qué y cómo utilizarla. [En linea]. 2018. [Fecha de consulta: 18 noviembre 2020]. Disponible en: //postcron.com/es/blog/marca-agua-facebook/

Superindustria ratifica que Facebook Colombia debe fortalecer medidas de seguridad para proteger datos personales de más de 31 millones de colombianos: Superintendencia de Industria y Comercio. [En linea]. 2020. [Fecha de consulta: 13 diciembre 2020]. Disponible en: https://www.sic.gov.co/slider/superindustria-ratifica-que-facebook-colombia-debe-fortalecer-medidas-de-seguridad-para-proteger-datos-personales-de-más-de-31-millones-de-colombianos#:~:text=Mediante la resolución 4885 del,otras, se concluyó lo siguiente:&text=•-,Facebook Colombia S.A.S.,el Tratamiento de Datos personales.&text=Sin esta información, esa sociedad colombiana no podría prestar sus servicios.

Tecnología + informática. ¿Qué es la criptografía? [En línea]. 2020. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/

Todo lo que tiene que saber sobre firma electrónica y firma digital [en línea]. 2020. [Fecha de consulta: 11 marzo 2020]. Disponible

en:https://www.portafolio.co/economia/todo-lo-que-tiene-que-saber-sobre-firma-electronica-y-firma-digital-541460

Universidad Politècnica de València. «¿Qué es una firma electrónica? » [en linea]. 2012. [Fecha de consulta: 24 marzo 2020] Disponible en: https://www.upv.es/contenidos/CD/info/711250normalc.html

VELASCO, J. J. Diario Turing. Criptografía: Breve historia de la criptografía [en línea]. 2014. [Fecha de consulta: 11 marzo 2020]. Disponible en: https://www.eldiario.es/turing/criptografia/Breve-historia-riptografia_0_261773822.html

VENTURINI, G.¿Qué es la Criptografía? [en línea]. 2020 [Fecha de consulta: 14 octubre 2020] Disponible en: https://www.tecnologia-informatica.com/que-es-la-criptografia/#:~:text=Básicamente