AUNANDO E INVESTIGANDO MÉTODOS DE ENCRIPTACIÓN DES Y 3DES

Diego Capera Tole[a]
Darwin Arias Tique[b]
Carlos Castellanos Calero[c]
Iván Vargas González[d]

[a] Facultad Tecnológica, Ingeniería en telemática, Universidad Distrital Francisco José de Caldas
drcaperat@correo.udistrital.edu.co

[b] Facultad Tecnológica, Ingeniería en telemática, Universidad Distrital Francisco José de Caldas dariast@correo.udistrital.edu.co

[c] Facultad Tecnológica, Ingeniería en telemática, Universidad Distrital Francisco José de Caldas
caacastellanosc@correo.udistrital.edu.co

[d] Facultad Tecnológica, Ingeniería en telemática, Universidad Distrital Francisco José de Caldas
idvargasg@correo.udistrital.edu.co

Resumen— Este documento pretende dar a conocer al lector información acerca de los algoritmos de Encriptamiento Des y 3Des, esto mediante la investigación en diferentes fuentes de datos de certificación científica y referenciadas en el documento. En la actualidad la usabilidad de estos algoritmos no es frecuente debido a la obsolescencia, pero sin duda fueron base para otros algoritmos de encriptación más robustos y que brindan más fiabilidad y seguridad para el usuario final en la actualidad. Con este documento se procura una visión crítica y argumentada para el conocimiento del lector acerca de la temática tomando como base investigaciones realizadas por los autores del documento, para esto es necesario dar a conocer la importancia de los algoritmos de encriptación y la usabilidad que tienen hoy en día.

***Palabras clave*— Des, 3Des, Encriptación, Seguridad.**

***Abstract*—** This document aims to provide the reader with information about the Des and 3Des Encryption algorithms, this through research in different sources of scientific certification data referenced in the document. Currently, the usability of these algorithms is not frequent due to obsolescence, but without a doubt they were the basis for other more robust encryption algorithms that provide more reliability and security for the end user today. This document seeks a critical and argued view for the reader's knowledge of the subject based on research carried out by the authors of the document, for this it is necessary to make known the importance of encryption algorithms and the usability that they have today in day.

***Keywords*— Des, 3Des, Encryption, Security**

I. INTRODUCCION

La criptografía se enfoca en el cifrado y descifrado, para lo cual se entiende que cifrado es el proceso de convertir un texto normal a un formato ilegible por cualquier ente no autorizado que pretenda acceder a la información, por descifrado se habla cuando se realiza el proceso de convertir el texto previamente cifrado en un texto que sea legible para el usuario final.

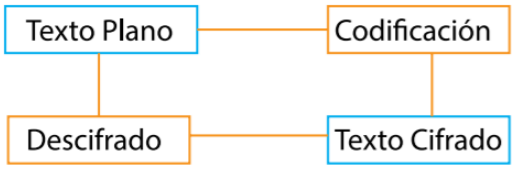

Fig. 1. Flujograma de cifrado y descifrado

Tomando como base la imagen podemos explicar el ciclo de encriptación mediante el siguiente ejemplo:

- Supongamos que un remitente desea enviar un mensaje "Hola amigo" a un destinatario.
- Este mensaje original que también es llamado "Texto claro" se convierte en bits aleatorios que usualmente se conoce como "Texto cifrado" y esto se realiza mediante un algoritmo y el uso de claves.
- El texto cifrado se transmite mediante el medio de ejecución demandado.
- El texto cifrado llega al destinatario, pero este posee en su sistema el mismo algoritmo y posee la clave original para poder descifrar el mensaje.

La criptografía tiene 5 objetivos fundamentales los cuales deben tenerse en cuenta, son los siguientes:

- Autenticación: Indica que se debe tener la capacidad de identificar al receptor y remitente evitando que cualquier intruso acceda a la información.
- Privacidad: Asegurar que nadie más aparte del receptor pueda leer el mensaje, esta característica muchas veces es llamada sistema seguro, es decir, solo las personas autenticadas en los sistemas podrán interpretar el mensaje.
- Integridad: Tomar precauciones de que el mensaje que recibe el receptor no se encuentre alterado a como fue enviado.
- No repudio: Mecanismo que ayuda a indicar e identificar si el remitente efectivamente envió un mensaje.
- Fiabilidad y disponibilidad: Es imprescindible que el usuario final cuente con el sistema seguro 24 horas y no dejar brechas abiertas para que algún intruso pueda acceder a su información privada.

Los algoritmos DES y 3DES son algoritmos de cifrado simétrico, pero ¿Qué es un algoritmo de cifrado simétrico?

Es necesario tener en cuenta que existen los algoritmos de cifrado simétrico y asimétrico, la diferencia entre estos dos

se basa en función del tipo de claves que utilizada cada uno de estos que son utilizadas para cifrar/descifrar mensajes. En este artículo nos compete abordar los algoritmos de cifrado simétricos.

Estos algoritmos de cifrado simétrico son conocidos como criptografía de clave única, como su nombre lo indica, solo se utiliza una clave. En el proceso del flujograma de la figura 1. Tanto en remitente como el receptor deben ponerse de acuerdo para establecer una clave única para cifrar y descifrar el mensaje, esta clave tratarse de manera confidencial y solo las dos partes deben conocerla. Se entiende que este paquete comprende de dos partes fundamentales: el mensaje y la clave, se cifra la información dejando los datos totalmente ilegibles que tienen casi la misma longitud del mensaje descifrado.

Para una información clara del proceso podemos visualizar la siguiente figura donde describe el papel empleado por la clave secreta para el cifrado y descifrado del mensaje.

Fig. 2. Proceso de clave para criptografía simétrica

Teniendo en cuenta que los algoritmos DES y 3DES hacen parte del conjunto de cifrado simétrico, estos a su vez se integran dentro del conjunto de cifrado por bloques. En criptografía el cifrado por bloques opera en una serie de grupos de bits los cuales poseen una longitud que ya se encuentra definida. Esto indica que el "Texto claro" posee la misma longitud de tamaño que el "Texto cifrado".

¿Qué es el algoritmo DES?

El algoritmo DES (Data Encryption Standard) fue el primer estándar que fue publicado por el NIST (Instituto nacional de estándares y tecnologías). Este estándar fue diseñado por IBM, en el año 1974 se estableció formalmente como un estándar. Este algoritmo utiliza una clave de 56 bits, los bloques de entrada son de 64 bits y su bloque de salida de igual valor. La clave parece realmente una cantidad de 64 bits, pero un bit en cada uno de los 8 octetos se utiliza para la paridad impar en cada octeto. Hay muchos ataques y métodos registrados hasta ahora los que explotan las debilidades de DES, lo que hizo un cifrado de bloques inseguro.

¿Qué es el algoritmo 3DES?

El algoritmo 3DES se implementó por razones que puedeN ser un poco obvias y es para reforzar las fallas presentadas por DES, esto con el fin de no tener que crear un nuevo sistema o algoritmo desde sus inicios, más bien tomando las bases de DES y reforzándolo. Triple DES extiende el tamaño de su clave, pues existe un dicho que dice: "Entre más larga sea la longitud de la clave, más difícil va a poder ser vulnerada" 3DES extiende el tamaño de su clave aplicando 3 veces el mismo algoritmo los cuales llevan una sucesión de 3 claves diferentes. El tamaño de la clave es

de 128 bits (3 veces más grande que DES). Triple DES siempre ha sido considerado con cierta sospecha, ya que el algoritmo original nunca fue diseñado para ser usado de esta manera, pero sin defectos graves se han descubierto en su diseño, y que es hoy un crypto sistema utilizado en un gran número de Internet protocolos.

II. DESARROLLO DEL ARTÍCULO

Los algoritmos de cifrado simétrico DES y 3DES, así como tienen sus semejanzas es importante poder definir y establecer sus diferencias, en la actualidad el algoritmo de cifrado simétrico DES se encuentra obsoleto y no es utilizado en sistemas más seguros o certificados por entidades aseguradoras, sin embargo 3DES es un algoritmo que aún se usa en la actualidad con diferentes mecanismo de usabilidad en el área de seguridad de tarjetas de crédito y cajeros automáticos.

Para poder observar las características principales de cada uno de estos algoritmos se presenta la siguiente tabla:

Factor	DES	3DES
Creador	IBM en 1974	IBM en 1978
Tamaño de clave en bits	56	168
Seguridad	No seguro	Medianamente seguro
Tipo de clave	Única	1 (dividida en 3 partes)
Rendimiento de descifrado	3/5	4/5
Resistencia al criptoanálisis	Vulnerable	Vulnerable
Tipo de cifrado	Simétrico	Simétrico
Tiempo para descifrar	Clave de 112 bits en 800 días.	Clave de 56 bits en 400 días.

A) Antecedentes

Hasta hace poco, el principal estándar para cifrar datos era un algoritmo simétrico conocido como Estándar de cifrado de datos (DES). Sin embargo, esto ahora ha sido reemplazado por un nuevo estándar conocido como Advanced Encryption Standard (AES).

DES es un cifrado de bloque de 64 bits, lo que significa que cifra los datos de 64 bits a la vez. Esto contrasta con un cifrado de flujo en el que solo se cifra un bit a la vez (o, a veces, pequeños grupos de bits, como un byte).

DES fue el resultado de un proyecto de investigación establecido por la corporación International Business Machines (IBM) a fines de la década de 1960 que resultó en un cifrado conocido como LUCIFER. A principios de la década de 1970 se decidió comercializar LUCIFER y se introdujeron una serie de cambios importantes. IBM no fue el único involucrado en estos cambios, ya que, buscaron asesoramiento técnico de la Agencia de Seguridad Nacional (NSA) (otros consultores externos estuvieron involucrados, pero es probable que la NSA fuera el principal contribuyente desde un punto de vista técnico). La versión alterada de LUCIFER se presentó como una propuesta para el nuevo estándar de cifrado nacional solicitado por la Oficina Nacional de Estándares (NBS). Finalmente fue adoptado en 1977 como el Estándar de cifrado de datos - DES (FIPS PUB 46).

A medida que evolucionaron la velocidad y la potencia de la informática, DES se volvió cada vez más susceptible a los ataques de fuerza bruta. En 1995, un grupo de trabajo de redes experimentales publicó RFC 1851 para recomendar 3DES como reemplazo de DES.

3DES refuerza la seguridad de DES utilizando no una, ni dos, sino tres claves DES de 56 bits. El algoritmo de cifrado 3DES se describe a continuación, donde K1, K2 y K3 son las tres claves de 56 bits:

B) Análisis de criptografía simétrica con DES y 3DES

Cada una de las técnicas de cifrado tiene sus propios puntos fuertes y débiles. Para aplicar una criptografía adecuada algoritmo a una aplicación, debemos tener conocimientos sobre el rendimiento, la fuerza y la debilidad de los algoritmos. Por lo tanto, estos algoritmos deben analizarse en función de varias características. En este documento se realiza un análisis con las siguientes métricas bajo las cuales se pueden comparar los criptosistemas se describen a continuación:

- Tiempo de encriptación: El tiempo necesario para convertir texto sin formato en texto cifrado es el tiempo de cifrado. El tiempo de cifrado depende del tamaño de la clave, tamaño y modo del bloque de texto plano. El tiempo de cifrado debe ser menor para que el sistema sea rápido y receptivo.

- Tiempo de descifrado: El tiempo para recuperar texto sin formato de texto cifrado se denomina tiempo de descifrado. Se desea que el tiempo de descifrado sea menor similar al tiempo de cifrado para hacer que el sistema responda y sea rápido.

- El tiempo de descifrado afecta el rendimiento del sistema.

- Memoria usada: Las diferentes técnicas de cifrado requieren un tamaño de memoria diferente para su implementación. Este requisito de memoria depende del número de operaciones que realizará el algoritmo, el tamaño de la clave utilizada, los vectores de inicialización utilizados y el tipo de operaciones. La memoria utilizada afecta el costo del sistema. Es deseable que la memoria requerida sea lo más pequeña posible.

- Efecto avalancha: En criptografía, una propiedad llamada difusión refleja la fuerza criptográfica de un algoritmo. Si hay un pequeño cambio en una entrada la salida cambia significativamente. Esto también se llama efecto de avalancha. Nosotros hemos medido Efecto de avalancha usando distancia de martilleo. La distancia de Hamming en la teoría de la información es una medida de disimilitud.

- Entropía: La aleatoriedad es una propiedad importante en los procesos criptográficos porque la información no debería poder ser adivinada por un

atacante. La entropía es una medida de aleatoriedad en la información.

El papel que juega la criptografía en la seguridad informática gracias al uso de algoritmos que permiten que un bloque de datos sea cifrado y descifrado; es decir, que se convierta de un texto normal a ilegible y de texto cifrado a legible, respectivamente. Se menciona el modelo convencional de encriptación donde se conceptualiza al texto plano, texto cifrado; además, aparecen cuáles son los objetivos de la criptografía que van direccionados hacia los cifrados simétricos que utilizan una sola clave y los asimétricos que manejan dos claves, la pública y la privada.

C) Importancia de la criptoagilidad en los sistemas con DES y 3DES

Las organizaciones deben ser conscientes de los peligros creados por la inercia o la aceptación de los riesgos comerciales de los conjuntos de cifrado profundamente incrustados que son inseguros. Con la amenaza de la computación cuántica en el horizonte, que amenaza con romper muchos de los algoritmos más populares de la actualidad, la recomendación del NIST es que las organizaciones "planifiquen la agilidad criptográfica para facilitar las transiciones a algoritmos resistentes a los cuánticos donde sea necesario en el futuro".

A medida que las empresas consideran el cumplimiento y las amenazas, la criptoagilidad puede permitir una respuesta rápida a las investigaciones y recomendaciones emergentes al respaldar la transición de un estándar de cifrado a otro en cualquier momento. Las soluciones para la criptografía como servicio permiten a las organizaciones de industrias altamente reguladas proteger los datos críticos para el negocio con soluciones de cifrado compatibles a nivel mundial.

D) ¿3DES ya no se permitirá usar después del 2023?

Teniendo en cuenta de DES desde hace muchos años se encuentra obsoleto, pero 3DES continúa en usabilidad, se define que en poco tiempo este pasará a ser obsoleto.

En 1997, NIST anunció una búsqueda formal de algoritmos candidatos para reemplazar DES. En 2001, AES se lanzó con la intención de convivir con 3DES hasta 2030, lo que permitirá una transición gradual. Sin embargo, es probable que la retirada de 3DES se haya acelerado debido a una investigación que ha revelado vulnerabilidades importantes y, según algunas fuentes, hace mucho que se debió.

NIST inició por primera vez la discusión sobre la desaprobación de 3DES después del análisis y demostración de ataques a 3DES. La vulnerabilidad Sweet32 fue hecha pública por los investigadores Karthikeyan Bhargavan y Gaëtan Leurent. Esta investigación explotó una vulnerabilidad conocida a los ataques de colisión en 3DES y otras suites de cifrado de bloques de 64 bits que son mayores durante transmisiones largas, el intercambio de archivos de

contenido o transmisiones vulnerables a la inyección de texto. Después de la exposición de esta vulnerabilidad, NIST propuso que 3DES fuera obsoleto y, poco después, restringió su uso.

E) Seguridad de DES y 3DES

La seguridad de 3DES depende de la opción de codificación que se utilice. La opción de codificación uno implica tres claves diferentes de 56 bits, lo que le da una longitud total de clave de 168 bits. La longitud efectiva se reduce considerablemente con los ataques de encuentro en el medio, que reducen su seguridad en el mundo real 112 bits.

Los ataques Meet-in-the-middle son útiles contra esquemas de cifrado que repiten el mismo algoritmo varias veces. La técnica almacena los valores inmediatos de cada etapa de encriptación y luego, usa esta información para mejorar radicalmente el tiempo que tomaría forzar el algoritmo.

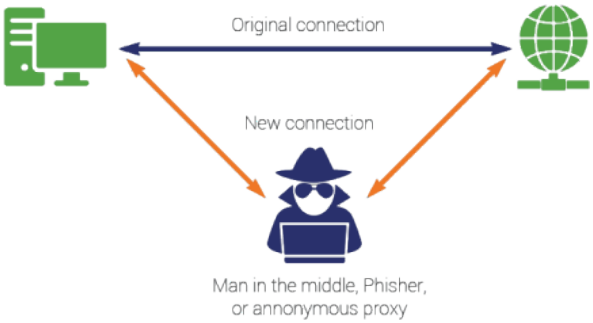

Fig. 3. Man in the middle

Las opciones dos y tres tienen claves significativamente más pequeñas y son vulnerables tanto a los ataques de texto sin formato conocido como a los de texto sin formato elegido, así como a otros.

Los ataques de texto sin formato conocido son posibles cuando un adversario tiene acceso tanto al texto sin formato como al texto cifrado de un mensaje. Si un algoritmo es susceptible a estos ataques, el atacante puede usar esta información para deducir la clave, lo que le permite descifrar todos los demás datos que han sido encriptados por la misma clave.

Un ataque de texto plano elegido es similar, pero implica que el atacante descubre la clave comparando textos cifrados con textos planos arbitrarios. Debido a estas vulnerabilidades y los pequeños tamaños de clave involucrados, las opciones de clave dos y tres son inseguras y no deben implementarse.

¿Es seguro usar 3DES?

Dado que 3DES quedará obsoleto en los próximos años, es mejor utilizar otros algoritmos. Si bien la opción de codificación uno todavía se considera segura para muchas aplicaciones, no hay buenas razones por las que deba usarse en lugar de una alternativa como AES.

Aunque, 3DES ocupa un lugar importante en la criptografía como seguimiento de DES, sus años de gloria han terminado y es hora de seguir adelante. Si desea proteger sus sistemas en el futuro, debería utilizar un algoritmo más actualizado.

F) Aplicaciones

1) Novedoso método de bloqueo de imágenes para cifrar y descifrar colores

El cifrado de la imagen en color digital se basa en el proceso de conversión de la imagen en color digital original en una encriptada para proteger la imagen de la piratería o para evitar que una persona autorizada obtenga la información valiosa ubicada en la imagen en color, el proceso para cifrar o descifrar de las imágenes en color es un tema muy importante en las actividades humanas por lo cual, en la actualidad se habla sobre un nuevo método simple, eficiente y altamente seguro que se utilizará para cifrado y descifrado, el método que se propone en él, articula, demuestra su validación e implementación, los parámetros de eficiencia se calcularán y se compararán con otros parámetros de métodos para probar los problemas de eficiencia del método propuesta.

2) Una codificación de red y dinámica basada en DES. Esquema de cifrado para la defensa de objetivos móviles

Se ha mencionado sobre los esfuerzos realizados sobre la investigación en la ciberseguridad, una teoría de defensa dinámica, llamada defensa de objetivos móviles aumenta la complejidad y los costos de los ataques al restringir de manera afectiva la exposición a la vulnerabilidad y las oportunidades de ataque a través de diversos mecanismos de evaluación, desarrollo y estrategia en constante cambio. El estándar de cifrado de datos DES era el esquema clásico de los esquemas tradicionales de cifrado de clave simétrica. Ahora ha sido reemplazado gradualmente por el triple DES o estándar de cifrado avanzado AES para que el codificador tenga un espacio de clave más grande. Sin embargo, tanto el 3DES como el AES no pueden cumplir con los requisitos de seguridad dinámica de la defensa dinámica debido a su extensión estática al espacio de las claves, el artículo detalla un esquema de cifrado dinámico de tres capas basado en DES y codificación de red, con un mecanismo de actualización de clave parcial de baja complejidad.

3) Una técnica de encriptación híbrida basada en autómatas celulares programable eficiente, para aplicaciones cliente-servidor de chat múltiple.

La base de este artículo reside en los atributos de varias reglas de CA y sus propiedades criptográficas, de ahí se derivan los principios, los cuales se basan en los datos estatales de sus vecinos y los suyos propios; asimismo, crea datos de estado siguiente confusos y aleatorios que son enormemente difíciles de anticipar y su inversión es prácticamente exorbitante en todos los aspectos, también está implementado en java.

Últimamente la información muestra una técnica de encriptación híbrida (PCHET) programable basada en Autómatas Celulares (CA) para aplicaciones de chat donde se incluyen a múltiples clientes que pueden conversar simultáneamente entre ellos.

El diseño propuesto es una técnica de cifrado de clave simétrica, todavía muy ligera y fácil de implementar, conjuntamente se realiza una investigación donde se compara de manera exhaustiva sobre los tipos de cifrados similares existentes, como el estándar de cifrado de datos (DES), 3DES y el estándar de cifrado avanzado (AES). El tiempo de implementación del trabajo propuesto es mucho mejor que el esquema existente, debido a que es prácticamente necesario para el cifrado de extremo a extremo en caso de aplicaciones de chat que involucren a varios clientes.

4) Combinación del algoritmo 3DES para la seguridad de los mensajes multimedia

En la era digital, la comunicación a través de redes informáticas juega un papel fundamental.

A través de la comunicación electrónica, una persona puede realizar transacciones o comunicaciones de manera muy rápida y práctica. El envío de datos / mensajes de un lugar a otro está muy limitado por el tema de la confidencialidad. Hay muchas formas de ocultar los datos / mensajes que se enviarán. Primero, usando técnicas criptográficas, es decir, codificando datos / mensajes usando ciertos algoritmos. Otra técnica consiste en insertar un mensaje que será enviado a otros medios, de manera que el mensaje quede oculto y lo que aparecerá son otros medios utilizados para insertar mensajes.

III. Conclusiones

- Utilizamos el cifrado para convertir nuestros datos de texto sin formato en texto cifrado, que es información a la que los atacantes no pueden acceder (siempre que utilicemos los algoritmos adecuados).

- La criptografía protege la información y las comunicaciones mediante un conjunto de reglas que permiten que solo aquellos previstos, y nadie más, reciban la información para acceder a ella y procesarla.

- Los algoritmos criptográficos se utilizan para tareas importantes como el cifrado de datos, la autenticación y las firmas digitales, pero hay que resolver un problema para habilitar estos algoritmos: vincular claves criptográficas a las identidades de la máquina o del usuario. Los sistemas de infraestructura de clave pública (PKI) están diseñados para unir identidades útiles (direcciones de correo electrónico, sistema de nombres de dominio). direcciones, etc.) y las claves criptográficas utilizadas para autenticar o cifrar los datos que pasan entre estas identidades.

- El algoritmo DES se encuentra obsoleto y prontamente lo hará el 3DES debido a los ataques de vulnerabilidad relacionados a lo largo de este documento.

- El cifrado simétrico utiliza una sola clave para cifrar y descifrar la información.

Pone toda la seguridad en la clave y ninguna en el algoritmo. El ejemplo más claro de este tipo de cifrado es el sistema alemán Enigma, los algoritmos de cifrado más recientes son el 3DES, Blowfish e IDEA, los cuales utilizan claves de 128bits. El implementar una única llave es precisamente el punto débil del sistema, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad.

REFERENCIAS

[1] Srinivasa, O. (2015). Performance Analysis of DES and Triple DES. International Journal of Computer Applications, 130(14), 30-34. https://doi.org/10.5120/ijca2015907190

[2] H.O.A., B.B.Z., A.A.Z., H.A.J., M.S., & Y.A.-N. (2016). New Comparative Study Between DES, 3DES and AES within Nine Factors. JOURNAL OF COMPUTING, 2(3), 1-6. Recuperado de https://arxiv.org/ftp/arxiv/papers/1003/1003.4085.pdf

[3] R. Pramono Adhie, Y. Hutama, A. Ahmar and M. Setiawan, "ShieldSquare Captcha", Iopscience.iop.org, 2020. [Online]. Available: https://iopscience.iop.org/article/10.1088/1 742-6596/954/1/012009/pdf. [Accedido: 08- Nov- 2020].

[4] Pizzuti, D., Spolon, R., Lobato, R. S., & Manecero, A. (2017, 1 enero). Vista do Desempenho dos Algoritmos 3DES e AES Usando Cuda. Recuperado 1 de febrero de 2021, de https://sol.sbc.org.br/index.php/eradsp/artic le/view/4351/4277

[5] PAl-Azzeh, J. (2019, 10 enero). A Novel Based On Image Blocking Method To Encrypt-Decrypt Color | Al-Azzeh | JOIV : International Journal on Informatics Visualization. Recuperado 17 de enero de 2021, de http://joiv.org/index.php/joiv/article/view/2 10

[6] H. Tang, Q. T. Sun, X. Yang and K. Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense," in IEEE Access, vol. 6, pp. 26059-26068, 2018, doi: 10.1109/ACCESS.2018.2832854.

[7] Ferreira A.C., Silva N.B.F. Comparison of secure communication with 3DES between embedded system and general purpose computer Proceedings - IEEE Symposium on Computers and Communications, Volumes 2016-July, 2016. https://www.sciencedirect.com/science/arti cle/abs/pii/1084804515002283

[8] Nash Andrew, Infraestructura de Claves públicas, Ed. McGraw Hill, México 2004. De Jemas. NET Framework Ed. McGraw Hill, México 2004. https://www.redalyc.org/pdf/5055/5055548 06007.pdf

[9] O. Salcedo, L. F. Pedraza y C. A. Hernández, "Modelo de Semaforización Inteligente para la Ciudad de Bogotá", Revista Ingeniería Universidad Distrital, vol. 11, no. 2, pp. 61-69, 2006. https://revistas.udistrital.

edu.co/index.php/T ecnura/article/ view/7236

[10] O. Salcedo, L. F. Pedraza y C. A. Hernández, "Modelo de Semaforización Inteligente para la Ciudad de Bogotá". Revista Ingeniería Universidad Distrital, vol. 11, no 2, pp. 61-69, 2006. https://revistas.udistrital. edu.co/index.php/T ecnura/article/ view/7236

[11] SANTOS, Daniel F.; AMAYA BARRERA, Isabel and SUÁREZ PARRA, César Augusto. Algoritmo de Encriptación para Imágenes a Color Basado en Sistemas Caóticos. ing. [online]. 2020, vol. 25, n. 2, pp.144-161. ISSN 0121-750X. http://dx.doi. org/10.14483/23448393.15530.

[12] CORTÉS-MARTÍNEZ, Luis Miguel; ALVARADO-NIETO, Luz Deicy and AMAYA-BARRERA, Isabel. Composite cellular automata based encryption method applied to surveillance videos. Dyna rev.fac.nac.minas [online]. 2020, vol.87, n.213, pp.212-221 ISSN 0012-7353. http://dx.doi. org/10.15446/dyna.v87n213.81 859.

[13] Universidad de la Costa, Navarro Núñez, W., & Bareño Gutiérrez, R. (2013, junio). Revisión de la Seguridad en la Implementación de Servicios sobre IPv6. INGE CUC. https://repositorio.cuc. edu.co/bitstream/handle/11323/2550/ Revisi%C3%B3n%20de%20la%20seguridad%20en%20la%20implementaci%C3%B3n%20de%20servicios%20sobre%20IPv6.pdf?sequence=1&isAllowed=y

[14] Restrepo, C., Universidad Católica de Oriente, & Castrillón Osorio, L. (2019, julio). Diseño y desarrollo de un sistema de cifrado de datos basado en curvas elípticas (No 43). Revista Universidad Católica de Oriente. http://200.9.158.34/index.php/uco/ article/vie w/156/190

[15] Revista Espacios. (2019, septiembre). Red óptica pasiva para proveer de Internet a la ciudad de Riobamba - Ecuador. Autor.

[16] Bart, M., and Bart, P. (2016). Triple and Quadruple Encryption: Bridging the Gaps. [Archivo PDF]. Asociación Internacional para la Investigación Criptológica. https://eprint.iacr.org/20 14/016.pdf

[17] Sohal, M. Sharma, S. (2018). BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. Revista de la Universidad King Saud - Ciencias de la Información y la Computación. https://www- sciencedirect- com. bdigital.udistrital.edu.co/science/ article/ pii/S1319157818303999

[18] Zong, R., Dong, X. (2016). Meet-in-the- Middle Attack on QARMA Block Cipher. ShandongUniversity. https:// eprint.iacr.org/2016/1160.pdf