Universidad Autónoma de Querétaro

Facultad de Informática

Maestría en Ciencias de la Computación

Estudio comparativo entre dos métodos numéricos matriciales aplicados a la criptografía simétrica desde una perspectiva computacional

Tesis

Que como parte de los requisitos para obtener el Grado de

Maestro en Ciencias de la Computación

Presenta

Alba Nidia Martínez Martínez

Dirigido por:

Doctor Fausto Abraham Jacques García

Co-Dirigido por:

Doctor Luis Adrián Lizama Pérez

Fausto Abraham Jacques García
Presidente
Luis Adrián Lizama Pérez
Secretario
Sandra Luz Canchola Magdaleno
Vocal
Alberto Lamadrid Álvarez
Suplente
Alberto Lara Guevara
Suplente

Centro Universitario, Querétaro, Qro.
Fecha de aprobación por el Consejo Universitario Noviembre 2022
México

Dedicatorias

Para Lupita, Johnny, Christian, Pepe, Dany y Pasita. Gracias por acompañarme en esta etapa. Dios los bendice.

Agradecimientos

Agradezco al Consejo Nacional de Ciencia y Tecnología (CONACYT) por los recursos financieros brindados. A mi asesor por la paciencia y asistencia en este proyecto.

Si el Señor no construye la casa, de nada sirve que trabajen los constructores; si el Señor no protege la ciudad, de nada sirve que vigilen los centinelas. De nada sirve trabajar de sol a sol y comer un pan ganado con dolor, cuando Dios lo da a sus amigos mientras duermen. Salmos 127, 1-2

Índice

Índice de Figuras

Índice de Tablas

Resumen

Este trabajo describe el análisis realizado en términos de tiempo de ejecución, procesamiento y uso de memoria de acceso aleatorio, para caracterizar la eficiencia de dos métodos numéricos matriciales, que son Gauss-Jacques con modularización euclidiana implícita y Gauss-Jordan con modularización explícita. Ambos métodos calculan la inversa modular de cualquier matriz dada en Z_n. La matriz inicial se conoce como la clave en el contexto de la criptografía simétrica. Las pruebas realizadas consideraron múltiples tamaños de matriz para lograr identificar el comportamiento de cada método, y los recursos que utiliza cada uno en términos de procesamiento y memoria para determinar cuál es el método más eficiente en el contexto computacional con aplicación a la criptografía simétrica.

Palabras Clave

Métodos numéricos, Matriz Inversa Modular, Estudio Comparativo, Método Gauss-Jacques, Método Gauss-Jordan.

Abstract

This document describes the analysis carried out in terms of execution time, processing and use of random access memory, to characterize the efficiency of two matrix numerical methods, which are Gauss-Jacques with implicit Euclidean modularization and Gauss-Jordan with explicit modularization. Both methods compute the modular inverse of any given matrix in Z_n. The initial matrix is known as the Key in the context of symmetric cryptography. The tests carried out considered multiple matrix-size in order to allow us identify the behavior of each method, and the resources that each one uses in terms of processing and memory to determine which is the most efficient method in the computational context with application to symmetric cryptography.

Keywords

Numerical Methods, Modular Inverse Matrices, Comparative Study, Gauss-Jacques method, Gauss-Jordan method.

Capítulo 1

Introducción

En los últimos años del siglo pasado y lo que va de este siglo, la tecnología ha evolucionado de tal manera que se considera un agente de cambio en la sociedad, desempeñando un rol fundamental en diferentes contextos: social, económico, productivo, educativo, en el consumo de bienes y servicios, en la ejecución de tareas cotidianas, entre otros. La llamada inteligencia artificial (AI) por sus siglas en inglés, la digitalización, las neurociencias y algunas novedades más, son la base de lo que algunos han identificado como sociedades físico-digitales (Martínez et al., 2020).

La tecnología se ha convertido en un tema de interés que va más allá del marco científico y tecnológico. Desde la perspectiva de las ciencias sociales, el acceso y la capacidad para hacer uso de la tecnología son figuras cruciales en las sociedades contemporáneas, teniendo dos aspectos importantes para los individuos, siendo el primero de ellos el acceso a la información y la comunicación, y el segundo ejercer la ciudadanía y participar en el mercado de trabajo (UNESCO, 2018).

La tecnología es un elemento central que configura la sociedad, detentando el poder y determinando las necesidades y productos en la dinámica actual que presentan las sociedades digitales (García, 2021).

Desde esta posición, la tecnología seguirá siendo un ingrediente esencial en constante evolución, dirigiendo así el desarrollo de las sociedades industriales avanzadas. El siglo XXI cuenta con un espacio donde la formación y el desarrollo de una nueva cultura mediática ha tomado lugar (Barlybayeva, 2022).

Ciertas posturas escépticas sugieren que la cultura digital actual, sustentanda por las grandes corporaciones, altera la vida social redefiniendo la experiencia humana al utilizar algoritmos sofisticados. La revolución de la información no está limitada a una solución tecnológica avanzada, también involucra la manera en que como individuos y sociedades se conceptualiza la idea básica de "ser"(Levin and Mamlok, 2021), modificando la comprensión de la propia identidad.

Algunos autores opinan que trasladarse a una forma digital de organizar la sociedad es ineludible, dando peso a los beneficios que brinda la red global de información, la economía organizada, la inteligencia articial, el gobierno electrónico, entre otros. Sin embargo, otros autores distinguen las consecuencias negativas de este proceso que promueve la divulgación de la vida privada de los individuos. La revolución digital produce la dependencia de las personas a la tecnología generando un control estricto sobre la privacidad de los sujetos, manteniendo registro de sus preferencias, hábitos, comportamientos y conductas frecuentes (Burkhanov et al., 2022).

La sociedad industrializada depende cada vez más de las tecnologías e infraestructuras digitales y la tendencia es aumentar el uso de estas herramientas con la promesa de una economía virtual infinitamente creciente y eficiente. La digitalidad es la expresión cultural y social que está vinculada al término digital (Dufva and Dufva, 2019). Las personas que utilizan medios digitales como principal herramienta de estudio, trabajo y ocio o diversión, a menudo tienen dificultad para diferenciar el ambiente virtual del mundo real.

Junto con la multiplicación de la disponibilidad del Internet, nuevas formas de desigualdades han surgido. La brecha digital se relaciona con el nivel económico y educativo, la ubicación geográfica, la edad y otros factores. La alfabetización digital se refiere a las habilidades necesarias para hacer un uso adecuado de la tecnología. La inclusión digital se refiere a las políticas para disminuir la brecha digital y promover la alfabetización digital (Bernhard et al., 2019).

Para algunos, la tecnología es la responsable de disminuir e incluso combatir las desigualdades. Para otros, el acceso a la información y a los dispositivos son algunos de

los factores que profundizan y multiplican las diferencias. Por ejemplo, estudiantes de todos los niveles educativos han interrumpido sus estudios debido a que no disponen de los medios para asistir a la clases virtuales en un contexto de pandemia mundial (Lemus, 2021).

En un ambiente altamente digitalizado, el proceso de comunicación tradicional ha sido modificado. La comunicación está estrechamente vinculada con el trabajo, siendo en sí un proceso productivo que permite a los humanos asimilar el mundo, comprenderse entre sí, alcanzar sus necesidades y estructurar las relaciones. El ser humano cumple su propósito último en el trabajo (Fuchs, 2020).

La misión de escuelas y universidades es preparar a individuos competitivos y competentes, aptos para una sociedad y cultura en constante cambio. A esto se suma el desafío de un mercado laboral moderno que demanda sujetos con cultura digital para vivir y trabajar. Para ello, es necesario reflexionar profundamente sobre la naturaleza de este fenómeno desde varias ciencias: filosofía, sociología, sicología y pedagogía (Zhardemova et al., 2021) .

Procurar capital humano con una cultura adecuada a las nuevas tareas en una sociedad digital, hace necesario intensificar los procesos de adaptación de una persona a la nueva realidad. Lo anterior requiere de inversión de tiempo, infraestructura, apoyo social y sicológico para algunos sectores de la población. El desarrollo de tecnologías digitales trae consigo ventajas y al mismo tiempo riesgos si no se brinda apoyo y educación a grupos vulnerables (Ivanova et al., 2020) .

Asimismo, las empresas requieren tomar algunas medidas para mantenerse competitivas. Entre los cambios que pueden implementar están: la reorganización de su modelo de negocio, la construcción de una arquitectura de negocio digital y la creación de una estructura organizacional digital. Es indispensable que formen alianzas con compañias donde la digitalización existe en diferentes niveles (Voronkova et al., 2021).

De esta manera, el entorno cotidiano de millones de personas alrededor del mundo está rodeado de productos y servicios que favorecen que el aprendizaje, el trabajo, las tareas coditianas y las actividades de esparcimiento se lleven a cabo de una forma

muy distinta a lo que se realizaba hace algunos años. La información, el conocimiento y el ocio están a una búsqueda rápida en Internet, siendo la inmediatez una de las características de las sociedades digitales (García Aretio et al., 2019).

La tecnología y su abrumador avance en los últimos 20 años ha marcado un antes y un después en la manera de vivir, trabajar, recrearse y relacionarse con otras personas. Hace algunos años, comunicarse con una persona podría requerir semanas al utilizar los medios tradicionales de comunicación, como el correo; actualmente establecer contacto es cuestión de segundos, por ejemplo con una llamada. De esta forma, es viable escuchar y ver a una persona que se encuentra a cientos o miles de kilómetros de distancia.

La rapidez para propagar noticias y acontecimientos relevantes, así como la ejecución de transacciones y contratos entre instituciones que se ubican en distintos puntos geográficos alrededor del mundo es una particularidad del mundo actual. Lo anterior produce un volúmen de información nunca antes vista y al mismo tiempo, una porción significativa son datos falsos o de fuentes no verificadas, que al ser considerados verdaderos, podrían modificar conductas sensibles en los individuos.

Por ejemplo, cuando una persona utiliza un dispositivo inteligente, en este caso un asistente virtual controlado por voz, conocido como altavoz inteligente, está interactuando con una gran cantidad de servidores, algoritmos, programas, bases de datos, la infraestructura de telefonía e incluso empleados en lugares al otro lado del mundo. Entonces, ¿qué huellas deja un individuo en un dispositivo inteligente y cómo se usará en un futuro? (Lindley et al., 2019).

El comportamiento de los individuos termina plasmado en mecanismos que se van ajustando o adquieren cierta inteligencia, generando información que es aprovechada por diversas organizaciones para ofrecer productos y servicios conforme a cada sujeto, disminuyendo el tiempo de toma de decisión para consumirlos. Por otro lado, información sensible y confidencial de millones de personas que cuentan con una vida digital activa podría caer en manos de grupos criminales organizados. El mundo real va generando datos que se expresan en la realidad virtual y viceversa. Ninguno de los dos contextos está exento de problemas o beneficios que afectan a la sociedad.

La evolución tecnológica y digital se ha expresado de diversas formas a través del tiempo. Hace muchos años, la rueda, la bombilla eléctrica, el automóvil hicieron posible que la forma de transportarse y de vivir se modificara. Años después, la computadora y diversos dispositivos facilitaron aún más la vida cotidiana, los procesos de producción y generación de riqueza.

Asímismo, se redefinió la manera en que las personas interactuaban, se comunicaban y trabajaban. Los dispositivos funcionaban de manera aislada o independiente; un auto tenía funciones concretas, limitadas al igual que un teléfono. Sin embargo, con la llegada de las redes digitales, la conectividad entre dispositivos ha aumentado gradualmente y compartir información entre ellos es cada vez más sencillo y rápido.

Anteriormente, se utilizaban medios físicos con capacidad limitada para transferir información de una computadora a otra, por ejemplo, un disco flexible o un disco compacto. Con la introducción del teléfono inteligente o smartphone en inglés, el volúmen de personas conectadas en tiempo real se incrementó considerablemente, y la convergencia con la evolución de los microprocesadores, las comunicaciones y la inteligencia artificial son la base de el Internet de las cosas (IoT) por sus siglas en inglés (Greengard, 2021).

Estos productos y servicios, conocidos como IoT consisten en la integracion de miles de millones de dispositivos inteligentes que pueden comunicarse entre sí con una mínima intervención humana (Al-Garadi et al., 2020).

Según (Diène et al., 2020) se trata de un modelo de red donde los dispositivos físicos, digitales y virtuales tienen funciones de identificación, detección, conexión en red y procesamiento para establecer comunicación entre sí y con otros dispositivos y servicios en Internet, con el propósito de ejecutar tareas solicitadas por los usuarios de una manera cómoda y fácil.

En la práctica, el concepto de IoT se puede observar en el mundo real en los teléfonos que pueden almacenar datos, voz, audio, ubicación geográfica o realizar consumo de bienes y servicios; relojes que almacenan patrones de sueño o el ritmo cardiaco.

Estos son algunos ejemplos de este cambio tecnológico sin precedentes que se ha desarrollado en los últimos años. Las empresas que los fabrican, crean productos con

diferentes capacidades y características, incrementando la complejidad en el contexto de la conectividad.

Otro factor para el creciente uso de dispositivos de IoT es la puesta en marcha de redes 5G y WiFi 6, y con ello, el aumento de ataques cibernéticos que pueden comprometer los bienes de una organización (Valdivia and Miranda, 2020).

Con el surgimiento de una realidad virtual mezclada con el mundo físico, ha surgido la necesidad de crear métodos que estructuren las relaciones que surgen a raíz de la compleja conectividad entre dispositivos y humanos.

Hace muchos años fue necesario fijar leyes y disposiciones que han permitido establecer orden y regular las relaciones entre los individuos, grupos y países. Actualmente existen procedimientos y herramientas físicas que permiten proteger aquello que se considera valioso, por ejemplo bienes materiales o información.

Dentro de este nuevo esquema de distribución de información y tareas comunes, surge el término de seguridad informática que consiste en proteger los activos que se consideran de valor, como es el caso de las computadoras, los teléfonos inteligentes o bien los programas y plataformas, datos, entre otros.

Este nuevo espacio se conoce como ciberespacio, y se refiere al mundo virtual compuesto por los dispositivos y los sistemas computacionales conectados y que intervienen en las tareas cotidianas de la población (Christen et al., 2020).

Algunas de las tecnologías usadas contra la sociedad como los robots y noticias falsas, entre otras, tienen el propósito de difundir información errónea que confunde y genera beneficios para algunos grupos de la población.

En respuesta ha surgido una nueva disciplina científica llamada ciberseguridad social que utiliza métodos como el análisis de red, ciencia de datos, aprendizaje automático y procesamiento de lenguaje natural para obtener evidencia sobre quien manipula información en Internet en contra de alguna organización, qué métodos utiliza y cómo se puede combatir.

A diferencia de la seguridad informática o ciberseguridad, la ciberseguridad social estudia y comprende la comunicación social y la creación de comunidades, estadísticas,

las redes sociales y el aprendizaje automático (Carley, 2020).

El nivel actual de conexión de dispositivos generada por IoT, permite que estén expuestos a un ataque o ciberataque en el contexto de tecnología y seguridad de información.

En una era altamente digital, en la cual es común que los intrusos en forma de virus, piratas informáticos, o fraudes electrónicos intenten vulnerar dispositivos y sistemas, la seguridad tiene prioridad (Stallings et al., 2020). El volumen de datos generados requieren un tratamiento específico para evitar retrasos y garantizar la seguridad (Rani et al., 2022).

Junto con el aumento de informacion disponible para un ciberataque, también ha ido incrementado el poder de cómputo utilizado para atacar o para proteger los datos compartidos (Vargas et al., 2019).

Un ataque consiste en la probabilidad de que un tercero vulnere el dispositivo o dispositivos y el resultado impacte de manera negativa en la organización, de acuerdo al Instituto Nacional de Estándares y Tecnología de Estados Unidos (US NIST) por sus siglas en inglés (Kandasamy et al., 2020).

De acuerdo a (Khraisat and Alazab, 2021) la información sin seguridad, producirá pérdidas considerables no sólo para las industrias, sino también para los individuos. La ausencia de un método de cifrado adecuado en los dispositivos es un factor primordial en cuanto a la seguridad de la información.

El número de ataques se ha incrementado causando diversas problemáticas, entre ellas la reputación, el cumplimiento y la operación de organizaciones que se han visto afectadas. A pesar de ello, tanto organizaciones como individuos carecen de una estrategia de seguridad, y en caso de contar con ella, sólo algunos la ponen en práctica.

Un ejemplo, es el robo de 78 millones de expedientes que sufrió Anthem Blue Cross Insurance System en los Estados Unidos de América en 2015. Aunque los ataques son cada vez más frecuentes, no existe una referencia completa del alcance que tiene un ciberataque en cuanto a la interrupcion del servicio, el impacto financiero y perjuicio a los pacientes (Ghafur et al., 2019).

El objetivo de la ciberseguridad es disminuir los riesgos a través del aseguramiento de los dispositivos y la privacidad. Es necesario considerar el aspecto tecnológico así como la gestión de riesgos para cubrir de manera integral el objetivo.

Desde la perspectiva de una arquitectura de capas en los dispositivos, cada una de ellas tiene cuestiones únicas que deben ser atendidas. En la capa de percepción, uno de los problemas es la clonación de chips de dispositivos para ataques cibernéticos.

En la capa de red, es crítico brindar un canal seguro para la transmisión de datos. En la capa de procesamiento, la computación en la nube y la computación en niebla, o cloud computing y fog computing en el idioma inglés, que son tecnologías comunes para procesar y almacenar volúmenes importantes de datos mediante dispositivos de IoT, el reto es realizar la detección oportuna de intrusos.

La seguridad de los protocolos usados, autenticación errónea y procedimientos de auditoría insuficientes son algunos de los problemas de la capa de aplicación, debido a que en este nivel se comparte información y se estable colaboración mediante dispositivos como teléfonos inteligentes, transporte inteligente, monitores de signos vitales inteligentes, entre otros.

Además la capa de administración de los servicios incluye el factor humano y la organización de la seguridad. Cuando la seguridad y la privacidad se ven amenazadas, se ve afectada la confianza de las organizaciones y de los usarios en el proceso de adopción de sistemas tecnológicos (Lee, 2020).

Debido a que la información recopilada por los diversos dispositivos de IoT incluye datos sensibles de organizaciones y usuarios, mantenerlos seguros y privados durante su transmisión en la red se ha constituido en un componente significativo, por lo cual en los últimos años aprender y poner en práctica habilidades de ciberseguridad es imprescindible.

El contexto de ciberseguridad abarca, como se mencionó, varias capas o niveles en los cuales es posible establecer mecanismos para disminuir los riesgos. Para realizarlo, se requiere considerar las diferentes competencias que intervienen en una visión integral de la ciberseguridad. De acuerdo a (Sánchez et al., 2020), algunas de estas compentencias

son:

- Capacidad para administrar redes, servicios, procesos y aplicaciones conocidas como sistemas de captura, transporte, procesamiento, almacenamiento entre otros, desde la perspectiva telemática.
- Capacidad para aplicar las técnicas base de las redes, servicios y aplicaciones telemáticas, como lo son los sitemas de gestión, señalización y conmutación, seguridad (protocolos criptográficos, mecanismos de recopilaicón, autenticación y protección de contenidos), calidad del servicio en entornos fijos y móviles, locales y de larga distancia, entre otros.
- Habilidad para diseñar arquitecturas de redes y servicios telemáticos.
- Capacidad para programar aplicaciones y servicios telemáticos en red y distribuidos.
- Crear sistemas informáticos centralizados o distribuidos que integren hardware, software y redes.
- Capacidad para trabajar en contextos que proporcionan información específica imprecisa.

El desafío es mantener los datos protegidos de cualquier ataque por medio de la seguridad de la información o seguridad cibernética. Es necesario concientizar e involucrar a la comunidad de usuarios de todos los niveles, establecer alianzas, encriptar y respaldar datos, brindar seguridad a las redes y contar con sistemas de recuperación de datos para combatir los ataques (Alhayani et al., 2021).

Como se mencionó, dentro de la ciberseguridad se encuentran los algoritmos criptográficos, que parecen proporcionar el único método práctico para proteger los datos.

Si bien no garantiza la seguridad absoluta, el cifrado de datos almacenados y durante la transmisión a menudo hace que sea más costoso y riesgoso penetrar en los sistemas (Konheim, 1981).

La criptografía es un instrumento fundamental para proveer el nivel de seguridad adecuado para los datos (Murad and Rahouma, 2022) y consiste en la escritura en código y la interpretación del mismo, llamado también cifrado y descifrado.

Se trata de un mecanismo que modifica el mensaje original en un mensaje distinto antes de ser transmitido. Los datos permanecen seguros mientras sean indescifrables para un tercero no autorizado. Para lograrlo, existen llaves a las cuales solo personas autorizadas tienen acceso, y son utilizadas para cifrar el mensaje antes de enviarlo, y descifrarlo para que el receptor tenga acceso al mensaje original.

El cifrado es una proceso de transformación; el texto original o texto plano es reemplazado por el llamado texto cifrado. El texto es formado por la concatenación de símbolos o letras de un alfabeto. Es una competencia entre dos adversarios: el diseñador del sistema que especifica la familia de transformaciones, y el oponente que intenta recuperar el texto sin formato y/o la clave y así anular el efecto del cifrado. El proceso mediante el cual un oponente intenta recuperar el texto sin formato y/o su clave del texto cifrado se denomina criptoanálisis (Konheim, 1981).

Los métodos criptográficos se han adaptado a la evolución de la tecnología, pues una vez que logran romperse, se muestra el camino para mejorarlos e invalidar los métodos de ruptura existentes. Utilizan más de una técnica como la sustitución, transposición y el número de llaves.

En la técnica de sustitución, cada letra del mensaje se sustituye por otra letra; en la transposición, cada letra del mensaje cambia de posición; en cuanto al número de llaves, se refiere a la criptografía simétrica o de una llave, y a la criptografía asimétrica o de dos llaves, una pública y una privada (Patil and Bansode, 2020). Los criptosistemas de sustitución se pueden categorizar como monoalfabéticos y polialfabéticos.

La criptografía clásica o manual se refiere a los métodos que se usaron desde la antigüedad hasta la Primera Guerra Mundial; utilizan la sustitución y transposición. El periodo entreguerras fue testigo de máquinas de cifrado complejas. Con la llegada de las primeras computadoras, la complejidad de los algoritmos y la capacidad de procesamiento de los dispositivos dejaron al ser humano con el rol de diseñadores (Prieto,

2020).

Un metodo de cifrado clásico muy conocido es el creado por Julio Cesar, político y militar romano del siglo I a. C. y consiste en sustituir cada letra del mensaje por la letra ubicada tres lugares delante en el alfabeto utilizado. Es decir, la letra A es sustituida por la letra D, la letra B por la letra E, y así sucesivamente. Las ultimas tres letras X, Y, Z se sustituyen por las letras A, B, C (Ryabko and Fionov, 2021).

El primer cifrado polialfabético documentado adecuadamente fue el cifrado de Alberti. En el año 1508 Johannes Trithemius en su libro Poligraphia crea la tabula recta, que consiste en una tabla cuadrada de alfabetos donde cada fila se completa desplazando la fila anterior hacia la izquierda, siendo este el cifrado Thithemius. Giovan Battista Bellaso describió el cifrado conocido como Vigenere en 1553, utilizando la tabula recta agregando una llave o contraseña repetida para cambiar el alfabeto de cada cifrado en cada letra, es decir, el patrón cambia cada vez que cambia la contraseña, a diferencia de Alberti y Trithemius que utilizaron un patrón de sustituciones fijo. Sin embargo, en 1556 Blaise de Vigenere propuso un cifrado similar al de Bellaso, con la diferencia de una clave más segura, razón por la que se le atribuyó este nombre (Esteve Romero, 2019). El cifrado de Vigenere fue utilizado durante la Guerra Civil de Estados Unidos.

Charles Wheatstone inventó el método Playfair para la comunicación telegráfica secreta en el año 1854, usando en la Primera Guerra Mundial. Se trata de de una matriz alfabética 5 x 5 que incluye la letras del alfabeto inglés. Se puede adaptar a otros alfabetos. Es el primer cifrado en la historia en cifrar cada par de letras a la vez y el resultado de ambas depende de ellas (Carrión, 2021).

El cifrado ADFGVX fue desarrollado por los alemanes para la Primera Guerra Mundial (Serrano Pinilla, 2018). ADFGVX es una cifra relativamente grande para ser manipulada manualmente y es la última importante antes de la aparición de las máquinas criptográficas. Su seguridad radica en la naturaleza confusa de la cifra junto con los métodos de sustitución y transposición aunque finalmente, este método fue decifrado por Georges Painvin criptográfo francés del Deuxieme Bureau.

Otro método simétrico de sustitución polialfabético muy conocido es el cifrado de

Hill. Su base es el álgebra lineal y fue inventado por Lester S. Hill en 1929. Se considera el primer cifrado práctico para operar con más de tres símbolos. Utiliza una matriz de dimensión n x n como llave para cifrar y descifrar (Nofriansyah et al., 2018). Es un método muy eficiente, veloz y simple, sin embargo, el emisor y receptor comparten la misma llave en canales no seguros. Por lo anterior, a través de los años numerosos investigadores han trabajado en mejorar su seguridad (Dawahdeh et al., 2018).

Durante el siglo XX la criptografía utiliza máquinas de cálculo para generar cifras más seguras. Una de estas máquinas fue inventada por los alemanes y es conocida como Enigma. Contiene rotores para automatizar los cálculos de cifrado y descifrado y fue utilizada en la Segunda Guerra Mundial. Oficialmente fue desarrollada por Arthur Scherbius en 1918; posteriormente se desarrollaron otras versiones llamadas Enigma A, B, C, etc. La versión final usada por el ejército germano fue Enigma I. Aunque inicialmente cualquier organización podía emplearlas, en 1932 el ejército cambió la regla y cualquier uso de la máquina Enigma debía ser aprobado por ellos. Varios países mostraron interés en este tipo de dispositivos aunque parecía ser un gran desafío manejarlas adecuadamente (Prasad and Kumari, 2020).

El siguiente paso en la evolución de la criptografía se da con las aportaciones de Claude Shannon en cuanto a la teoría de la información, posterior a la Segunda Guerra Mundial. Shannon estableció la secrecía perfecta, que consiste en que el mensaje original no podrá ser revelado usando el texto cifrado.

Varios años depués, alrededor de 1975 aparece en escena el primer diseño lógico del principal cifrador hasta finales del siglo, conocido como Data Encryption Standard (DES) en inglés. Casi al mismo tiempo surgió la criptografía asimétrica o de llave pública que actualmente se aplica en procesos como la firma digital.

En términos de privacidad, la criptografía simétrica produce menos contratiempos que los metodos avanzados basados en criptografía asimétrica (Avoine and Hernandez-Castro, 2021).

La empresa IBM desarrolló DES; el Instituto Nacional Estadounidense de Estándares (ANSI) por sus siglas en inglés, lo nombró como ANSI X3.92 y es uno de los

estándares simétricos más comunes actualmente. Utiliza una llave de 56 bits realizando el proceso de cifrado y descifrado en bloques de datos de 64 bits como entrada o texto plano y salida o texto cifrado respectivamente. El algoritmo principal se repite 16 veces hasta obtener el texto cifrado. Estos ciclos son exponencialmente proporcionales al tiempo necesario para que un ataque de fuerza bruta encuentre la llave (Hamouda, 2020).

Advanced Encryption Standard (AES) por sus siglas en inglés, es un cifrado de tipo simétrico que sustituye el cifrado DES. AES fue el producto que el Instituto Nacional de Estándares y Tecnología o NIST por sus siglas en inglés, organismo del gobierno de los Estados Unidos, obtuvo al iniciar en 1997 y hasta el 2000 una convocatoria mundial para presentación de algoritmos de cifrado. Lo anterior fue considerado necesario al detectar lo factible que era un ataque para el método DES. Aunque en las últimas dos décadas han sido desarrollados varios algoritmos eficientes, AES se destaca como el algoritmo más seguro dado que es fácil implementarlo con un costo bajo en hardware como en software. Tiene categorías de acuerdo al tamaño de la llave, por ejemplo AES-128, AES-192, AES-256 con llaves de 128, 192 y 256 bits respectivamente (Kumar et al., 2021).

En el entorno de la seguridad de la información, un ataque tiene diversas formas y nombres. La intercepción ocurre cuando una entidad no autorizada accede directamente a datos confidenciales que viajan entre fuentes y destinos autorizados; por ejemlo, un hacker puede acceder al tránsito de correos electrónicos y otras transferencias de datos. La interferencia es una acción donde una entidad no autorizada accede directamente a datos confidenciales, no necesariamente a los datos de la comunicación. Un ejemplo es el análisis del tránsito, donde el adversario puede obtener información observando el patrón en la red, así como el volúmen de información en particular entre un par de terminales. Una intrusión se da cuando una entidad no autorizada obtiene información confidencial eludiendo la seguridad de un sistema. En lo que respecta a la criptografía simétrica, existen dos perspectivas generales para realizar un ataque, el criptanalisis y el ataque de fuerza bruta. El primero considera la naturaleza del algoritmo y características

del texto plano y del texto cifrado para descubrir la llave usada, y de esta forma, podrán descrifrar todos los textos cifrados que consigan. El segundo tiene variaciones, pero en términos generales consiste en usar un fragmento o porción del texto cifrado y probar al menos la mitad de todas las llaves posibles hasta obtener el texto plano. Es necesario tener la habilidad para identificar cuando el texto plano es realmente texto plano. Para tener éxito, también se debe considerar el idioma o tipo de datos usados en el mensaje, y si ha sido comprimido o no (Stallings et al., 2020).

La mayoría de los algoritmos de cifrado son seguros en la práctica, debido al poder computacional de los equipos que actualmente se utilizan. Sin embargo, con la computación cuántica sería posible romperlos debido al número de operaciones que se pueden ejecutar.

En el presente documento, se abordará la criptografía simétrica desde una perspectiva computacional. El objetivo es realizar un estudio comparativo de dos métodos numéricos matriciales a la criptografía simétrica. Se utilizarán métodos estadísticos para realizar la evaluación de tres dimensiones: procesamiento, memoria de acceso aleatorio y complejidad. Se busca conocer cuál es el método más eficiente para dejar disponible estos resultados a la comunidad que trabaja en el contexto de ciberseguridad.

Capítulo 2

Marco teórico

2.1. Criptografía

Un día hace casi 4000 años, en un pueblo llamado Menet Khufu bordeando la delgada cinta del Nilo, un maestro escriba esbozó los jeroglíficos que contaban la historia de la vida de su señor, y al hacerlo, abrió la historia registrada de la criptología. El suyo no era un sistema de escritura secreta como la que conoce el mundo moderno; no usó ningún código completamente desarrollado de jeroglíficos y sustituciones de símbolos. La inscripción no era escritura secreta, sino que incorporó uno de los elementos esenciales de la criptografía: una deliberada transformación de la escritura. Es el texto más antiguo que se sabe que lo hace. La adición del secreto a las transformaciones dan origen a la criptografía. Cierto, era más un juego que otra cosa: buscaba retrasar la comprensión sólo el menor tiempo posible, y el criptoanálisis era, igualmente, sólo un rompecabezas. La de Egipto era por lo tanto, una cuasi criptología en contraste con la ciencia seria de hoy. Sin embargo, las grandes cosas tienen comienzos pequeños, y estos jeroglíficos incluyen, aunque de manera imperfecta, los dos elementos de secreto y transformación que comprenden los atributos esenciales de la ciencia. Y así nació la criptología (Kahn, 1967).

La criptografía es una parte de la criptología, y es el arte de escribir en código e interpretar código, el proceso de cifrar y descifrar respectivamente. Su propósito es mantener los mensajes transmitidos en secreto, conservando la privacidad de la comunicación.

Mantener información en secreto para sí mismo o entre dos o más personas autorizadas ha sido vital para resolver situaciones que, de no ser por una comunicación segura, habrían finalizado de una forma distinta. En el marco de conflictos armados o guerras, la posibilidad de que un enemigo intercepte y comprenda un mensaje ha generado diversas propuestas para garantizar la privacidad de la comunicación.

La competencia para desarrollar mecanismos de comunicación seguros y romperlos, entre criptógrafos y criptoanalistas respectivamente, es la causa de la evolución gradual tanto de los mecanismos como de los ataques. En 1923 el criptógrafo William Friedman dió origen al concepto criptoanálisis, que se refiere a los mecanismos usados para resolver un criptograma o mensaje cifrado, sin determinar el sistema que lo generó. De ahí se deriva el término criptoanalista.

La técnica básica en el ambiente criptográfico es la esteganografía y consiste en ocultar el mensaje. No es una técnica para cifrar información, pero es lo más cercano a la criptografía. Como se mencionó, han surgido diversos mecanismos a lo largo de la historia, teniendo como base el siguiente procedimiento (Prieto, 2020):

- El emisor cifra el texto original con algún algoritmo o método.
- El mensaje cifrado se envía al receptor. Si un tercero no autorizado intercepta el mensaje, no debería poder descifrarlo o conocer el texto original, pues no conoce el algoritmo o la llave utilizados.
- El receptor recibe y descrifra el mensaje, obteniendo el texto original.

Ha habido una relación simbiótica entre la criptografía y el desarrollo de sistemas informáticos de alto rendimiento. A medida que los sistemas criptográficos aumentaron en su sofisticación, la necesidad de desarrollar métodos más eficientes para criptoanalizarlos se convirtió en el estímulo para el desarrollo de las computadoras. Alemania utilizó tres sistemas criptográficos durante la Segunda Guerra Mundial (Konheim, 2007):

1. Las comunicaciones militares por radio fueron cifradas por el sistema de rotor Enigma.

2. El T52e fabricado por Siemens y Halske era un dispositivo binario en el que el texto plano se convirtió por primera vez en el código Baudot de 5 bits.

3. El SZ40/AZ42 también realizó el cifrado de texto plano convertido en datos binarios.

La criptografía es clasificada en criptografía clásica la cual data desde la antigüedad hasta la primera guerra mundial y criptografía moderna, que abarca alrededor de la segunda guerra mundial hasta nuestros días; desde la perspectiva de la tecnología, la criptografía moderna consiste en el estudio de técnicas matemáticas para la seguridad de la información, sistemas y cálculos distribuidos contra ataques de terceros, de acuerdo a (Katz and Lindell, 2020).

Existen diferentes técnicas: métodos de sustitución, de transposición o número de llaves usadas, ver Figura 2.1.

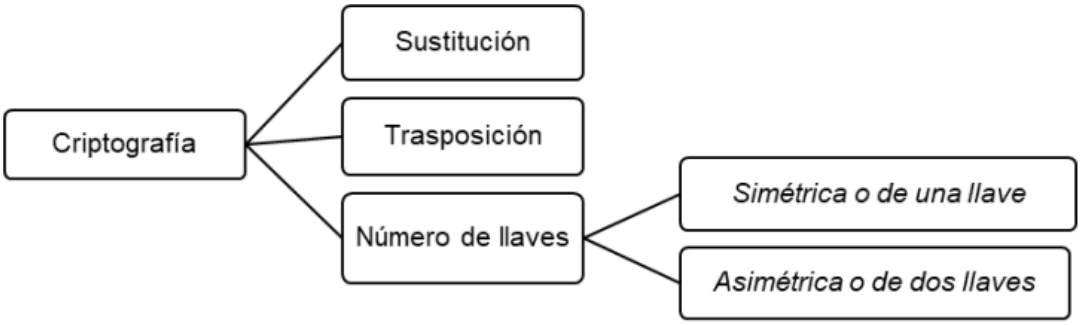

Figura 2.1. Clasificación de las técnicas de la criptografía (Fuente: Elaboración propia).

El método de sustitución consiste en que una letra o símbolo del alfabeto utilizado para escribir el mensaje original, se sutituye por otra letra del mismo alfabeto, en este caso se trata de sustitución monoalfabética; es polialfabética cuando una letra podría ser sustituída por más de una letra. En el método de trasposición, en lugar de sustituir, cada letra del mensaje original se cambia de posición; existen algunos métodos que combinan los dos anteriores. En cuanto al número de llaves, se refiere a la criptografía simétrica o de una llave y a la criptografía asimétrica o de dos llaves. Desde la antiguedad hasta 1976 la criptografía se basó únicamente en métodos simétricos. A partir de la introducción

del método asimétrico o de llave pública por Whitfield Diffie, Martin Hellman y Ralph Merkle, la criptografía ha ampliado su alcance.

El lingüista y criptógrafo holandés Auguste Kerckhoffs publicó ensayos sobre criptografía militar en 1883 dando como resultado algunos principios. Uno de ellos hace referencia a que la seguridad de un sistema criptográfico se basa en mantener la llave en secreto, independientemente de que el algoritmo de cifrado se conserve o no en secreto.

En 1945 Claude Elwood Shannon estableció el concepto de la perfecta secrecía, el cual es ampliamente aceptado en la actualidad como la notación más precisa de seguridad y por ello, sigue siendo utilizado en sistemas ciberfísicos, de control distribuido, redes inalámbricas, entre otros(Zhou and El Gamal, 2020).

En el entorno de la criptografía, la máxima aspiración es aproximarse a la secrecía perfecta y consiste en que el mensaje original no podrá ser conocido utilizando el texto cifrado. También es conocida como seguridad incondicional y se describe de la siguiente forma: un esquema de cifrado con los elementos generación, cifrado y descifrado (Gen, Enc, Dec), con espacio de mensaje M, espacio de texto cifrado C y espacio de clave K tiene secreto perfecto si, para cada distribución de probabilidad en M, cada mensaje $m \in M$, y cada texto cifrado $c \in C$ para cada $Pr(C = c) > 0$, $Pr(M = m/C = c) = Pr(M = m)$ (Jara-Vera and Sánchez-Ávila, 2020).

La perspectiva computacional de la secrecía perfecta es aproximarse de manera práctica y no de forma teórica; en otras palabras considera el tiempo y poder computacional requerido para que un atacante consiga de modo eficiente la información (Hwang et al., 2021). En la Figura 2.2 se representa un ejemplo de la secrecía perfecta.

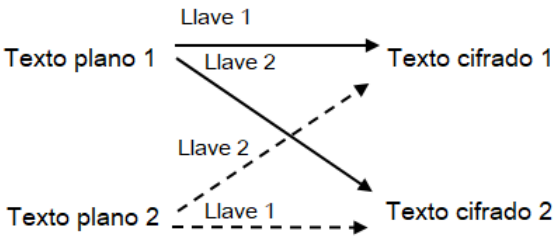

Figura 2.2. Probabilidad de distribución en la secrecía perfecta. (Fuente: Elaboración propia).

La criptografía simétrica o de una llave, objeto de estudio en este trabajo, utiliza una llave, la misma, para cifrar y descifrar. Esta llave debe mantenerse en secreto o de lo contrario, un tercero no autorizado podría conocer el mensaje. En la Figura 2.3 se muestra el proceso de criptografía simétrica.

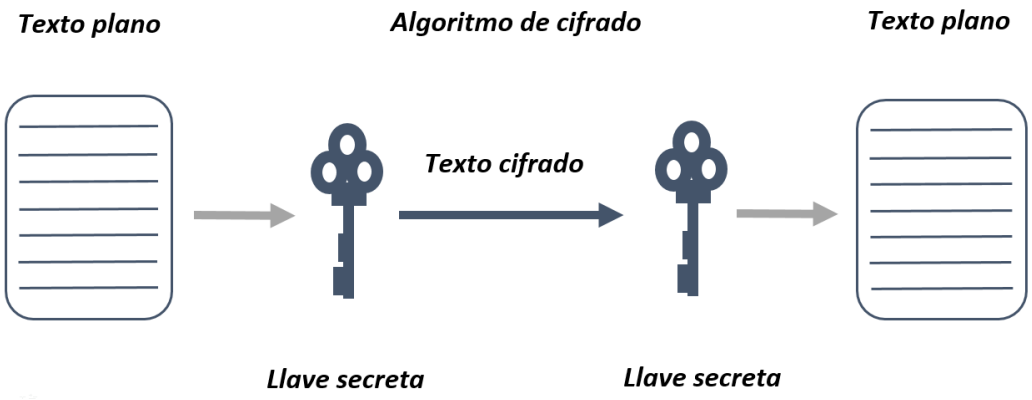

Figura 2.3. Proceso de criptografía simétrica. (Fuente: Elaboración propia).

Mantener en secreto la llave es lo que Shannon llamó secrecía perfecta y uno de los principios de Kerckhoffs, anteriormente mencionados.

El secreto perfecto se refiere a una llave de números aleatorios con distribución uniforme del mismo tamaño o mayor que el mensaje, garantizando que sin importar el poder computacional usado, no sea posible descubrir la llave en un tiempo razonable.

El propósito principal al diseñar cualquier algoritmo de cifrado debe ser la seguridad, el desempeño y el costo de implementarlo. La criptografía simétrica requiere un menor tiempo de procesamiento (Hammad et al., 2020), lo que generalmente significa un requerimiento menor de recursos. La principal ventaja del método simétrico sobre el asimétrico es la rapidez y eficiencia para volúmenes grandes de información aunque la desventaja es la administración de la llave, es decir, mantenerla en secreto. Por otro lado, en el cifrado asimétrico o de llave pública es posible tener una llave secreta compartida (Chi Domínguez, 2019).

La teoría de la información es un concepto aportado por Shannon y es la base científica de la criptografía, dividiéndose en teoría de códigos y criptología. La criptología se divide en criptografía y criptoanálisis. La criptografía dejó de ser un arte, dando paso

a algoritmos avanzados que brindan seguridad a la información transmitida. La complejidad algorítmica, la estadística y la teoría de números son usadas en el desarrollo de un algoritmo criptográfico. La estructura de un criptosistema matemáticamente es una función (Moreno and Díaz, 2020), y la expresión se muestra como una quíntupla (M, C, K, E, D) que representa:

- M o conjunto finito de posibles textos plano.
- C o conjunto finito de posibles mensajes crifrados.
- K o conjunto finito de posibles llaves.
- E o conjunto de transformaciones de cifrado.
- D o conjunto de transformaciones de descifrado

Para todo K en k existe una regla de cifrado e_K que pertenece a E y una regla de descifrado D; cada una definidas $e_K : M = C$ y $d_K : C = D$ tal que, ver ecuación 2.1:

$$d_K(e_K(x)) = x \tag{2.1}$$

Para todo x en M.

2.2. Aritmética modular

Dentro de la teoría de números se ubica la aritmética modular. En su mayoría, tanto algoritmos simétricos y asimétricos la utilizan considerando un número finito de elementos enteros (Paar and Pelzl, 2009). Un ejemplo de criptografía clásica que la utiliza es el cifrado de César, creado por el militar y político romano Julio César para la comunicación de asuntos cruciales de forma segura; este método conocido como cifrado por desplazamiento radica en sustituir cada letra del mensaje, por la letra que se ubica tres posiciones delante de la letra original, tomando como base el alfabeto utilizado (Ryabko and Fionov, 2021). Su denotación matemática, considerando la aritmética

modular, que radica en cambiar las letras por números, siguiendo la estructura A = 0, B = 1, C = 2,... Z = 26, se presenta en la ecuación 2.2 para cifrar y en la ecuación 2.3 para descifrar.

$$E_n = (x + n)\ mod\ 27 \tag{2.2}$$

$$D_n = (x - n)\ mod\ 27 \tag{2.3}$$

Donde x es la letra a sustituir, n es el desplazamiento y mod es el módulo, que en este caso consiste en el número de letras a usar del alfabeto en cuestión.

La aritmética modular está formada por clases de equivalencia de números enteros, conocidas como clases de congruencia. Se trata de una relación entre enteros que se representa también con un anillo o reloj de enteros usando la suma y la multiplicación, para un módulo n. Se describe de la siguiente forma:

a y b están en la misma clase de congruencia módulo n, si al dividir a entre n o b entre n el resto es igual o bien si el resultado de $a - b$ es un múltiplo de n. Se puede expresar como:

$$a \cong b\ (mod\ n) \tag{2.4}$$

Se lee a es congruente con b módulo n. Las propiedades de la congruencia son:

- Reflexiva, a es congruente con a, módulo n.

$$a \cong a\ (mod\ n) \tag{2.5}$$

- Simétrica, si a es congruente con b módulo n, entonces b es congruente con a módulo n.

$$a \cong b\ (mod\ n) \tag{2.6}$$

$$b \cong a \ (mod\ n) \tag{2.7}$$

- Transitiva, si a es congruente con b módulo n, y b es congruente con c módulo n, entonces a es congruente con c módulo n.

$$a \cong b \ (mod\ n) \tag{2.8}$$

$$b \cong c \ (mod\ n) \tag{2.9}$$

$$a \cong c \ (mod\ n) \tag{2.10}$$

En resumen, una relación de congruencia módulo n distribuye los números enteros en n conjuntos distintos o clases de equivalencia indicadas por [0], [1], [2],...[$n-1$] (García Merayo, 2015).

2.3. Máximo común divisor y algoritmo extendido euclidiano

La teoría de números incluye además de la aritmética modular, el algoritmo euclidiano. Este algoritmo calcula el máximo común divisor o mcd de dos enteros de una manera eficiente. Existen otros métodos para calcular el mcd, por ejemplo por descomposición en factores primos; sin embargo, pueden ser poco eficientes.

El mcd es el número entero más grande que divide a los dos enteros distintos de cero a y b, donde el residuo es cero y se escribe $mcd(a, b)$. Entonces, si un número c divide a a y b, también como $c|a$ y $c|b$, c es divisor común de ambos. El siguiente ejemplo ilustra lo anterior (Johnsonbaugh, 2005).

- Los divisores positivos de 30 son $1, 2, 3, 5, 6, 10, 15, 30$.
- Los divisores positivos de 105 son $1, 3, 5, 7, 15, 21, 35, 105$.

- Los divisores comunes son $1, 3, 5, 15$.
- El máximo común divisor de 30 y 105 es el 15, $mcd(30, 105) = 15$

a y b pueden tener más de un divisor en común, pero son números coprimos cuando los únicos divisores en común son 1 y -1.

Un entero mayor que 1 que sólo puede dividirse entre 1 y él mismo, es un número primo; en caso contrario, es un número compuesto. Por ejemplo, el número 7 sólo puede dividirse entre 1 y si mismo dejando un residuo igual a cero; entonces es un número primo. El número 14 se puede dividir entre 1,2,7 y 14 con residuo igual a cero, por lo tanto es un número compuesto.

Para cualesquiera $a, b \in Z$ existe un único $c \in Z$ que es el máximo común divisor o mcd de a, b (Grimaldi, 2003). Para demostrarlo, se tiene:

$$\text{Dados a,b} \in Z, \text{sea } S = as + bt \mid s, t \in Z, as + bt > 0 \tag{2.11}$$

Como $S \neq 0$, por el principio del buen orden, S tiene un elemento mínimo c. Entonces c es el máximo común divisor de a, b.

Como $c \in S$, $c = ax + by$, para algunos $x, y \in Z$, por lo tanto si $d \in Z$ y $d \mid a$ y $d \mid b$, entonces $d \mid (ax + by)$ por tanto $d \mid c$ de acuerdo al teorema en la ecuación 2.12

$$[(a \mid b) \wedge (a \mid c)] \rightarrow a \mid (bx + cy), \text{ para todos } x, y \in Z. \tag{2.12}$$

La expresión $bx + cy$ es una combinación lineal de b, c. Cuando mcd(a,b) = 1 o $x, y \in Z$ con $ax + by = 1$, a,b son primos relativos.

El algoritmo extendido euclidiano calcula el máximo común divisor de a, b denotándolo como una combinación lineal. En el ejemplo para $mcd(42, 70) = 14$, se tiene que:

$$x, y \in Z \text{ tales que } 42x + 70y = 14 \text{ o } 3x + 5y = 1 \tag{2.13}$$

Una solución es $x = 2$ y $y = -1$, de tal forma que $3(2) + 5(-1) = 1$. Sin embargo, para $k \in Z$, $1 = 3(2 - 5k) + 5(-1 + 3k)$, por lo tanto $14 = 42(2 - 5k) + 70(-1 + 3k)$ por lo que las soluciones para x y y son infinitas.

El algoritmo extendido euclidiano además de expresarse como una combinación lineal, despeja el residuo de cada ecuación y sustituye el resto de la última ecuación en la penúltima, es decir lo realiza en orden inverso de la última ecuación hasta la primera ecuación. Es posible utilizarlo junto con el concepto de módulo, de manera que si $r =$ a mod b, entonces:

$$mcd(a, b) = mcd(b, r) \tag{2.14}$$

Se puede ilustrar con los siguientes valores, donde $a = 105$, $b = 30$, es decir el valor del módulo es 30, por lo tanto el del residuo $r = 15$:

$$105 \bmod 30 = 15 \tag{2.15}$$

El valor de a ahora es el valor de b, mientras que el valor de b será el valor del residuo r, de esta forma

$$mcd(105, 30) = mcd(30, 15) \tag{2.16}$$

El residuo r de 30 módulo 15 es 0

$$30 \bmod 15 = 0 \tag{2.17}$$

Se repite la sustitución de los valores de a, b y r

$$mcd(30, 15) = mcd(15, 0) \tag{2.18}$$

El residuo r de 15 módulo 0 es 15

$$15 \bmod 0 = 15 \tag{2.19}$$

Se concluye entonces que

$$mcd(105, 30) = mcd(30, 15) = mcd(15, 0) = 15 \tag{2.20}$$

El algoritmo euclidiano funciona para encontrar el inverso modular de un entero en sistemas criptográficos. Un número multiplicado por su inverso es igual a 1. En aritmética modular no existe la operación división pero si los inversos modulares:

$$\text{El inverso modular de a mod b es } a^{-1}, \text{ entonces } (a * a^{-1}) \bmod \text{b } = 1 \tag{2.21}$$

En este ejemplo se muestra el cálculo del inverso modular de un número, donde $a = 273$ y $b = 110$,

$$r = 273 \bmod 110 = 53 \tag{2.22}$$

Ahora, $a = 110$ que en el paso anterior es el módulo b, y el residuo r es el valor del módulo $b = 53$

$$r = 110 \bmod 53 = 4 \tag{2.23}$$

Actualizando el valor de $a = 53$ y $b = 4$ se tiene que

$$r = 53 \bmod 4 = 1 \tag{2.24}$$

Entonces $a = 4$ y $b = 1$

$$r = 4 \bmod 1 = 0 \tag{2.25}$$

Al ser $r = 0$, el mcd de 273 y 110 es 1. Ahora se procede de forma inversa, iniciando donde $r \neq 0$, en la ecuación 2.24, ahora con la ecuación como sigue:

$$1 = 53 - 4 * 13 \text{ siendo 13 el cociente al dividir 53 entre 4} \tag{2.26}$$

La ecuación 2.23 se transforma en:

$$4 = 110 - 53 * 2 \text{ siendo 2 el cociente al dividir 110 entre 53} \tag{2.27}$$

En la fórmula 2.26 se sustituye el valor del 4 considerando lo que está en la fórmula 2.27

$$1 = 53 - 4 * 13 \tag{2.28}$$

$$1 = 53 - (110 - 53 * 2) * 13 = 27 * 53 - 13 * 110 \tag{2.29}$$

La ecuación 2.22 se transforma en:

$$53 = 273 - 110 * 2 \tag{2.30}$$

Y se utiliza para sustituir el valor de 53 en la fórmula 2.29

$$1 = 27 * 53 - 13 * 110 = 27 * (273 - 110 * 2) - 13 * 110 = 27 * 273 - 67 * 110 \tag{2.31}$$

Se obtiene $x = 27$ y $y = -67$ de la ecuación 2.31 de acuerdo a:

$$mcd(273, 110) = 1 = x * 273 + y * 110 \tag{2.32}$$

Donde $x = 27$ es el inverso modular calculado.

2.4. Matrices inversas modulares

Existen diversos trabajos realizados con el propósito de brindar modelos de criptografía simétricos seguros y resistentes a los ataques. Uno muy conocido es Hill Cipher, creado en 1929 por Lester. S. Hill.

Dicho modelo utiliza matrices, álgebra lineal y aritmética modular junto con la sustitución polialfabética. La matriz cuadrada o llave se procesa mediante una transformación lineal para obtener la matriz inversa modular y poder usarla en el paso de descifrado. Sin embargo, la llave puede ser conocida usando álgebra lineal, lo cual minimiza la confiabilidad del método (Ibañez, 2017).

Otro inconveniente es la selección de la llave, pues se realiza de forma aleatoria, lo cual consume tiempo pues no todas las matrices tienen su respectiva matriz inversa modular.

Las matrices cuadradas tienes diversas aplicaciones, entre ellas servir como la llave única en el marco de la criptografía simétrica. Algunas matrices cuadradas n x n carecen de su respectiva matriz inversa. Cuando esto sucede, la matriz se denomina singular; caso contrario, cuando una matriz es invertible, se conoce como no singular; la matriz inversa es única (Stanley and Flores Godoy, 2012). Por lo anterior, es significativo estudiar y brindar métodos que identifiquen aquellas matrices invertibles con el propósito de disminuir el tiempo que se dedica a este fin. Las características de una matriz invertible consisten en lo siguiente:

1. Determinante no nula.

2. El mcd del valor absoluto de la determinante, aplicando el módulo m, debe ser igual a 1.

2.5. Cifrados de Hill

Hill cipher es un método criptográfico de sustitución poligráfico creado por Lester S. Hill en 1929. Fue el primer método general en aplicar de manera práctica el álgebra lineal a los cifrados poligráficos. En esta técnica, cambiar solo una o dos letras del texto plano puede cambiar completamente el texto cifrado correspondiente. Es posible trabajar con n-cifrado de Hill, donde la clave es una matriz n x n con elementos desde 0 hasta $m-1$, donde m es el módulo o la longitud del alfabeto utilizado. Los cifrados de Hill utilizan matrices y vectores cuyas entradas pertenecen a Z_m para algún entero $m > 1$, y haciendo toda la aritmética módulo m. Z_m es un campo finito de elementos desde 0 hasta $m-1$. Cuando m es primo, se garantiza que cada valor distinto de cero en Z_m tiene un inverso multiplicativo. Es posible utilizar como clave de cifrado una matriz con entradas en Z_m para un $m > 1$ arbitrario, sin embargo a menos que las entradas de la matriz se elijan con cuidado, no es posible calcular una matriz inversa módulo m, en otras palabras, obtener una clave inversa para el desciframiento. Un n-cifrado de Hill con matriz clave A es la transformación lineal de Z_m^n a Z_m^n con una matriz estándar A y aunque el dominio y codominio son los mismos, se puede referir al dominio como el conjunto de todos los vectores de texto plano y el codominio sería el conjunto de todos los vectores de texto cifrado (Eisenberg, 1999).

Entres sus aplicaciones está la mejora de la seguridad (Sehgal and Gupta, 2019). También ha sido combinado con algunos algoritmos de cifrado asimétrico, con el propósito de disminuir la vulnerabilidad a los ataques de texto plano conocidos (Hasoun et al., 2021). Además ha sido utilizado en el cifrado de imágenes debido a su operación simple y rapidez en el cálculo (Sulaiman and Hanapi, 2021).

El proceso de cifrado y descifrado para el método Hill, se expresa en la ecuación 2.33 y la ecuación 2.34 respectivamente.

$$C = KP \, mod \, m \tag{2.33}$$

$$P = K^{-1}C \, mod \, m \tag{2.34}$$

Donde C es el texto cifrado, K es la llave o matriz cuadrada no singular, P es el texto plano, m es el módulo a utilizar y la llave o matriz inversa es K^{-1}.

Para calcular la matriz inversa K^{-1} es necesario que el determinante de la matriz K no sea nulo y el máximo común divisor del valor absoluto del determinante con respecto al módulo m debe ser igual a 1.

Dado que la llave se genera de forma aleatoria, conseguir que cumpla con las características mencionadas es un proceso que prefiere evitarse, debido a la poca efectividad para disminuir el tiempo de procesamiento y el espacio de memoria (Meizar et al., 2019).

Obtener una llave que sea invertible a través de un método que sea eficiente en el tiempo de procesamiento y uso de memoria es un proceso fundamental. El método Gauss-Jacques y el método Gauss-Jordan con modularización explícita son métodos numéricos matriciales que tienen como objetivo calcular matrices inversas modulares. La comparacion de ambos es el enfoque principal de este estudio, con el objetivo de identificar su rendimiento en tres dimensiones: tiempo de procesamiento, uso del procesador y uso de memoria.

2.6. Método Gauss-Jacques

El método Gauss-Jacques, utiliza la eliminación gaussiana en tres ejes lineales, y no requiere la determinante ni la matriz adjunta para calcular la inversa modular de una matriz (Jacques-García et al., 2022). Se hace uso del módulo euclidiano, números primos relativos, algoritmo extendido de Euclides, congruencias, entre otros conceptos. Los pasos para calcularla son:

1. Establecer el tamaño de la matriz llave n x n.

2. Generar de forma aleatoria la matriz llave.

3. Seleccionar un número primo para el módulo m.

4. Escribir junto a la matriz llave, la matriz identidad.

5. Encontrar x, donde $k_{ij}x = 1$ (mod m).

6. Aplicar a toda la fila, la formula $r_n x$ mod m = nuevo r_n, donde r_n es n-fila.

7. Realizar la eliminación gaussiana.

8. Repetir desde el paso 5 hasta el siguiente pivote.

9. La matriz ubicada a la derecha, es la matriz inversa modular.

Se propone la siguiente matriz K como ejemplo de cálculo de la matriz inversa modular; en la parte derecha está la matriz identidad. El módulo es el número primo 89, entonces $m = 89$.

$$\left|\begin{array}{ccc|ccc} 23 & 55 & 87 & 1 & 0 & 0 \\ 1 & 0 & 23 & 0 & 1 & 0 \\ 45 & 62 & 52 & 0 & 0 & 1 \end{array}\right|$$

Lo anterior permite realizar el paso 5, es decir encontrar x. El valor en $k_{11} = 23$ es el pivote, y será transformado en 1, de acuerdo a $23x \; mod \; 89 = 1$. Entonces, se utiliza la ecuación diofantina lineal $ax + by = 1$, donde $a = 23$ y $b = 89$:

89 = 23(3) + 20
23 = 20(1) + 3
20 = 3(6) + 2
3 = 2(1) + 1

Se calcula:

89 - 23(3) = 20

23 - 20(1) = 3

20 - 3(6) = 2

3 - 2(1) = 1

Utilizando el algoritmo extendido de Euclides:

23 - 20(1) = 3

23 - (89-23(3))(1) = 3

23 + 89(-1) + 23(3)(1) = 3

23(4) + 89(-1) = 3

89 - 23(3)- (23(4) + 89(-1))(6) = 2

89 + 23(-3) + 23(-24) + 89(6) = 2

89(7) + 23(-27) = 2

(23(4) + 89(-1))-(89(7) + 23(-27))(1) = 1

23(4) + 89(-1) + 89(-7) + 23(27) = 1

23(31) + 89(-8) = 1

El valor de $x = 31$, es el resultado junto al valor en $k_{11} = 23$. A continuación, se aplica el paso 6, donde el renglón 1 de la matriz K será modificado de acuerdo a $r_1(31)\ mod\ 89 = r_1$, de manera que el pivote $k_{11} = 23$ se convierta en 1. La matriz modificada en el renglón 1 queda de la siguiente forma:

$$\left|\begin{array}{ccc|ccc} 1 & 14 & 27 & 31 & 0 & 0 \\ 1 & 0 & 23 & 0 & 1 & 0 \\ 45 & 62 & 52 & 0 & 0 & 1 \end{array}\right|$$

El paso 7, la eliminación gaussiana, se realiza usando el pivote $k_{11} = 23$ que se transformó en 1. Se utiliza para transformar a 0 los elementos $k_{21} = 1$ y $k_{31} = 45$.

Se usa la fórmula $(r_1(-1) + r_2)\, mod\, 89 = r_2$ para el renglón 2. Se usa la fórmula $(r_1(-45) + r_3)\, mod\, 89 = r_3$ para el renglón 3. La matriz que resulta del proceso anterior es:

$$\left|\begin{array}{ccc|ccc} 1 & 14 & 27 & 31 & 0 & 0 \\ 0 & 75 & 85 & 58 & 1 & 0 \\ 0 & 55 & 83 & 29 & 0 & 1 \end{array}\right|$$

Ahora el nuevo pivote es $k_{22} = 75$, por lo que se aplica el paso 8, es decir, repetir el paso 5, que es encontrar x. Al encontrar x usando el nuevo pivote, es necesario repetir los pasos 6 y 7, hasta el siguiente pivote. El proceso para calcular la matriz inversa modular finaliza cuando se realiza el mismo proceso con cada pivote. La matriz final es:

$$\left|\begin{array}{ccc|ccc} 1 & 0 & 0 & 32 & 40 & 52 \\ 0 & 1 & 0 & 25 & 72 & 41 \\ 0 & 0 & 1 & 76 & 37 & 79 \end{array}\right|$$

Por lo tanto, la matriz inversa modular K^{-1} es la matriz ubicada a la derecha:

$$\left|\begin{array}{ccc} 32 & 40 & 52 \\ 25 & 72 & 41 \\ 76 & 37 & 79 \end{array}\right|$$

La Eq. 2.35 expresa como calcular la matriz inversa modular:

$$K_m^{-1} = \{\sum_{i=1}^{s}\sum_{j=1}^{s}[-k_{j(i+1)} + (k_{ij}e(k_{ii}, m) mod\ m)] mod\ m\} \tag{2.35}$$

Donde k_{ij} y k_{ji} son elementos de la matriz K, para el renglón i y la columna j. El algoritmo extendido euclidiano para calcular x, está representado por $e(k_{ii}, m)$, donde k_{ii} es el pivote y m es el valor del módulo utilizado.

La complejidad computacional expresada en notación O grande es $O(n^3 logm)$. La complejidad además se expresa en la ecuación 2.36, como un polinomio de tercer grado.

$$f(n,m) = (n^3 + (n^2 - n)n(log_{\emptyset})m!) \tag{2.36}$$

Donde n es el tamaño de la matriz y m es el módulo utilizado.

2.7. Gauss-Jordan con modularización explícita

El metodo de eliminación Gauss-Jordan llamado así en reconocimiento a Carl Friedrich Gauss y Wilhelm Jordan, tiene como objetivo calcular la inversa de una matriz nxn; también se usa para determinar la solución de un sistema de ecuaciones lineales (Larson and Falvo, 2010).

Para calcular la matriz inversa modular de una matriz llave se utiliza el siguiente procedimiento:

1. Establecer el tamaño de la matriz llave K n x n.
2. Generar de forma aleatoria la matriz llave K.
3. Seleccionar un número primo para el módulo m.
4. Calcular el determinante $|K|$ de la matriz llave. El determinante debe ser diferente de nulo, para que la matriz llave sea invertible.
5. Obtener la matriz inversa natural de la matriz llave K utilizando el método Gauss-Jordan: a)Adjuntar a la matriz llave K, la matriz identidad I para obtener la matriz aumentada. b) Realizar las operaciones necesarias sobre las filas de la matriz aumentada para obtener la forma escalonada reducida de la matriz llave. Es decir, hasta que la matriz identidad se calcule en la parte izquierda, la matriz inversa natural estara en la parte derecha de la matriz aumentada.
6. Encontrar el recíproco x para $x = e(|K|, m)$. Donde e, es la función Euclidiana extendida, $|K|$ es el valor absoluto de la determinante de la matriz llave, y m el valor de la aritmética modular o módulo.

7. Multiplicar el valor encontrado de x, por cada elemento de la matriz inversa natural calculada en el paso 5.

8. Aplicar el módulo m a cada elemento de la matriz anterior. El resultado es la matriz inversa modular K_m^{-1}.

Se propone la siguiente matriz A como ejemplo de cálculo de la matriz inversa modular; a la derecha se adjunta la matriz identidad. El módulo es el número primo 89, entonces $m = 89$.

$$\left|\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 1 & 3 & 2 & 0 & 1 & 0 \\ 2 & 4 & 9 & 0 & 0 & 1 \end{array}\right|$$

Se realiza la reducción por renglones. Se inicia con el valor $a_{11} = 1$ y se usará para transformar $a_{21} = 1$ y $a_{31} = 2$ en 0. Entonces $R2 \longrightarrow (-1)R1 + R2$,

$$\left|\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 1 & (-3) & (-1) & 1 & 0 \\ 2 & 4 & 9 & 0 & 0 & 1 \end{array}\right|$$

El siguiente paso es $R3 \longrightarrow (-2)\ R1 + R3$,

$$\left|\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 1 & (-3) & (-1) & 1 & 0 \\ 0 & 0 & (-1) & (-2) & 0 & 1 \end{array}\right|$$

Para obtener la diagonal principal con valores 1 en cada posición, $R3 \longrightarrow (-1)R3$.

$$\left|\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 1 & (-3) & (-1) & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 & (-1) \end{array}\right|$$

Se requiere tranformar a_{12}, a_{13} y a_{23} a valores 0. Entonces $R2 \longrightarrow (3)R3 + R2$

$$\left|\begin{array}{ccc|ccc} 1 & 2 & 5 & 1 & 0 & 0 \\ 0 & 1 & 0 & 5 & 1 & (-3) \\ 0 & 0 & 1 & 2 & 0 & (-1) \end{array}\right|$$

El siguiente paso es $R1 \longrightarrow (-5)R3 + R1$

$$\left|\begin{array}{ccc|ccc} 1 & 2 & 0 & -9 & 0 & 5 \\ 0 & 1 & 0 & 5 & 1 & -3 \\ 0 & 0 & 1 & 2 & 0 & -1 \end{array}\right|$$

Para transformar a_{12} se realiza $R1 \longrightarrow (-2)R2 + R1$

$$\left|\begin{array}{ccc|ccc} 1 & 0 & 0 & -19 & -2 & 11 \\ 0 & 1 & 0 & 5 & 1 & -3 \\ 0 & 0 & 1 & 2 & 0 & -1 \end{array}\right|$$

A la izquierda se observa la matriz identidad, y a la derecha la matriz inversa natural de la matriz A.

La determinante de la matriz A es $|A| = -1$, por lo tanto es una matriz invertible.

Se calcula el recíproco x del paso 6 utilizando la función Euclidiana extendida, entre el valor absoluto del determinante y el módulo m, donde $x = e(1, 89)$. El resultado es $x = 1$.

Se multiplica el valor de $x = 1$ por cada elemento de la matriz inversa natural, indicado en el paso 7.

$$\left|\begin{array}{ccc} -19 & -2 & 11 \\ 5 & 1 & -3 \\ 2 & 0 & -1 \end{array}\right|$$

Se aplica el módulo $m = 89$ a cada elemento de la matriz anterior, para obtener la matriz inversa modular A_m^{-1},

$$\begin{vmatrix} 70 & 87 & 11 \\ 5 & 1 & 86 \\ 2 & 0 & 88 \end{vmatrix}$$

La complejidad computacional expresada en notación O Grande es $O(n^2 + logm)$. Es una complejidad cuadrática, una dimensión menos que el método Gauss-Jacques.

Capítulo 3

Hipótesis

3.1. Preguntas de investigación

- ¿Cuál será el método numérico más eficiente, en términos de memoria o RAM, a usar junto con el Hill Cipher?
- ¿Cuál será el método numérico más eficiente, en términos de complejidadcomputacional, a usar junto con el Hill Cipher?
- ¿Cuál será el método numérico más eficiente, en términos de procesamiento, ausar junto con el Hill Cipher?
- ¿Cuál será el método numérico más eficiente, en términos de economía computacional, a usar junto con el Hill Cipher?

3.2. Hipótesis, Supuestos y/o proposiciones de investigación

Si son comparados dos métodos numéricos para criptografía simétrica, entonces se obtendrá el más eficiente en términos computacionales.

Capítulo 4

Objetivos

Objetivo general

Comparar dos métodos numéricos matriciales para criptografía simétrica, desde una perspectiva computacional en términos de memoria, complejidad y procesamiento, tal que se proporcione una heurística para la adaptabilidad de proyectos particulares de un método numérico sobre otro, es decir, orientar a la comunidad en la elección de un método sobre otro.

Objetivos específicos:

1. Caracterizar el método Gauss-Jacques.
2. Caracterizar el método Gauss-Jordan con modularización explícita.
3. Comparar ambos métodos en sus dimensiones de memoria, complejidad computacional y procesamiento.
4. Generar inferencias de eficiencia derivadas del análisis comparativo, para proporcionar una matriz de adyacencia y la heurística de usabilidad y/o adaptabilidad.

Capítulo 5

Material y metodología

El alcance propuesto para este estudio comparativo, es el experimental, siguiendo el método científico de Descartes y Bacon. El enfoque experimental implica realizar algunas acciones y analizar el resultado de las mismas. Es decir, se realizan ciertas actividades deliberadamente, con el fin de observar cuál es el efecto de las mismas, dentro de un ambiente controlado. Esto permite obtener las inferencias planteadas en un inicio, sea que éstas se confirmen o no (Hernández-Sampieri and Torres, 2018).

5.1. Ruta metodológica

Se utilizo una computadora portátil con un procesador Intel® Core™ i5-8300H CPU @ 2.30GHz, memoria de acceso aleatorio o RAM en inglés instalada de 8.00 GB (7.85 GB utilizable), sistema operativo Windows 10 Home Single Language version 20H2 de 64 bits, procesador x64.

5.1.1. Caracterización del método Gauss-Jacques

Para realizar la caracterización del método Gauss-Jacques se utilizó el algoritmo Gauss-Jacques® y el algoritmo para calcular el extendido euclidiano; ambos se obtuvieron de forma gratuita en la plataforma MathWorks®; su ejecución se realizó en el

software libre GNU Octave® version 5.2.0.

En la Figura 5.1 se muestra el procedimiento realizado para la caracterización del método Gauss-Jacques.

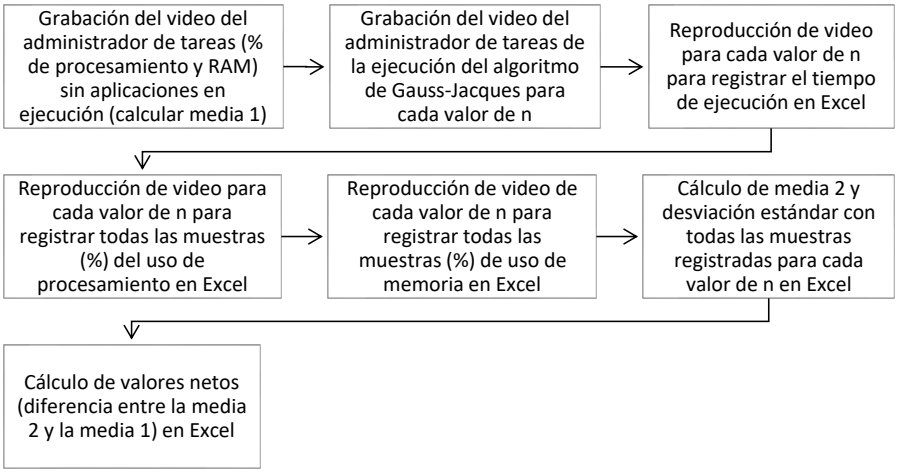

Figura 5.1. Procedimiento para obtención y registro de muestras y cálculo de medidas estadísticas del método Gauss-Jacques. (Fuente: Elaboración propia).

Para cada escenario o valor de la variable n la cual determina la dimensión de la matriz cuadrada n x n, se generó un video que contiene la ejecución del algoritmo Gauss-Jacques® que implícitamente ejecuta el algoritmo extendido euclidiano; el video muestra el inicio y fin del algoritmo al obtener la matriz inversa modular y el administrador de tareas de Windows® en el apartado rendimiento, el cual permite observar el uso en porcentaje de los recursos procesamiento y memoria, entre otros. Se utilizó el software libre OBS Studio 27.0.1 (64 bit) para la grabación de los vídeos.

Cada vídeo obtenido se reprodujo nuevamente para registrar el tiempo de ejecución del algoritmo, las muestras del uso en porcentaje de procesamiento (CPU) por sus siglas en inglés y finalmente las muestras del uso en porcentaje de memoria.

Para registrar el tiempo de ejecución se utilizó un cronómetro de un celular inteligente; las muestras de uso en porcentaje de procesamiento se obtuvieron al observar y registrar los diferentes valores de CPU que se mostraban en cada vídeo según el valor de la variable n; las muestras de uso en porcentaje de memoria se obtuvieron al ob-

servar y registrar los diferentes valores de CPU que se mostraban en cada vídeo según el valor de la variable n. El tiempo de ejecución, las muestras de uso en porcentaje de procesamiento y las muestras de uso en porcentaje de memoria se registraron en Excel de Microsoft Office Professional Plus 2013 para calcular la media y desviación estándar muestral.

5.1.1.1. Consideraciones para ejecutar el algoritmo Gauss-Jacques

Para ejecutar el algoritmo Gauss-Jacques y obtener como resultado la matriz inversa modular, se requieren los parámetros de entrada K y m, donde K es una matriz cuadrada n x n aleatoria y m es el módulo.

Se utilizó la función randi() para generar la matriz K que se convierte en la llave de entrada al algoritmo. La variable n determina la dimensión de la matriz cuadrada n x n, y sus valores en este estudio inician en 100 hasta 3000 con un intervalo de 100; es decir, 30 distintas dimensiones de la llave o escenarios de prueba.

El módulo utilizado fue el número primo 89, por lo tanto los elementos de la matriz son de dos dígitos, desde 1 hasta 89.

El resultado al finalizar la ejecución del algoritmo es la matriz inversa modular y la matriz identidad la cual permite comprobar que la matriz inversa calculada es correcta.

5.1.2. Caracterización del método Gauss-Jordan con modularización explícita

Para realizar la caracterización del método Gauss-Jordan con modularización explícita se utilizaron los algoritmos rref(), extendedeuclidean() y det() que calculan la matriz escalonada reducida con el método Gauss-Jordan, el inverso modular y la determinante de una matriz respectivamente; los procedimientos se observan en las Figuras 5.2, 5.3 y 5.4. Los algoritmos se obtuvieron de forma gratuita en la plataforma MathWorks® y se ejecutaron en el software libre GNU Octave® versión 5.2.0.

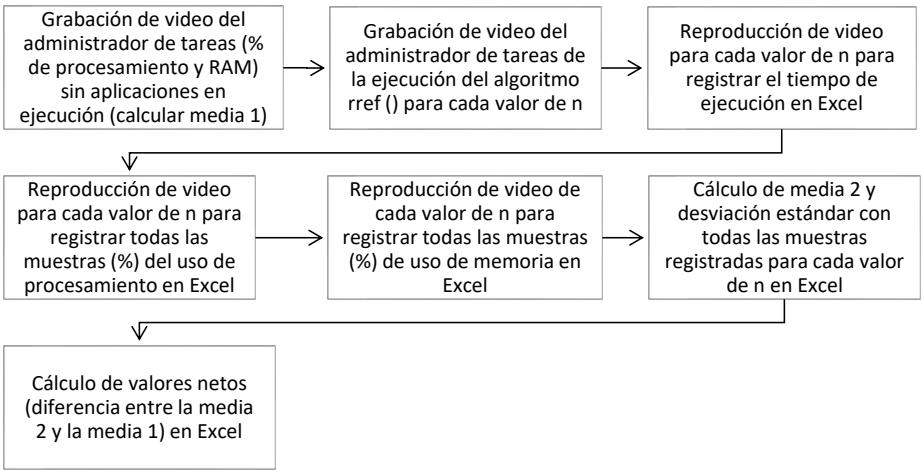

Figura 5.2. Procedimiento para obtención y registro de muestras y cálculo de medidas estadísticas del método Gauss-Jordan con modularización explícita - función rref. (Fuente: Elaboración propia).

5.1.2.1. Función rref

Para la función rref() se utilizó la variable n con distintos valores, donde n determina la dimensión de la matriz cuadrada n x n. En la Figura 5.2 se muestra el procedimiento utilizado.

Se generó un vídeo para cada valor de n, el cual contiene su ejecución y muestra el inicio y fin del algoritmo al obtener la matriz inversa; es decir en esta función no se obtiene la matriz inversa modular. En cada vídeo se puede observar el administrador de tareas de Windows® en el apartado rendimiento, mostrando el uso en porcentaje de los recursos procesamiento y memoria, entre otros. Se utilizó el software libre OBS Studio 27.0.1 (64 bit) para la grabación de los vídeos.

Los vídeos se utilizaron para registrar el tiempo de ejecución del algoritmo con ayuda de un cronómetro de un celular inteligente. En cuanto a las muestras del uso en porcentaje de CPU y las muestras del uso en porcentaje de memoria se obtuvieron al observar y registrar los diferentes valores de CPU y memoria que se mostraban a lo largo de la reproducción del vídeo para cada valor de n.

El tiempo de ejecución, las muestras de uso en porcentaje de procesamiento y las muestras de uso en porcentaje de memoria se registraron en Excel de Microsoft Office

Professional Plus 2013 para calcular la media y desviación estándar muestral.

5.1.2.2. Función extended euclidean

Para la función extendedeuclidean() se utilizó la variable n que es una cifra aleatoria del sistema numérico decimal, es decir unidad, decena, centena hasta la unidad de millar de millón, en total 10 cifras aleatorias. En la Figura 5.3 se muestra el procedimiento utilizado.

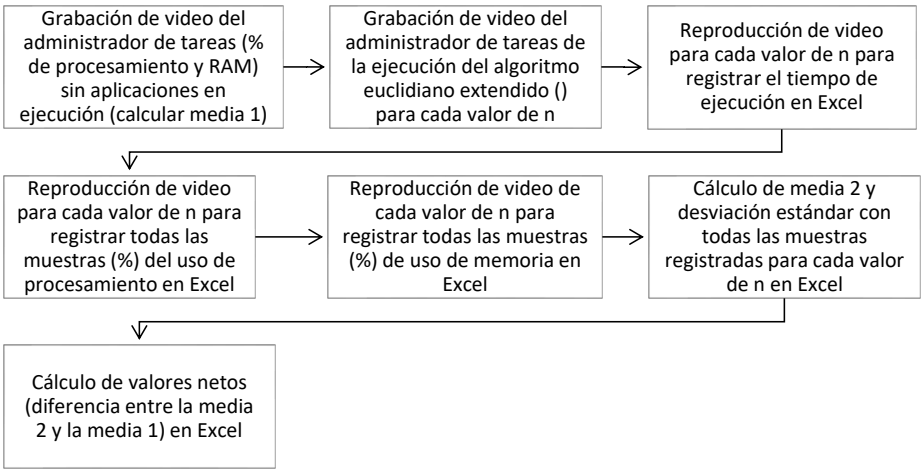

Figura 5.3. Procedimiento para obtención y registro de muestras y cálculo de medidas estadísticas del método Gauss-Jordan con modularización explícita - función euclidiano extendido. (Fuente: Elaboración propia).

Para cada valor de n se generó un vídeo con el software libre OBS Studio 27.0.1 (64 bit) el cual muestra el inicio y fin al obtener el inverso modular de un número dado n. El vídeo muestra el uso en porcentaje de los recursos procesamiento y memoria mediante el administrador de tareas de Windows® en el apartado rendimiento.

Con la reproducción de cada vídeo, se registró el tiempo de ejecución usando un cronómetro de un teléfono celular inteligente, las muestras de uso en porcentaje de procesamiento y las muestras en porcentaje de memoria se obtuvieron observando los distintos valores mostrados a lo largo de cada vídeo y se registraron en Excel de Microsoft Office Professional Plus 2013 para calcular la media y desviación estándar muestral.

5.1.2.3. Función det

Para la función det() se utilizó la variable n desde 1 hasta 134 para generar matrices cuadradas aleatorias de dimensión n x n con elementos de hasta dos dígitos, para calcular la determinante. En la Figura 5.4 se muestra el procedimiento utilizado.

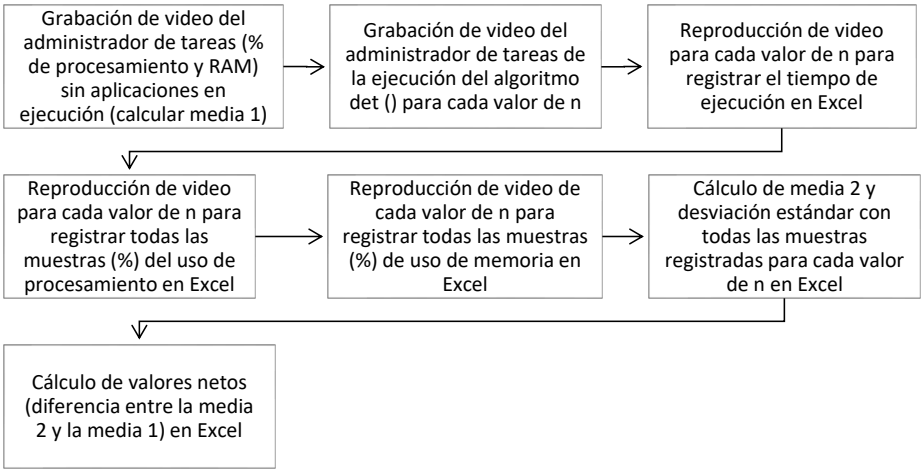

Figura 5.4. Procedimiento para obtención y registro de muestras y cálculo de medidas estadísticas del método Gauss-Jordan con modularización explícita - función determinante. (Fuente: Elaboración propia).

Para cada matriz se generó un vídeo con el software libre OBS Studio 27.0.1 (64 bit) el cual muestra el inicio y fin al obtener la determinante. El vídeo muestra el uso en porcentaje de los recursos procesamiento y memoria mediante el administrador de tareas de Windows® en el apartado rendimiento.

Con la reproducción de cada vídeo, se registró el tiempo de ejecución usando un cronómetro de un teléfono celular inteligente, las muestras de uso en porcentaje de procesamiento y las muestras en porcentaje de memoria se obtuvieron observando los distintos valores mostrados a lo largo de cada vídeo y se registraron en Excel de Microsoft Office Professional Plus 2013 para calcular la media y desviación estándar muestral.

5.1.2.4. Consideraciones del método Gauss-Jordan con modularización explícita

Para obtener la matriz inversa modular dada una matriz K con el método Gauss-Jordan con modularización explícita, se utilizaron las funciones rref(), extendedeuclidean() y det(), obteniendo la matriz escalonada reducida con el método Gauss-Jordan, el inverso modular de un número dado y la determinante de una matriz, respectivamente.

La función rref() requiere como entrada el parámetro K o matriz cuadrada aleatoria n x n y el parámetro n o dimensión de la matriz. El valor de n comenzó en 100 y finalizó en 3000 con intervalos de 100, con un total de 30 distintas dimensiones o llaves que fueron generadas con la función randi(). Se utilizó la matriz K aumentada con la matriz identidad para obtener la matriz inversa.

Para la función extendedeuclidean(), los parámetros de entrada son n y m, donde n es una cifra numérica tal que $nx \cong 1 \bmod m$; m representa el módulo y es el número primo 89. La variable x es el resultado, es decir el inverso modular de una cifra n. Se utilizó la función randi() para obtener la cifra aleatoria n con inicio en unidad, seguida por decena, centena hasta la unidad de millar de millón, obteniendo un total de 10 cifras aleatorias diferentes.

Para la función det(), es necesario contar con los parámetros de entrada n y K, donde n es la dimensión de la matriz cuadrada y K es la matriz cuadrada aleatoria n x n. Los elementos de la matriz son de hasta dos dígitos, de 1 hasta 99. Se utilizó la función randi() para generar las matrices. La variable n es un número consecutivo desde 1 hasta 134.

5.1.3. Medidas estadísticas calculadas

Las medidas estadísticas permiten representar una variable aleatoria. Se utilizaron los dos primeros momentos estadísticos, es decir la media y la varianza; se aplicó la raíz cuadrada de la varianza que es la desviación estándar.

La media o promedio es una medida de tendencia central que se calcula sumando todos los elementos o muestras y el resultado se divide entre el número total de elementos; por otro lado la varianza es una medida que identifica que tan dispersos están los datos en relación a la media, estableciendo las variaciones de cada valor de un grupo de datos (Triola, 2018).

La fórmula para calcular la media y la varianza se definen en las Ecuaciones 7 y 8.

$$\mu = 1/n \sum_{i=1}^{n} x_i. \tag{5.1}$$

$$\sigma^2 = 1/n \sum_{i=1}^{n} (x - \bar{x})^2 \tag{5.2}$$

Capítulo 6

Resultados y discusión

En la Tabla 6.1, se observa el resumen estadístico de uso de procesamiento y uso de memoria del método Gauss-Jacques para todos los valores de n. Los datos fueron registrados en porcentaje, según lo muestra el administrador de tareas de Windows® y el tiempo de ejecución se presenta en segundos.

Se observó que el tiempo de ejecución es mayor conforme el valor de la variable n aumenta, aunque no fue proporcional. Un ejemplo es cuando n =200 con tiempo de ejecución de 5 s mientras que n = 400 tiene 10 s de ejecución; si bien es el doble de tiempo entre ambos escenarios, el número de elementos de la matriz en el primer caso fue 40,000, mientras que en el segundo caso 160,000.

Otro ejemplo fue donde n= 1500 y n= 3000, con tiempos de ejecución de 247 s y 1937 s, respectivamente. El número de elementos del segundo escenario fue cuatro veces el del primer escenario, mientras que el tiempo de ejecución no fue proporcional en relación al valor de n y al número de elementos, indicando un comportamiento de tipo función logaritmo, que se aleja del eje de las ordenadas mientras aumenta en el eje de las abscisas mostrado en la Figura 6.1.

Para obtener los valores netos de la dimensión procesamiento y la dimensión memoria, primero se registraron los valores en % de CPU y RAM durante 30 minutos en el administrador de tareas de Windows® sin ejecutar aplicaciones, para calcular la media

Tabla 6.1. Resumen estadístico de procesamiento y RAM del método Gauss-Jacques. (Fuente: Elaboración propia).

n	Tiempo[s]	$\bar{x}$ CPU %	SD CPU %	$\bar{x}$ RAM %	SD RAM %
100	3	5	5	5	0
200	5	11	8	5	0
300	7	11	10	5	0
400	10	19	7	5	0
500	14	22	8	5	0
600	20	22	5	5	0
700	32	24	8	5	0
800	43	20	6	5	0
900	63	23	6	5	0
1000	80	25	7	5	0
1100	110	24	6	5	1
1200	136	30	15	8	1
1300	166	25	5	3	0
1400	207	26	11	3	1
1500	247	24	5	4	1
1600	294	27	8	3	1
1700	354	25	5	3	1
1800	415	25	5	3	1
1900	480	25	6	8	6
2000	542	23	4	15	2
2100	640	24	5	16	1
2200	731	25	5	6	1
2300	830	27	11	8	3
2400	941	23	3	8	1
2500	1050	26	10	5	1
2600	1210	25	5	6	1
2700	1374	26	7	7	2
2800	1508	26	6	8	1
2900	1663	25	5	5	2
3000	1937	26	5	20	4

y desviación estándar o media 1 de acuerdo a la Figura 1. Este valor de media se restó de los valores de media obtenidos de los distintos escenarios, desde n = 100 hasta n = 3000, y el resultado es el valor neto que se muestra en la Tabla 6.1.

En el canal de procesamiento los resultados mostraron el valor mínimo de media fue de 5 % donde n = 100 y el valor máximo fue de 30 % donde n = 1200. Se observó

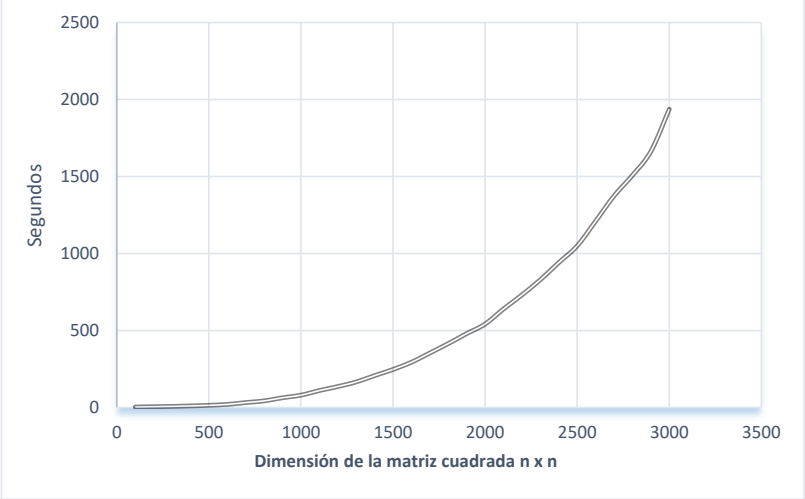

Figura 6.1. Tiempo de ejecución en segundos del método de Gauss-Jacques. (Fuente: Elaboración propia).

una media de 26 % cuando n = 3000, únicamente cinco veces el valor mínimo con el valor máximo de la variable n. El uso no aumenta de forma proporcional y los valores atípicos son mínimos y no afectan significativamente en el resultado final. Los valores de desviación estándar fueron 3 % el mínimo y 15 % el máximo, esto significa que el procesamiento no excede los recursos del dispositivo. Calcular una matriz inversa donde n = 3000, con 9000000 elementos consumió en promedio el 26 % del procesamiento disponible, por debajo del máximo obtenido en esta dimensión.

En el canal de memoria o RAM, se obtuvieron medias del 3 % y 20 % como valores mínimo y máximo. En desviación estándar los resultados fueron 0 % y 6 % como valores mínimo y máximo, es decir los recursos disponibles no son excedidos para matrices pequeñas o matrices grandes de 3000 x 3000 con 9000000 elementos. Es relevante que obtener la matriz inversa modular de una matriz de 1800 x 1800 con 3240000 elementos utiliza en promedio el 3 % de memoria.

En la Tabla 6.2, se observa el resumen estadístico del método Gauss-Jordan con modularización explícita en la función rref(), para todos los valores de n. Los datos fueron registrados en porcentaje, según lo muestra el administrador de tareas de Windows® y el tiempo de ejecución se presenta en segundos.

Tabla 6.2. Resumen estadístico de procesamiento y RAM del método Gauss-Jordan con modularización explícita para la función rref. (Fuente: Elaboración propia).

n	Tiempo[s]	$\bar{x}$ CPU %	SD CPU %	$\bar{x}$ RAM %	SD RAM %
100	2	11	1	2	2
200	2	4	4	2	0
300	3	11	6	2	0
400	4	21	16	2	0
500	5	40	21	6	1
600	8	43	19	7	0
700	11	45	20	5	0
800	15	50	22	4	0
900	20	58	18	4	1
1000	28	58	18	4	1
1100	36	65	7	4	0
1200	46	65	6	5	1
1300	60	66	8	5	1
1400	73	67	10	7	1
1500	90	67	7	7	1
1600	107	67	6	7	1
1700	129	68	6	8	1
1800	156	67	6	8	1
1900	176	68	4	8	1
2000	202	67	6	7	1
2100	221	68	4	7	1
2200	276	68	4	6	1
2300	311	68	4	5	1
2400	355	68	5	5	1
2500	387	67	4	4	1
2600	446	69	4	4	1
2700	513	69	6	8	1
2800	560	66	4	5	1
2900	614	67	4	5	1
3000	677	67	5	4	2

Se observó el aumento del tiempo de ejecución cuando la el tamaño de la matriz aumenta, definido por la variable n. El aumento no es proporcional, y se identifica cuando n = 500 fueron 5 s, para n = 1000 fueron 28 s, aunque es el doble de dimensión, no es el doble en tiempo.

Otro caso fue cuando n = 1500 fueron 90 s, mientras que para n = 3000 fueron 677

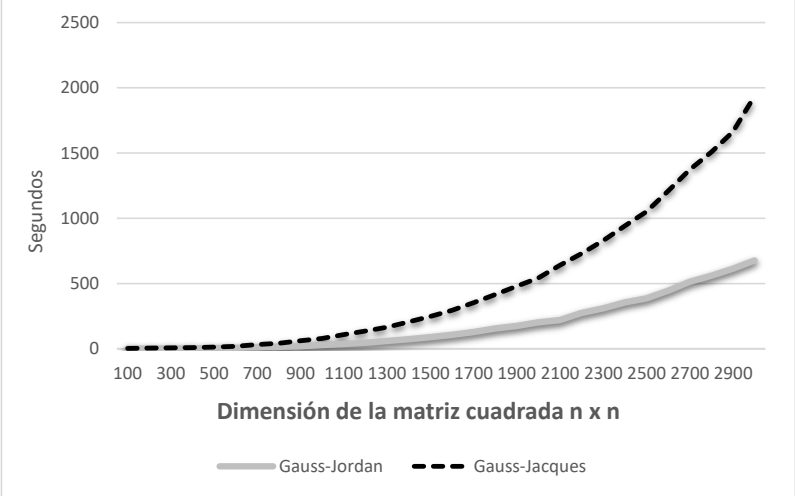

Figura 6.2. Comparación del tiempo de ejecución entre el método Gauss-Jacques y el método Gauss-Jordan con modularización explícita (función rref). (Fuente: Elaboración propia).

s, el primero con 2250000 elementos mientras que el segundo tuvo 9000000 elementos, confirmando así la no proporcionalidad en dimensión de la matriz o en número de elementos.

Se identificó un comportamiento logarítmico, alejándose del eje de las ordenadas mientras aumenta el eje de las abscisas, como se ve en la Figura 6.2.

Los resultados para Gauss-Jordan con modularización explícita en la función extendido euclidiano se muestran en la Tabla 6.3.

Tabla 6.3. Resumen estadístico de procesamiento y RAM del método Gauss-Jordan con modularización explícita función extendido euclidiano. (Fuente: Elaboración propia).

n	Tiempo[s]	$\bar{x}$ CPU %	SD CPU %	$\bar{x}$ RAM %	SD RAM %
9	1	35	20	8	0
99	1	1	3	8	1
999	1.3	2	2	8	0
9999	1.7	1	2	8	0
99999	1.3	2	3	8	1
999999	1.3	1	3	8	1
9999999	1.8	6	6	8	1
99999999	1.4	1	2	8	0
999999999	1.7	6	5	7	0
9999999999	1	1	4	7	0

Se observó que el tiempo para calcular el inverso modular de una cifra, cuando n = unidad o n = unidad de millar de millón es el mismo, no existe incremento significativo, siendo el valor máximo cuando n = unidad de millón o siete dígitos para la cifra n.

En procesamiento, se observó un valor atípico cuando n = unidad, siendo 35 % el máximo valor en este apartado y 2 % el menor cuando n = centena, unidad e millar o decena de millón. La desviación estándar confirma que no se excede el uso del procesador en ningún escenario, aunque el valor máximo 20 % cuando n = unidad muestra inestabilidad. En memoria o RAM, el valor mínimo es 7 % y el valor máximo es 8 % y se observó en el 80 % de los escenarios de la variable n. La desviación estándar confirma que no se excede el uso de la memoria, y para esta función este recurso se utiliza de forma estable.

Los resultados para Gauss-Jordan con modularización explícita en la función determinante se muestran en la Tabla 6.4.

Se observó que el tiempo para calcular el determinante de una matriz cuadrada n x n tiene un mínimo de 2 s y un máximo de 2.5 s. El valor máximo calculado como determinante fue 1.20E+45 para una matriz cuadrada donde la dimensión n = 23, calculada en 2 s.

En procesamiento, el uso mínimo fue de 2 % y el máximo de 5 %. Alrededor del 63 % de los casos utilizaron el 2 % del procesador para calcular el determinante, y sólo el 4 % utilizaron el valor máximo es decir el 5 % del procesador. El determinante 3.16E+18 utilizó el 5 % del procesador aunque no fue el valor máximo de todos los determinantes calculados. La desviación estándar muestra que no se excede el uso del procesador y también que existe estabilidad en el uso de este recurso.

En memoria o RAM, el valor mínimo es 16 % y el valor máximo es 19 %, teniendo poca diferencia entre sí. Calcular la determinante consumió más memoria que calcular la matriz reducida escalonada y que el extendido euclidiano, las funciones rref y extended euclidean respectivamente. La desviación estándar indica que los recursos no se exceden y que existe estabilidad en el uso de memoria.

También se observa a que a partir de la matriz de dimensión 134 x 134, el deter-

Tabla 6.4. Resumen estadístico de procesamiento y uso de RAM del método Gauss-Jordan con modularización explícita función determinante. (Fuente: Elaboración propia).

n	det	$\bar{x}$ CPU %	SD CPU %	$\bar{x}$ RAM %	SD RAM %
2	6598	2	4	16	0
3	-202277	2	4	17	0
4	13047186	3	3	17	0
5	1291702783	2	4	18	0
6	4067588053	3	4	18	0
7	8.94E+11	3	4	18	0
8	4.55E+14	2	3	19	0
9	-2.62E+14	2	3	18	0
10	3.16E+18	5	6	18	0
11	-3.22E+20	2	3	18	0
12	7.71E+22	3	4	18	0
13	-2.74E+24	3	3	18	0
14	-4.46E+26	2	4	18	0
15	-1.21E+29	2	4	18	0
16	2.20E+29	2	4	19	1
17	1.35E+32	2	4	19	1
18	-1.90E+35	2	3	18	0
19	-3.09E+36	2	4	18	0
20	-4.08E+38	2	3	18	0
21	3.26E+40	2	3	19	0
22	1.22E+43	3	3	19	0
23	1.20E+45	2	3	19	0
24	-7.94E+46	3	4	19	0
25	-3.59E+49	3	4	19	0
100	-2.25E+224	2	3	17	0
133	-3.63E+307	2	5	17	0
134	Inf	3	4	17	0

minante calculado es el valor Inf, que hace referencia a un número tan grande que no puede ser representado, generando así un desbordamiento de los recursos del sistema, es decir excede los recursos disponibles. Usar el método Gauss-Jordan con modularización explícita es conveniente para matrices menores a la dimensión 134 x 134, si son mayores se sobrepasan los recursos.

En la Figura 6.3 se muestra la comparación del uso del procesador que tuvieron ambos métodos. En el caso del método Gauss-Jordan con modularización explícita son

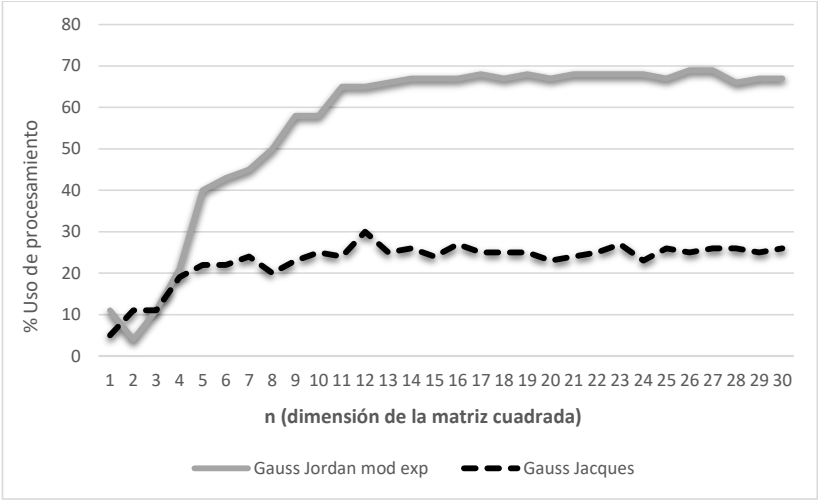

Figura 6.3. Comparación de uso de procesamiento entre el método Gauss-Jacques y el método Gauss-Jordan con modularización explícita (función rref). (Fuente: Elaboración propia).

los resultados para la función rref de la Tabla 6.2, es decir sólo se calcula la matriz inversa natural, y no la matriz inversa modular, sin embargo, demanda más uso del procesador comparado con Gauss-Jacques, que exige menos uso de procesador pero genera la matriz inversa modular.

En la Figura 6.4 se muestra la comparación del uso de memoria o RAM que tuvieron ambos métodos.

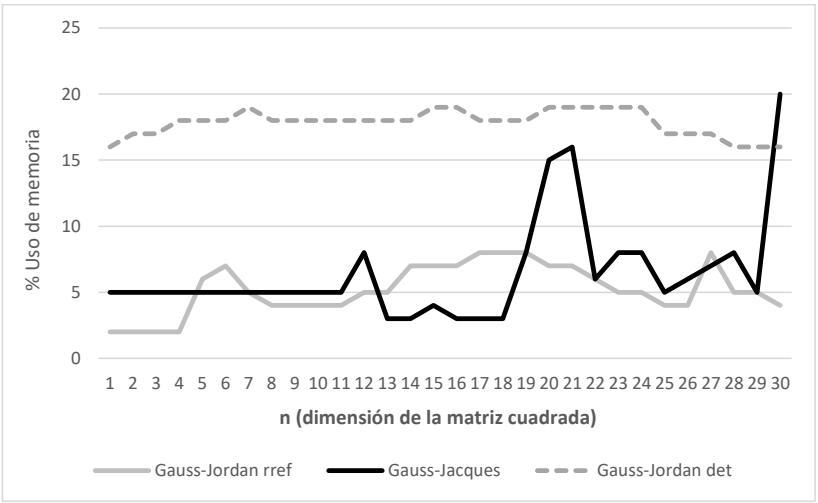

Figura 6.4. Comparación de uso de memoria entre el método de Gauss-Jacques y el método Gauss-Jordan con modularización explícita (función rref y función det). (Fuente: Elaboración propia).

El resultado de Gauss-Jordan rref pertenece a la Tabla 6.2. El resultado de Gauss-Jacques pertenece a la Tabla 6.1. El resultado de Gauss-Jordan det pertenece a la Tabla 6.4, agregando tres muestras con el valor mínimo de 16 % para hacer una equivalencia en el total de valores comparados. No se agregó el uso de memoria al calcular el extendido euclidiano mostrado en la Tabla 6.3 debido a que tiene únicamente diez muestras. Se observó que Gauss-Jordan con modularización explícita para la función que calcula el determinante demanda más memoria que para la función rref o matriz escalonada reducida o modular inversa natural y también demanda más memoria que el método Gauss-Jacques.

Capítulo 7

Conclusiones

Las pruebas realizadas brindaron información sobre las características y el funcionamiento de cada método en un ambiente controlado con un dispositivo habitual que dispone de recursos moderados, lo que hace posible considerar trabajos futuros con dispositivos de recursos limitados frecuentemente utilizados en IoT.

Ambos métodos calculan la matriz inversa modular de una matriz dada. Entre los usos de una matriz inversa modular es la criptografía simétrica, donde es utilizada como llave para cifrar el mensaje y finalizar el proceso, es decir descifrarlo. El tamaño de la llave debe ser del mismo tamaño que tiene el mensaje, con el propósito de brindar seguridad, por lo que trabajar con llaves de diversas dimensiones en este trabajo fue necesario hacia una aproximación de la secrecía perfecta de Shannon.

El módulo utilizado fue el número primo 89, las matrices inversas modulares obtenidas contiene números enteros positivos hasta 89. Trabajos futuros podrán realizarse utilizando módulos distintos.

El método Gauss-Jacques utilizó el 30 % de procesamiento como valor máximo y el 20 % de memoria, donde la matriz más pequeña tenía 10000 hasta 9000000 de elementos de la matriz más grande, donde cada elemento son números enteros positivos de hasta dos dígitos. El tiempo de ejecución es mayor que en Gauss-Jordan con modularización explícita para la función que calcula la matriz escalonada reducida o la matriz inver-

sa natural; sin embargo Gauss-Jacques calcula la matriz inversa modular, es decir, el proceso completo.

El método Gauss-Jordan con modularización explícita utilizó el 69 % de procesamiento como valor máximo y pertenece a la función que calcula la matriz inversa natural, mientras que utilizó el 19 % de memoria como valor máximo y se generó en la función que calcula el determinante. Aunque el tiempo de ejecución es menor que en el método Gauss-Jacques, a menor o mayor dimensión de la matriz, el valor de la función determinante cambia proporcionalmente. El cálculo del determinante es un algoritmo recursivo con un costo computacional significativo, haciendo que sea eficiente para matrices de menor tamaño pero no para matrices de mayor dimensión. En el caso de Gauss-Jacques, el tamaño de la matriz no fue una limitante en este trabajo.

La complejidad computacional de Gauss-Jacques es una dimensión mayor a la complejidad de Gauss-Jordan con modularización explícita, cúbica y cuadrática respectivamente. En términos precisos, esta diferencia hace más eficiente el método de menor complejidad, que en este caso es Gauss-Jordan con modularización explícita. No obstante, los resultados muestran que el método Gauss-Jacques es más estable, no sobrepasa los recursos disponibles y permite trabajar con matrices de mayor tamaño, haciendo posible tener una aproximación al secreto perfecto de Shannon aplicado a la criptografía simétrica.

Referencias

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., and Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (iot) security. *IEEE Communications Surveys & Tutorials*, 22(3):1646–1685.

Alhayani, B., Abbas, S. T., Khutar, D. Z., and Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. *Materials Today: Proceedings*.

Avoine, G. and Hernandez-Castro, J. (2021). *Security of Ubiquitous Computing Systems: Selected Topics*. Springer Nature.

Barlybayeva, S. (2022). Creativity and media culture in modern kazakhstan. volume 345 LNNS.

Bernhard, I., Gustafsson, M., Hedström, K., Seyferin, J., and Whilborg, E. (2019). A digital society for all?: meanings, practices and policies for digital diversity. In *52nd Hawaii International Conference on System Sciences (HICSS-52), January, Grand Wailea, Maui, 8-11, 2019*, pages 3067–3076.

Burkhanov, R., Gagarin, A., and Novopashin, S. (2022). Human, posthuman and culture in the digital society. *KnE Social Sciences*, pages 61–69.

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and mathematical organization theory*, 26(4):365–381.

Carrión, Ó. (2021). Criptografía para principiantes: método de playfair (wheatstone). *Entorno Abierto*, 40:27–30.

Chi Domínguez, J. J. (2019). Elliptic curves in classical and post-quantum cryptography= curvas elípticas en la criptografía clásica y post-cuántica.

Christen, M., Gordijn, B., and Loi, M. (2020). *The ethics of cybersecurity*. Springer Nature.

Dawahdeh, Z. E., Yaakob, S. N., and bin Othman, R. R. (2018). A new image encryption technique combining elliptic curve cryptosystem with hill cipher. *Journal of King Saud University-Computer and Information Sciences*, 30(3):349–355.

Diène, B., Rodrigues, J. J., Diallo, O., Ndoye, E. H. M., and Korotaev, V. V. (2020). Data management techniques for internet of things. *Mechanical Systems and Signal Processing*, 138:106564.

Dufva, T. and Dufva, M. (2019). Grasping the future of the digital society. *Futures*, 107.

Eisenberg, M. (1999). Hill ciphers and modular linear algebra. *Mimeographed notes*, 165(9):1–19.

Esteve Romero, A. (2019). *Arqueología informática: Implementación de sistemas clásicos de cifrado en Scratch*. PhD thesis, Universitat Politècnica de València.

Fuchs, C. (2020). Towards a critical theory of communication as renewal and update of marxist humanism in the age of digital capitalism. *Journal for the Theory of Social Behaviour*, 50(3):335–356.

García, F. M. J. (2021). Reflexiones acerca del papel de la tecnología en el pensamiento marcusiano en el marco de la sociedad industrial avanzada. *Revista Tecnologia e Sociedade*, 17.

García Aretio, L. et al. (2019). Necesidad de una educación digital en un mundo digital. *RIED. Revista Iberoamericana de Educación a Distancia*.

García Merayo, F. (2015). *Matemática discreta*. Ediciones Paraninfo, SA.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., and Aylin, P. (2019). A retrospective impact analysis of the wannacry cyberattack on the nhs. *NPJ digital medicine*, 2(1):1–7.

Greengard, S. (2021). *The internet of things*. MIT press.

Grimaldi, R. P. (2003). *Matemáticas discretas y combinatoria: una introducción con aplicaciones*. Pearson Educación.

Hammad, B. T., Sagheer, A. M., Ahmed, I. T., and Jamil, N. (2020). A comparative review on symmetric and asymmetric dna-based cryptography. *Bulletin of Electrical Engineering and Informatics*, 9(6):2484–2491.

Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. *Journal of Information Security*, 11(3):138–148.

Hasoun, R. K., Khlebus, S. F., and Tayyeh, H. K. (2021). A new approach of classical hill cipher in public key cryptography. *International Journal of Nonlinear Analysis and Applications*, 12(2):1071–1082.

Hernández-Sampieri, R. and Torres, C. P. M. (2018). *Metodología de la investigación*, volume 4. McGraw-Hill Interamericana México^ eD. F DF.

Hwang, S. O., Kim, I., and Lee, W. K. (2021). *Modern Cryptography with Proof Techniques and Implementations*. CRC Press.

Ibañez, R. (2017). Criptografía con matrices, el cifrado de hill.

Ivanova, I., Pulyaeva, V., Vlasenko, L., Gibadullin, A., and Safarov, B. (2020). Collaboration of different generations in the digital environment of the economy. In *IOP Conference Series: Earth and Environmental Science*, volume 421, page 032039. IOP Publishing.

Jacques-García, F. A., Uribe-Mejía, D., Macías-Bobadilla, G., and Chaparro-Sánchez, R. (2022). On modular inverse matrices a computation approach. *South Florida Journal of Development*, 3(3):3100–3111.

Jara-Vera, V. and Sánchez-Ávila, C. (2020). Cryptobiometrics for the generation of cancellable symmetric and asymmetric ciphers with perfect secrecy. *Mathematics*, 8(9).

Johnsonbaugh, R. (2005). *Matemáticas discretas*. Pearson Educación.

Kahn, D. (1967). *The Codebreakers The Story of Secret Writing*. Macmillan.

Kandasamy, K., Srinivas, S., Achuthan, K., and Rangan, V. P. (2020). Iot cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, 2020:1–18.

Katz, J. and Lindell, Y. (2020). *Introduction to modern cryptography*. CRC press.

Khraisat, A. and Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, 4(1):1–27.

Konheim, A. G. (1981). *Cryptography, a primer*. John Wiley & Sons, Inc.

Konheim, A. G. (2007). *Computer security and cryptography*. John Wiley & Sons.

Kumar, T. M., Reddy, K. S., Rinaldi, S., Parameshachari, B. D., and Arunachalam, K. (2021). A low area high speed fpga implementation of aes architecture for cryptography application. *Electronics*, 10(16):2023.

Larson, R. and Falvo, D. C. (2010). *Fundamentos de álgebra lineal, Sexta edición*. Cengage Learning Editores, S.A. de C.V.

Lee, I. (2020). Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. *Future Internet*, 12(9):157.

Lemus, M. (2021). Articulaciones entre desigualdades, aprendizajes y tecnologías digitales: un recorrido por conceptos clave. *Cuestiones de sociología*, page e118.

Levin, I. and Mamlok, D. (2021). Culture and society in the digital age. *Information (Switzerland)*, 12.

Lindley, J. G., Coulton, P., Akmal, H., Hay, D., Van Kleek, M., Cannizzaro, S., and Binns, R. (2019). The little book of philosophy for the internet of things.

Martínez, R., Palma, A., and Velásquez, A. (2020). Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en américa latina.

Meizar, A., Tambunan, F., Ginting, E., et al. (2019). Optimizing the complexity of time in the process of multiplying matrices in the hill cipher algorithm using the strassen algorithm. In *2019 7th International Conference on Cyber and IT Service Management (CITSM)*, volume 7, pages 1–4. IEEE.

Moreno, G. C. F. and Díaz, E. A. V. (2020). Estudio de la teoría de números aplicada a algunos métodos criptográficos haciendo uso de las tic. *Revista Electrónica de Conocimientos, Saberes y Prácticas*, 3(1):49–71.

Murad, S. H. and Rahouma, K. H. (2022). Hybrid cryptography for cloud security: Methodologies and designs. In *Digital Transformation Technology*, pages 129–140. Springer.

Nofriansyah, D., Defit, S., Nurcahyo, G. W., Ganefri, G., Ridwan, R., Ahmar, A. S., and Rahim, R. (2018). A new image encryption technique combining hill cipher method, morse code and least significant bit algorithm. In *Journal of Physics: Conference Series*, volume 954, page 012003. IOP Publishing.

Paar, C. and Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

Patil, P. and Bansode, R. (2020). Performance evaluation of hybrid cryptography algorithm for secure sharing of text & images. *International Research Journal of Engineering and Technology*, 7(9):3773–3778.

Prasad, K. and Kumari, M. (2020). A review on mathematical strength and analysis of enigma. *arXiv preprint arXiv:2004.09982*.

Prieto, M. J. (2020). *Historia de la criptografía: Cifras, códigos y secretos desde la antigua Grecia a la Guerra Fría*. La Esfera de los Libros.

Rani, S., Kataria, A., and Chauhan, M. (2022). Fog computing in industry 4.0: Applications and challenges—a research roadmap. In *Energy Conservation Solutions for Fog-Edge Computing Paradigms*, pages 173–190. Springer.

Ryabko, B. and Fionov, A. (2021). *Cryptography in the Information Society*. World Scientific.

Sehgal, S. K. and Gupta, R. (2019). A comparative study of classical and quantum cryptography. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 869–873.

Serrano Pinilla, P. (2018). Reproducción de ataque de fallos en el algoritmo advanced encryption standard utilizando simulación hdl.

Stallings, W., Brown, L., Bauer, M. D., and Bhattacharjee, A. K. (2020). *Computer security: principles and practice*. Pearson Education Upper Saddle River, NJ, USA.

Stanley, G. S. and Flores Godoy, J. J. (2012). *Algebra lineal*. McGrawHill.

Sulaiman, S. and Hanapi, Z. M. (2021). Extensive analysis on images encryption using hybrid elliptic curve cryptosystem and hill cipher. *Journal of Computer Science*, 17.

Sánchez, J., Mallorquí, A., Briones, A., Zaballos, A., and Corral, G. (2020). An integral pedagogical strategy for teaching and learning iot cybersecurity. *Sensors (Switzerland)*, 20.

UNESCO (2018). A global framework of reference on digital literacy skills for indicator 4.4.2.

Valdivia, E. J. S. and Miranda, J. M. (2020). Proposal of a intelligent agent for management and mitigation in cibersecurity risk for iot environments. In *2020 9th International Conference On Software Process Improvement (CIMPS)*, pages 148–154. IEEE.

Vargas, K. A. D., de Abiega, A. F., L'Eglisse, G. G.-G., and Cabarcas, D. (2019). Un acercamiento a la línea del tiempo de los algoritmos criptograáficos. *Revista Digital Universitaria*, 20(5).

Voronkova, V., Nikitenko, V., Oleksenko, R., Cherep, O., Andriukaitiene, R., and Briki, I. (2021). Digital paradigm of economy and management in the conditions of global human transformation. *Technology transfer: innovative solutions in Social Sciences and Humanities*, pages 37–40.

Zhardemova, M., Khristidis, T., Karmazina, N., Fedorova, S., and Yakovleva, E. (2021). Digital competences in the aspect of sociocultural education. In *SHS Web of Conferences*, volume 98. EDP Sciences.

Zhou, H. and El Gamal, A. (2020). Network information theoretic security. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 978–983. IEEE.