Tecnológico de Costa Rica

Escuela de Computación

Programa de Maestría en Computación

Mecanismo de seguridad multinivel utilizando encriptación de lattices y estenografía

Propuesta de tesis para optar por el título de Máster en Computación con énfasis en Ciencias de la Computación

Autor

Javier Buzano González

Tutor

PhD. Antonio González Torres

Cartago, 12 de junio de 2023

Índice general

1 Introducción **1**

1.1 Estado del arte 2
1.2 Planteamiento del problema 4
1.3 Justificación del problema 6
1.4 Hipótesis 8
1.5 Objetivos 8
1.5.1 Objetivo general 8
1.5.2 Objetivos específicos 8
1.6 Alcance, limitaciones y entregables 9
1.6.1 Alcance y limitaciones 9
1.6.2 Entregables 9

2 Marco teórico **11**

2.1 Criptografía 11
2.1.1 Criptografía Clásica 12
2.1.2 Criptografía Moderna 13
2.1.3 Criptografía Post Quantum 16
2.2 Estenografía 20
2.2.1 Estenografía basada en inyección 20
2.2.2 Estenografía basada en sustitución 21
2.2.3 Estenografía basada en transformación 21

3 Metodología **25**

3.1 Descripción de la metodología 25
3.2 Planteamiento de los experimentos 26
3.2.1 Comparar la ejecución secuencial de Shinobice y RSA 27
3.2.2 Comparar la eficiencia entre las ejecuciones secuenciales y paralelas basadas en multihilo de Shinobice 27
3.2.3 Comparar las ejecuciones secuenciales y paralelas con operaciones vectoriales de Shinobice 28
3.2.4 Comparar la ejecución secuencial, paralela con multihilos y paralela con operaciones vectoriales de Shinobice 29

4 Calendario propuesto **31**

4.1 Detalle de tareas 31

Bibliografía **33**

Capítulo 1

Introducción

La criptografía nació de la necesidad de incrementar los niveles de seguridad en épocas de guerra. El objetivo es que los enemigos no obtuvieran información vital que se transmitía por diversos medios de comunicación relacionados con la logística de la guerra. El uso de la criptografía es uno de los medios más utilizados para mantener la confidencialidad de la información.

La información es un activo que despierta el interés de los hackers, aún en la ausencia de conflictos. Por eso es vital resguardar su confidencialidad, integridad, disponibilidad y garantizar el no repudio de los datos [37]. La preservación de estas características permiten garantizar la transmisión segura de la información en cualquier escenario.

La realización de comunicaciones seguras requiere utilizar instrumentos que aseguren que las características mencionadas prevalecen durante las transmisiones. Los principales métodos de encriptación son los simétricos y los asimétricos. Los primeros utilizan una llave privada para encriptar y desencriptar los mensajes, mientras que los segundos usan una llave pública y una privada para realizar las mismas operaciones. Los dos métodos necesitan contar con mecanismos para intercambiar las llaves entre las partes.

La criptografía asimétrica, conocida como criptografía de llave pública (PKE)[1], puede utilizar mecanismos como las firmas digitales basados en algoritmos como Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA)[9] y los basados en distribución de llaves y secretos, como Diffie-Hellman (DH) [13].

En cuanto a la criptografía simétrica, los algoritmos que se utilizan son Data Encryption Standard (DES) [6] y Advanced Encryption Standard (AES) [7]. Este último cuenta con un gran número de variantes que son las más utilizados en la actualidad, y han sustituido en la mayoría de aplicaciones a DES. AES es en la actualidad el algoritmo más importante en criptografía, y es usado por la *National Security Agency* (NSA) de los Estados Unidos de América [1] y un gran número de institutiones financieras a nivel mundial.

A lo largo de los años se han usado múltiples métodos para romper la seguridad de los

[1]PKE se deriva del término en inglés Public Key Encryption.

algoritmos mencionados utilizando medios arcaicos, como estrategias de fuerza bruta, el azar o ideas truculentas que facilitan engañar a alguna o ambas partes de la comunicación para interponerse entre ellos e interceptar, reemplazar o modificar la información [28].

Los algoritmos que históricamente se conocen como seguros, porque teóricamente no se cuenta con la capacidad para romper su seguridad en un tiempo polinomialmente acotado, están siendo amenazados por métodos emergentes como la computación cuántica. La promesa de estas tecnologías es proporcionar la capacidad computacional suficiente para resolver la complejidad de estos algoritmos, en tiempo logarítmico. Entre los algoritmos cuya seguridad podría estar más comprometida se encuentran RSA y DH [43, 14] en relación con AES, que es más resistente y puede sufrir un impacto menor [33].

Los esfuerzos para definir mecanismos para garantizar las propiedades de la seguridad de la información consideran la criptografía post-cuántica (PQC[2]) o criptografía cuántica-resistente. Esta busca sustituir los algoritmos de llave pública que comprometen a estas propiedades [2].

En la actualidad la criptografía de *lattices* [3] está siendo considerada como una de las mejores alternativas en este campo. Este tipo de criptografía es más robusta que los métodos actuales de PKE debido a que se fundamenta en problemas matemáticos complejos (fuertes) para encontrar o detectar vectores inusualmente pequeños (SVP, CVP y LWE [11]).

Con los métodos actuales que cuentan los hackers es posible que obtengan información a partir del establecimiento de la existencia de comunicaciones entre dos actores importantes. Por ejemplo, si tienen conocimiento de las horas y días que los altos ejecutivos de determinadas compañías realizan transacciones en la bolsa, pueden lanzar ataques para interceptar esas transmisiones y obtener ventajas económicas en el mercado bursátil.

La propuesta de métodos de seguridad para incrementar los niveles de seguridad de las comunicaciones es un reto, tanto para los gobiernos como las compañías. Esta investigación tiene por fin proponer un método de seguridad multinivel considerando el uso de criptografía de *lattices* y mecanismos estenográficos en archivos multimedia. La propuesta tiene por fin ocultar la información crítica para que pase desapercibida durante las comunicaciones y ofrecer una alternativa resistente a los ataques con computación cuántica.

1.1 Estado del arte

La estenografía y la criptografía son de gran relevancia en el campo de la ciberseguridad. La esteganografía se refiere al encubrimiento de mensajes (sin trazabilidad) de manera que solo el receptor pueda interpretarlos. Mientras que la criptografía es el arte de convertir texto plano en algo ilegible. El uso de cada una por separado son métodos de seguridad

[2]La cual deriva del término en inglés Post Quantum Cryptography.

[3]El término en inglés lattice se traduce al español como enrejado. Un enrejado periódico de puntos en $\mathbb{Z}^m$, en criptografía, m se encuentra al menos en varios miles de dimensiones.

robustos, pero la combinación de ambas puede proporcionar resultados con mayores niveles de seguridad. En ese sentido, Mohamed *et al.* realizan un análisis comparativo de métodos que combinan diferentes técnicas de criptografía y estenografía para obtener sistemas híbridos [45] y muestran conclusiones interesantes.

La estenografía se ha usado no solo para ocultar mensajes sino también para esconder el intercambio de llaves por medio de la utilización de textos estenográficos. Este método fue denominado por Von Ahn y Hoper como Estenografía de Llave Pública [47].

En conjunto con la estenografía se pueden aplicar estrategias ingeniosas para mejorar la seguridad. Un ejemplo interesante contempla el intercambio de múltiples llaves y fue aplicado por Srihitha *et al.* [44]. La aplicación que efectuaron consistió en utilizar una llave para encriptar la imagen donde se oculta el mensaje, y a su vez encriptaron el mensaje con otra llave. Con este método el receptor necesita las dos llaves para decodificar el mensaje.

De acuerdo con la revisión bibliográfica efectuada, existe poca información sobre la combinación de criptografía de *lattices* con estenografía. La mayoría de trabajos de investigación se enfocan en mejorar el rendimiento de los algoritmos que se utilizan en la criptografía de *lattices* sin sacrificar el nivel de seguridad. En este contexto conviene señalar que los *lattices* son parte esencial de la criptografía post-cuántica, y que por esa razón se seleccionaron recientemente los primeros candidatos a ser considerados como estándares de este tipo de mecanismos.

El 22 de julio del 2020, en la tercera ronda de evaluación de evaluación de candidatos de candidatos de criptografía post-cuántica a convertirse en estándares [3], el Instituto Nacional de Estándares y Tecnología (NIST[4]) publicó los finalistas, dentro de los cuales existían varias propuestas relacionadas con *lattices*. Los candidatos seleccionados utilizan firmas digitales y llave pública. En el caso de los candidatos seleccionados que utilizan llave pública CRYSTALS, NTRU y SABER, mientras que FALCON y CRYSTALS son propuestas para firmas digitales. En este caso CRYSTALS tenía propuestas para ambos métodos.

CRYSTALS[5] propone un método de llave pública (PKE) que usa una primitiva de criptografía conocida como Kyber [15], la cual se basa en problemas duros sobre *lattices* modulares. En tanto, NTRU [25] comprende la unificación de otras dos propuestas que se presentaron, NTRUEncrypt [8] y NTRU-HRSS-KEM [27]. La propuesta de NTRU se fundamenta en el Shortest Vector Problem (SVP) para encriptación/desencriptación y en el Closest Vector Problem (CVP) para firmas digitales. Mientras que SABER [16] se basa en la solución del problema de *Module Learning With Rounding (MLWR)*, que es una variante de *Learning With Errors (LWE)*.

Con respecto a las propuestas para firmas digitales, y que también se encuentran basadas

[4]NIST es la abreviatura en inglés para *National Institute of Standards and Technology*.
[5]CRYSTALS es la abreviatura para el término en inglés *Cryptographic Suite for Algebraic lattices*.

en *lattices*, CRYSTALS utiliza la primitiva de Dilithium [41] junto a FALCON[6] [19], que se basa en el marco teórico de Gentry *et al.* [21], para utilizar los esquemas de firma basados en *lattices*.

La elección final de los primeros candidatos que se convertirán en estándares se publicó el 5 de julio del 2022 [5]. Los candidatos seleccionados fueron CRYSTALS-Kyber en la categoría de criptografía pública, CRYSTALS-Dilithium y FALCON en firmas digitales. Los algoritmos mencionados son un subconjunto de los elegidos, y se encuentran relacionados con *lattices*. Ese mismo día se convocó la cuarta ronda de envío de propuestas [4]. Con respecto a esta elección, Ingrid Verbauwhede (i.e., integrante del equipo de implementación de SABER) manifestó en una presentación en la conferencia de *Intel Crypto Frontiers Center*[46] que CRYSTALS-Kyber resultó elegido, incluso cuando SABER ofrecía mejores resultados en términos de rendimiento, debido a que su base matemática es más sólida.

El número de publicaciones que se encontró sobre investigaciones que combinan el uso de *lattices* con esteganografía es reducido. Entre los trabajos que destacan se encuentra el realizado por Hadi *et al.* [42], quiénes proponen un método esteganográfico que usa cuantización sobre vectores de *lattices* y Discrete Wavelet Transform (DWT). Este proporciona un mecanismo efectivo para ocultar la información.

Por su parte, Febrian y Bayu [29] indican que el robo de credenciales es una de las formas más comunes de filtración de datos. Por lo que consideran que el uso aislado de la criptografía no es suficiente, y la utilización de criptografía de *lattices* con NTRU, junto con métodos estenográficos, como *Least Significant Bit (LSB)* para ocultar los mensajes en imágenes, es una alternativa que puede tener especial relevancia.

En tanto, Yiming *et al.* [26] utilizan *lattices* con R-LWE para ocultar mensajes en vídeo. Los investigaroes implementaron el mecanismo estenográfico de *Discrete Cosine Transform (DCT)*, con el cual permite obtener imágenes poco distorsionadas.

1.2 Planteamiento del problema

En los últimos años las personas y las organizaciones se han visto beneficiadas con el incremento de la capacidad de procesamiento, memoria y almacenamiento de los equipos computacionales. Esto incluye los teléfonos inteligentes, tabletas, computadoras portátiles, de escritorio, servidores, FPGAs[7] y ASICs[8]. Este incremento en la capacidad de cómputo de los dispositivos ha favorecido la aparición de nuevos algoritmos, métodos y técnicas para el análisis y procesamiento de datos.

Estos avances han permitido la creación de nuevos mecanismos de protección de la información, pero también ha favorecido a los cibercriminales, que de forma análoga cuentan con mayor capacidad de cómputo y herramientas más sofisticadas para llevar a

[6]FALCON se deriva de *Fast-Fourier Lattice-based Compact Signatures Over NTRU* en inglés.
[7]Acrónimo derivado del inglés Field Programmable Gates Array
[8]Acrónimo derivado del inglés Application-Specific Integrated Circuit

cabo los ataques a los sistemas informáticos.

Así, por ejemplo, la computación cuántica supone un incremento significativo en la capacidad de cómputo para resolver problemas complejos que no pueden ser abordados con la tecnología precedente, pero también ofrece mayores oportunidades a los cibercriminales para afectar la seguridad de los sistemas informáticos. Esto requiere anticipar el impacto negativo de las nuevas tecnologías en la seguridad de los sistemas y la información mediante el diseño e implementación de mecanismos de defensa no convencionales. Entre los aspectos más importantes que se deben considerar durante el diseño de las soluciones de ciberseguridad es necesario contemplar que los agentes externos no deben conocer:

- Los mecanismos de seguridad que utilizan las soluciones.
- Los activos de información que tienen valor estratégico y económico.
- La existencia de las comunicaciones de datos sensibles.

El diseño de métodos para garantizar los aspectos mencionados utilizando técnicas aisladas es poco factible. Esto requiere combinar métodos complementarios con características particulares para brindar una solución robusta que oculte y proteja las comunicaciones sensibles con altos niveles de seguridad. Como consecuencia, este trabajo de investigación tiene por fin proponer una solución de seguridad multinivel, que combina el uso de criptografía y esteganografía, que busca responder la pregunta de investigación **PI1**:

PI1 ¿Es posible diseñar e implementar un mecanismo de seguridad multinivel basado en criptografía de *lattices* (M-LWE) y estenografía (DCT) aplicada a imágenes?

La respuesta a esta pregunta tiene como objetivo contribuir en la solución de problemas en diferentes contextos. En particular, se puede considerar el siguiente escenario en el ámbito militar:

Un equipo militar especial se encuentra operando un grupo de drones (e.g un UAV[a]) en territorio enemigo. Estos drones están capturando imágenes sobre instalaciones militares y puntos estratégicos. Las imágenes se deben transmitir con los detalles del análisis que han realizado los especialistas, que incluye posibles estrategias de incursión desde sus campamentos. Además, las imágenes no deben ser las originales, por lo que a partir de estas se crean otras de forma aleatoria utilizando un algoritmo genético que las combina con las de un banco de figuras de dibujos animados de películas de entretenimiento. La transmisión de las imágenes y el análisis debe pasar desapercibida, para que en caso de que sean capturadas el contenido no despierte interés y la información no sea descifrada con facilidad.

[a]UAV deriva del término en inglés *Unnamed Aerial Vehicle*

1.3 Justificación del problema

DES [6] estuvo vigente por 24 años (1977-2001), AES [7] de momento lleva 21 años en vigencia y mucho del éxito que han tenido estos algoritmos es dado a la sana competencia por definir estándares que protejan la seguridad de los sistemas de información que facilitan nuestro diario vivir. NIST, al igual que con DES y AES, es el encargado de supervisar la justa escogencia de los mecanismos que busquen defender nuestros datos una vez existan algoritmos que puedan vulnerar los actuales sistemas de seguridad.

La criptografía de *lattices* ha sido considerada de interés desde finales de los noventas con las publicaciones de Ajtai [12]. Hoy en día, gran cantidad de las propuestas a ser el nuevo estándar para criptografía post-cuántica se encuentran basados en ellos.

El uso de *lattices* es considerado por múltiples investigaciones como una alternativa a los esquemas de criptografía tradicional, que pueden ser vulnerados utilizando computadoras cuánticas, debido a su capacidad para conservar los niveles de seguridad [40, 35]. La seguridad relacionada a la criptografía de *lattices* radica en la complejidad matemática de la especificación de problemas, como por ejemplo, *CVP*, *SVP*, *LWE*, *R-LWE* y *M-LWE*.

La utilización de *R-LWE* permite hacer uso de mecanismos rápidos y prácticos como lo son las Transformadas Rápidas de Fourier, lo cual habilita operaciones eficientes [$\mathrm{O}(n * \log n \mod q)$] y embarazosamente paralelizables [25, 34, 38, 32].

Los métodos basados en problemas fuertes sobre *lattices* brindan una amplia gama de aplicaciones a nivel de criptografía, dado que habilitan el intercambio de llaves y la criptografía de llave pública, lo cual ayuda a suplir las deficiencias que trae a colación la computación cuántica en algunos de los algoritmos que se utilizan actualmente. También facilita cifrados de bloque, los cuales son pilares de *AES*, y la transferencia inconsciente.

En un caso hipotético, donde se tiene en posesión materia prima valiosa la cual necesita ser trabajada para poder ponerse en venta y donde existe el temor al robo, es necesario contar con los mecanismos adecuados:

> Como dueño de una tienda de joyería, es necesario dar con un método en el cual los dependientes puedan trabajar sobre la materia prima sin exponer la misma y una vez pulida, vender los productos terminados. Para ello se confecciona una **caja de seguridad especial** en la cual en conjunto a la utilización de unos **guantes particulares** es posible manipular los bienes con la salvedad de que solo los que poseen estos guantes son capaces de acceder a los materiales. Dato importante es que con los guantes se puede modificar los objetos dentro de la caja e inclusive añadir nuevos, mas no es posible sacar nada de ella.

La metáfora anterior fue parafraseada de los ejemplos expuestos en la disertación doctoral de Gentry [20] en el año 2009. La misma hace referencia a lo que se conoce como el santo grial de la criptografía, la encriptación homomórfica completa que fue demostrada posible

por medio del uso de criptografía de *lattices* en la misma publicación.

De momento se cuenta con pocas aplicaciones las cuales alcancen niveles prácticos para el estado de la tecnología, pero gracias a este aporte se han desencadenado una serie de investigaciones y múltiples propuestas de esquemas que ayudan a solventar esta problemática. Enfocarse en mejorar los núcleos de estas aplicaciones como lo es la criptografía de *lattices* tendría un impacto no solo para esta propuesta, sino que que a todo lo que involucre el uso de criptografía l*attices* como base de su tecnología.

Como se ha mencionado como parte de este estudio, la criptografía por sí sola cuenta con niveles de seguridad los cuales inclusive hoy en día se pueden ver vulnerados. Dicha premisa no discrimina a uno de los algoritmos elegidos por NIST para PQC, el cual se demostró vulnerable a tan solo meses de haber sido seleccionado.

CRYSTALS-Kyber, uno de los algoritmos que fue seleccionado para ser estandarizados, se diseñó con el fin de que resistiera ataques de canal lateral. Este algoritmo, en su momento, fue calificado como un avance en las pruebas cuántico-seguras. Sin embargo, los investigadores del KTH Royal demostraron sus debilidades al utilizar ataques de canal lateral.

Los científicos del KTH Royal determinaron que las pequeñas variaciones de consumo de energía o de radiación electromagnética que se utilizan en los sistemas sirven para reconstruir el estado de la máquina, y con esto encontraron pistas que les permitieron obtener acceso forzado a los equipos que lo utilizaban.

Las pruebas realizadas a CRYSTALS-Kyber demostraron que es seguro hasta el tercer nivel de enmascaramiento de llaves, en contraste con los resultados obtenidos por Dubrova, Ngo y Gärtner [17] que demostraron que el método no era efectivo en el quinto orden de enmascaramiento. Este grupo de investigación aprovechó las capacidades del aprendizaje automático para superar el nivel de protección de las contra-medidas convencionales del enmascaramiento.

La existencia de mecanismos de seguridad confiables, no garantiza la confidencialidad de la información, debido que contar con conocimiento sobre la existencia de una comunicación, revela más que los mensajes secretos que se puedan estar transmitiendo.

Al igual que en muchos casos del reino animal, la sobrevivencia no está definida por las fortalezas del más fuerte, o seguro, en el caso de este planteamiento. En ocasiones es necesario ser el más listo y pasar desapercibido. Muchos animales cuentan con mecanismos que les permiten camuflarse de manera natural. Esto es análogo en la seguridad de la información y comunicaciones, que cuentan con estrategias ingeniosas para ocultar los mensajes y que no sean detectados fácilmente, como es el caso de la estenografía.

Existen diferentes tipos de métodos estenográficos aplicables a múltiples tipos de archivos. El estudio comparativo que presenta Kumar contrasta la aplicación de *Least Significant Bit (LSB)*, *Discrete Wavelet Transform (DWT)* y *Discrete Cosine Transform (DCT)* sobre imagenes concluyendo que *DCT* obtiene mejores resultados [22].

Acorde al trabajo realizado por Taha *et al* [45], los métodos estenográficos por más elaborados e interesantes que sean, no suplen o brindan la seguridad que proveen los mecanismos de criptografía. Lo que sí se puede decir es que la combinación de estos mejora las condiciones, la robustez, y que al utilizar solo uno de ellos implica estar propenso a las vulnerabilidades que poseen estos por sí solos. Esto presenta fuertes indicios de que los sistemas de seguridad multinivel brindan ciertas ventajas sobre el aislamiento.

1.4 Hipótesis

Esta sección presenta la hipótesis principal de este trabajo de investigación, que será validada mediante un conjunto de experimentos.

Hipótesis 1: Las comunicaciones de datos de principio a fin basado en *lattices* con estenografía proporcionan un nivel de eficiencia similar a las comunicaciones de datos seguras utilizando RSA con estenografía.

Hipótesis 2: El uso de computación paralela contribuye en la mejora de la eficiencia de ejecución del algoritmo de seguridad propuesto.

1.5 Objetivos

Esta sección presenta el objetivo general y los objetivos específicos de este trabajo de investigación.

1.5.1 Objetivo general

Diseñar un algoritmo multinivel para comunicaciones seguras de datos basado en criptografía de *lattices*, para llevar a cabo paso de mensajes en conjunto con estenografía.

1.5.2 Objetivos específicos

1. Implementar un marco de evaluación para realizar pruebas de estrés a la implementación del algoritmo propuesto.

2. Comparar la eficiencia del algoritmo utilizando criptografía de *lattices* en conjunto con estenografía basada en DCT en términos de tiempo de ejecución en relación con la eficiencia que proporcionan RSA usando estenografía DCT.

3. Analizar los resultados que se obtienen sobre el algoritmo al hacer uso de operaciones vectoriales sobre la implementación de la criptografía de *lattices*.

4. Contrastar los resultados de la eficiencia del algoritmo propuesto al ejecutarlo de forma secuencial y paralela, a través de una librería que provea programación multihilo.

1.6 Alcance, limitaciones y entregables

En esta sección se detalla cuál es el alcance de este trabajo de investigación. Ello conlleva a anticipar las delimitaciones requeridas para el desarrollo de este proyecto.

1.6.1 Alcance y limitaciones

Al plantear el diseño e implementación de un algoritmo de seguridad multinivel que involucra criptografía de *lattices* y estenografía aplicada sobre imágenes, se deben direccionar los esfuerzos sobre los esquemas y algoritmos que brinden facilidad de acceso, relevancia y eficiencia.

Al tener pocos candidatos selectos a ser estandarizados para ser utilizados en *PQC*, la idea principal será enfocarse en la utilización y modificación de librerías relacionadas a la implementación de dichas propuestas. Lo que se busca es que estas librerías suplan con lo que respecta a la necesidad de encriptar y desencriptar de los mensajes. Estos algoritmos deben de estar basados en el problema de LWE o alguna de sus derivaciones. La librería encargada de suplir esas necesidad es CRYSTALS-Kyber la cual se fundamenta en M-LWE[15].

En relación a estenografía, se procederá a utilizar DCT para ocultar los mensajes encriptados en imágenes. Esto dados los resultados obtenidos por Kumar al comparar el uso y eficiencia de la aplicación de DCT, DWT y LSB. En la cual se concluye que DCT proporciona mejores resultados en términos de eficiencia [22].

Por último, pero no menos importante, como parte de esta investigación también se buscará mejorar el rendimiento del algoritmo propuesto por medio de la utilización de computación paralela, donde tanto la elección de la plataforma como de las tecnologías para la implementación de programación multihilo son de vital importancia. La plataforma que se utilizará para desarrollar esto será una Intel. Con esto se busca explotar la arquitectura selecta por medio del software, la paralelización que brindan las operaciones vectoriales, también conocidas como *Single Instruction Multiple Data (SIMD)*, y la programación multihilo para aprovechar el paralelismo de datos y de tareas que proporciona la librería de Open MP.

1.6.2 Entregables

A continuación se presenta una lista de entregables de la investigación:

1. Marco de pruebas para evaluar rendimientos.
2. Aplicación de mecanismo de criptografía de *lattices*.
3. Empotrado de mensajes por medio del método estenográfico DCT.
4. Implementación del algoritmo de seguridad multinivel.
5. Adaptación de algoritmo de seguridad multinivel con programación multihilo.
6. Mecanismo de seguridad multinivel modificado con operaciones vectoriales.
7. Algoritmo de seguridad multinivel que utilice programación multihilo y operaciones vectoriales.
8. Herramienta para recopilar y analizar resultados de manera automática.

Capítulo 2

Marco teórico

Esta sección muestra el marco teórico de este trabajo de investigación, enfocando la teoría presentada en critografía y estenografía. Se describen los conceptos requeridos de mecanismos de encriptación convencionales y los de criptografía post-cuántica que son la base de esta propuesta. También se cubren diferente métodos estenográficos los cuales en conjunto con los criptográficos serán utilizados para la implementación y corroboración de las hipótesis de la investigación.

2.1 Criptografía

De acuerdo con Easttom en su libro Criptografía Moderna Aplicada, la criptografía se define como la disciplina antigua de asegurar situaciones que se encuentran comprometidas por personajes maliciosos, donde también la llama la ciencia de defender protocolos de potenciales saboteadores. Easttom brinda frases elaboradas para entender el fin de la criptografía, mas esta se encuentra definida, acorde a la RAE como el arte de escribir con clave secreta o de un modo enigmático. Llámese arte, ciencia o disciplina, el fin nunca cambia y este se enfoca en mantener la información protegida.

Desde el inicio de la civilización, cuando la gente empezó a vivir en diferentes grupos o tribus, existió la necesidad de mantener las comunicaciones seguras para así ser más poderoso que sus oponentes. Esta fue la principal razón para que la aparecieron las primeras formas, primitivas, de criptografía. El deseo de mantener comunicaciones secretas es casi tan antiguo como las comunicaciones escritas en sí [18].

El término criptografía ha ido evolucionando con respecto a la seguridad que puedan proveer los mecanismos que califican como tal. Si se traza en el tiempo, se pueden categorizar estos métodos de defensa en 3 categorías:

1. Criptografía clásica.
2. Criptografía moderna o convencional.
3. Criptografía *post quantum*.

2.1.1 Criptografía Clásica

Los cifrados históricos y más comunes son conceptos fundamentales en el estudio de la criptografía, mas estos pueden ser quebrados fácilmente por cualquier computador en la actualidad. Se puede hacer referencia de ellos desde tiempos ancestrales hasta mediados del siglo 19 [18].

Estos corresponden a un conjunto de mecanismos los cuales pueden ser clasificados como métodos de transposición y de sustitución.

Sustitución: Mediante este mecanismo el cifrado consta en sustituir cada letra del texto plano por algún otro símbolo. Si el alfabeto del mensaje es el mismo que el del mensaje cifrado, entonces se le llama monoalfabético. En caso de que eso no se cumpla, se conoce como un cifrado polialfabético [18].

Escítala: En los tiempos modernos, las computadoras facilitan la encriptación de los mensajes, díganse correos, tráfico web y demás. En tiempos ancestrales, se utilizaban ciertos dispositivos para llevar a cargo la tarea y la escítala es uno de los más populares.

Este utiliza un cilindro con cuero enrollado alrededor del mismo. Si se tiene el diámetro correcto para el cilindro, el cuero se posicionaba de tal forma que hacía el mensaje legible. Si no se tenía el cilindro adecuado, e inclusive si el mensaje fuese intersectado por el oponente, solo se obtenía una tira de cuero con símbolos ilegibles. Ver ejemplo en figura (2.1)

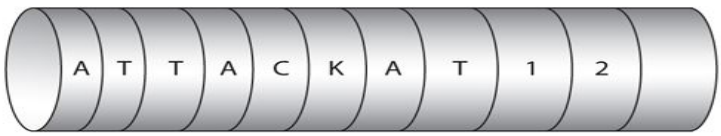


Figura 2.1: Escítala [18]

Transposición: También era común implementar cifrados en los cuales se cambiaba el orden del mensaje o partes del mismo, esto se conoce como cifrados de transposición.

Figura geométrica: Los mecanismos pueden ser tan simples como revertir el texto plano, pero también pueden seguir métodos un poco más complejos como por ejemplo el cifrado de figura geométrica.

El que envía el mensajes escribe el texto plano en columnas y lo mapea a un camino (a una figura) y así crea su texto cifrado. Para ejemplificar, se tiene el texto plano de *"Attack the beach at sunrise"*, el cual se podría alinear en columnas como se ilustra en la figura (2.2).

```
A t t a c k t
h e b e a c h
a t s u n r i s e
```

Figura 2.2: Texto a cifrar posicionado[18]

El emisor decide cuál es el camino necesario en el mensaje para crear un texto cifrado. Al usar el camino ilustrado en la figura 2.3, se obtiene el texto cifrado *"Ahatettbsaeucankcrthise"*. Basta con que el receptor utilice el mismo patrón para decodificar el mensaje.

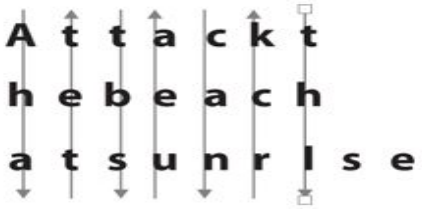


Figura 2.3: Patrón geométrico del cifrado [18]

2.1.2 Criptografía Moderna

Los métodos de la criptografía moderna se basan en distintos mecanismos matemáticos que proporcionan diferentes niveles de seguridad a las comunicaciones [18]. Esta se puede clasificar en la criptografía de llave privada o simétrica y la criptografía de llave pública o asimétrica.

Simétrica: la criptografía simétrica se fundamenta en algoritmos que utilizan la misma llave tanto para encriptar como desencriptar un mensaje.

El proceso es bastante directo y la llave funciona bastante similar al concepto de tener una puerta física, donde la llave funciona para cerrar y para abrir. Esta llave debe de intercambiarse *a priori* para poder llevar a cabo la comunicación. Ver figura (2.4) como referencia.

En este tipo de cifrados se encuentran 2 tipos de bloque, los que hacen uso de redes de Feistel[31] como DES [6] y los que utilizan bloques de sustitución-permutación como AES [7].

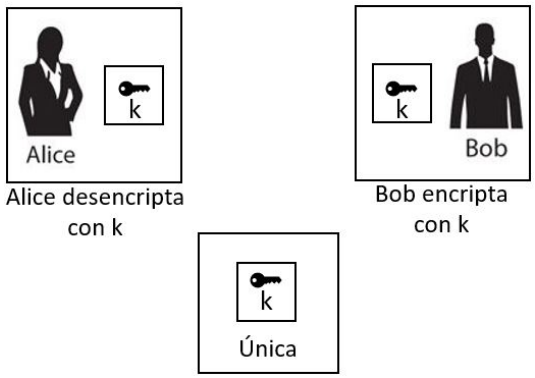


Figura 2.4: Criptografía simétrica

Asimétrica: La criptografía asimétrica utiliza un par de llaves que se generan al mismo tiempo. Una de las llaves se utiliza para encriptar el mensaje y la otra llave para desencriptarlo.

Entre las ventajas de los algoritmos que utilizan criptografía asimétrica se encuentra que no deben efectuar el intercambio de llaves, a diferencia de los algoritmos de clave simétrica. Por lo cual no existe la posibilidad de que las llaves se vean comprometidas durante el intercambio.

En la figura (2.5), se asume que Alice quiere enviarle un mensaje a Bob pero tiene miedo de que Eve pueda escuchar su comunicación. Ahora bien si ellos no poseen criptografía asimétrica deben de tener un proceso de intercambio de llaves en el cual Eve podría tomar ventaja.

Al hacer uso de criptografía asimétrica o de llave pública (PKE) Alice posee la llave pública de Bob con la cual puede encriptar un mensaje y enviarselo a Bob. Eve puede ver los mensajes, mas no tiene cómo descifrarlos. La única manera de leer el mensaje es desencriptándolo al hacer uso de la llave de Bob. En caso de que Bob quisiera responderle a Alice, es tan simple como aplicar el proceso al revés.

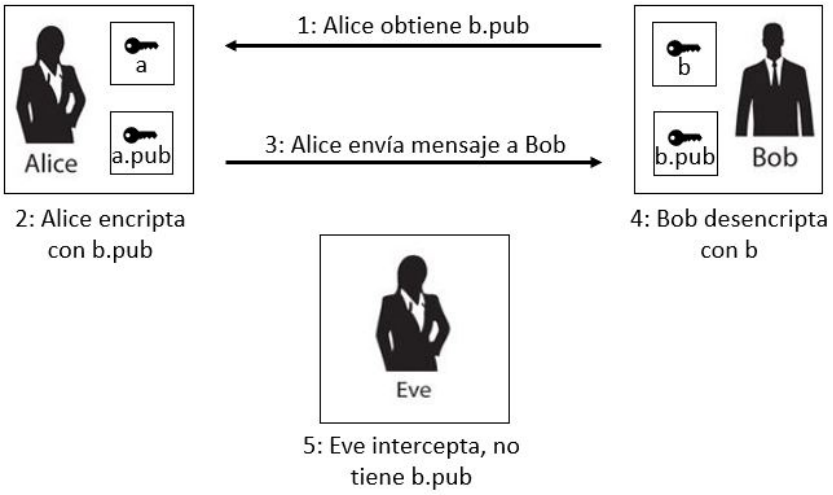


Figura 2.5: Criptografía asimétrica

La criptografía de llave pública se puede dividir en dos tipos de mecanismos: distribución de llaves y secretos, y firmas digitales.

Distribución de llaves y secretos: Este método permite que dos partes intercambien sus llaves y establezcan llaves compartidas sobre un canal no seguro. Este mecanismo es fuertemente utilizado en criptografía simétrica.

Uno de los más conocidos algoritmos en esta categoría es Diffie-Hellman (DH)[13]. Supóngase que Alice y Bob necesitan intercambiar una llave, la Figura 2.6 describe el proceso que se detalla a continuación:

1. Alice y Bob eligen dos enteros, a y b respectivamente y los mantienen secretos.
2. Alice transmite g^a a Bob y Bob transmite g^b a Alice.
3. Alice calcula $(g^b)^a$ y Bob calcula $(g^a)^b$.

La llave común será entonces g^{ab}.

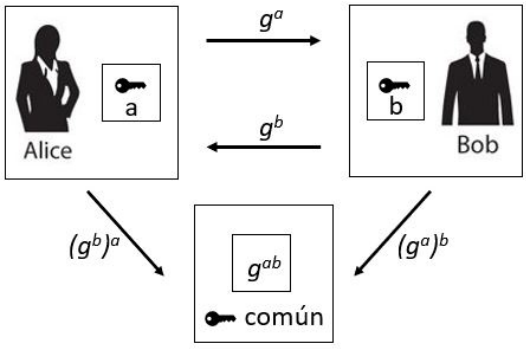


Figura 2.6: Diffie-Hellman

Firmas digitales: Las firmas digitales invierten la criptografía asimétrica, para que esta pueda proteger la integridad. Una firma digital hace uso de la llave privada del remitente para encriptar el mensaje o una porción de este para que cualquiera que posea la llave pública que se encuentra relacionada con la privada del remitente, pueda desencriptar estos mensajes. Una firma digital verifica que el que envía el mensaje es quien este dice ser y es un aspecto esencial en la seguridad del mensaje. Como parte de estos se puede nombrar el Digital Signatura Algorithm (DSA)[9], a continuación en la figura (2.7) se presenta una firma digital generada utilizando DSA.

Uno de los algoritmos más conocidos en llave pública es Rivest-Sharir-Adleman (RSA), al clasificarlo, se puede confirmar que este se encuentra tanto en intercambio de llaves como en firmas digitales. RSA es uno de los algoritmos más importante y más conocidos en la actualidad, tanto así que se encuentra en un sin fin de aplicaciones.

ssh-dss AAAAB3NzaC1kc3MAAACBAIA8J7HHkxe4xYWmLO4kHx61XohepTKRcfhq
RmPB6OgCUXYFDqMzwbUIYwYqvZ4dqxq9dQs34daE5ZTTwFT78kPnKWdxOZa8h
+2LQtSmPTKDyJp1gMNKEOrKiNsbr6ZpNDXn2Lpcnb6UC0ITIMVYshdhRJWmG63
hlu9U1BoRsh2LAAAAFQD6pvXdkt8mCy1inj+XVbrDbJMUNwAAAIAjv7WRj8TcM
nQWq/Fgu+Rt6aP+sfoM2e++CcUp8gUFPRl+jdZKMDzVfyW72tfMrFEPtCKjgp9
m+E++/oBhs4unWmD3O7576ugvTU3IF/m4x+vxTLwrtQdPhqAvC8i9MeomwOqxH
HJ3QeM+9xcsS4YfCMCxZquT/sJtHKlF8D6JogAAAIADmCopJMLBlJWScnFuxJy
Xdg5K3P1wDfppEmbSwYBUUKCFn4GQMz+eZ7AEi9bSdNuow36QQ0oxXMCMkv+F
aAICgRj6C91iWQGJZdvucrVEgScSWAYVYHMXUGh9HMx5znu3gLUWAaOaxyqB4s
SaE4J2I3KlbVX4TPywa7QgP9ZyvA== user@device

Figura 2.7: Firma digital generada con DSA

2.1.3 Criptografía Post Quantum

Afortunadamente este no es el fin del mundo de la criptografía, al contrario, es la respuesta por parte de la comunidad tratando de organizarse para investigar algoritmos existentes y desarrollar nuevos a su vez para contra-restar los efectos expuestos por Shor [43] y Grover[23].

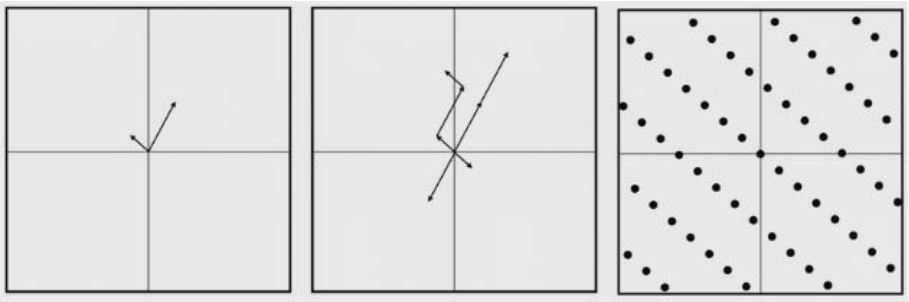
Este cambio de paradigma no es tan sencillo como simplemente escoger algoritmos para suplir los que actualmente se encargan de la "llave pública". Para ello se necesita que los entes estandarizadores, la academia y las organizaciones a nivel mundial inviertan recursos para el diseño, implementación y escogencia de estos mecanismos de defensa.

Como parte de la base teórica que fundamenta esta propuesta, se decidió enfocarse en los cimientos de la criptografía post cuántica que se enfoca o trabaja en referencia a los *lattices*. Una parte importante de las propuestas y elecciones que forman parte del proceso que lidera NIST, se encuentran basados en *lattices*.

***lattices*:** Un lattice es el conjunto de combinaciones lineales de n vectores base. Una buena base está conformada por vectores cortos. Dicho esto, la definición como tal no brinda un entendimiento de la implicación de los *lattices* en las criptografía.

Por ejemplo, RSA se basa en problemas de factorización. Esto no implica que RSA utilice factorización, en cambio, significa que el problema de factorización es la manera de atacar RSA, siendo factorización un problema duro, se dice que RSA es seguro. Este tren de pensamiento es también aplicable a los sistemas de criptografía basados en *lattices*, los *lattices* son estructuras con problemas fuertes, estos sistemas de criptografía se mantendrán seguros mientras los problemas sobre *lattices* permanezcan fuertes [48].

En base a la figura (2.8), un lattice es un espacio vectorial donde todos los números relacionados son enteros. La ilustración de la figura 2.8.a representa los vectores base. La figura 2.8.b puede ser formada al tomar todas las posibles combinaciones lineales



(a) (b) (c)

Figura 2.8: Representación de Lattice [18]

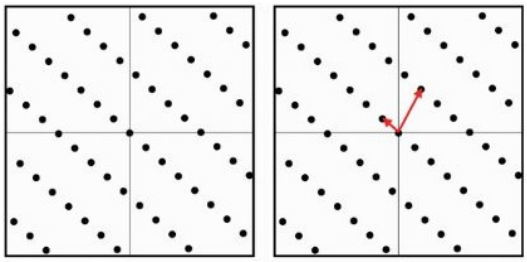
de los vectores base. El lattice resultante en la figura 2.8.c puede ser interpretado como los patrones de puntos que se repiten hacia el infinito.

Problemas duros sobre *lattices*: Existen varios problemas duros los cuales son bien conocidos en el espacio de los *lattices*, para cada uno de estos problemas, se cuenta con un algoritmo para resolverlos. Estos algoritmos son usualmente la mejor manera a la que se ha llegado para su solución, mas no necesariamente implica que sean eficientes o inclusive prácticos. Por lo tanto se dice que el problema es duro hasta que se encuentre una solución eficiente a ellos [48].

Shortest Vector Problem (SVP): El problema de Vector más Pequeño o mejor conocido por sus siglas en inglés *SVP* responde la pregunta:

¿Cuál es el vector, que no sea $\langle 0 \rangle$, más pequeño en su lattice?

Dicho esto, SVP apunta a encontrar el vector más pequeño que no sea $\langle 0 \rangle$ que pueda servir como base del lattice. En la figura (2.9), una ilustración de cómo se puede mapear esto, donde 2.9.a es la representación gráfica de un lattice y 2.9.b es la representación de SVP sobre el mismo lattice.

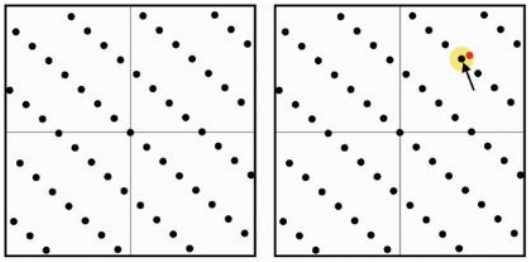


(a) (b)

Figura 2.9: Shortest Vector Problem (SVP)[18]

Closest Vector Problem (CVP): El problema de Vector más Cercano o mejor conocido por sus siglas en inglés *CVP* consta de la siguiente premisa:

Dada una coordenada que no se encuentra en el lattice, encuentre el punto más cercano a la coordenada en el lattice.



(a) (b)

Figura 2.10: Closest Vector Problem (CVP)[18]

CVP apunta a encontrar el punto más cercano dentro del lattice en referencia a un punto que no sea del lattice. La figura 2.10.a representación gráfica de un lattice y 2.10.b es la representación de CVP sobre el mismo lattice.

Learning With Error: En el año 2005, Odev Regev [39] presentó el problema conocido como Aprendizaje con Error, derivado del inglés *Learning With Error (LWE)*, el cual dio paso a varios esquemas y algoritmos importantes en el ámbito de la criptografía. Para ejemplificar de qué trata LWE, las ecuaciones 2.1 y 2.1, las cuales son combinaciones lineales de los enteros x y y, son sencillas de resolver con eliminaciones Gaussianas. De esta manera, se puede rápida y eficientemente obtener los valores de x y y si se cuenta con la cantidad suficiente de ecuaciones.

$$5x + 2y = 27 \tag{2.1}$$

$$2x + 0y = 6 \tag{2.2}$$

Ahora bien, si se añade cierto ruido a las ecuaciones 2.1 y 2.1 el problema se vuelve mucho más complicado. Con este ruido añadido en las ecuaciones 2.3 y 2.4, no es muy difícil encontrar soluciones, se vuelve más complicado a la hora de incrementar el tamaño de los números involucrados y el valor de las incógnitas. Esto en esencia es lo que LWE es, pero en vez de enteros, usualmente se utilizan vectores.

$$5x + 2y = 28 \tag{2.3}$$

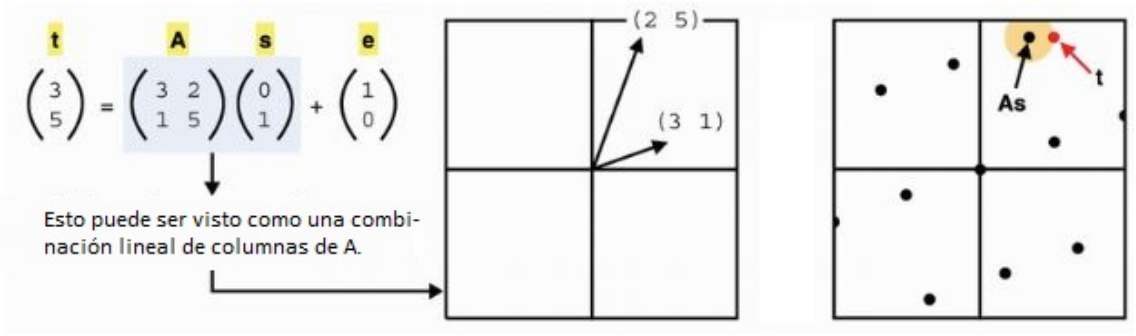
$$2x + 0y = 5 \tag{2.4}$$

La definición formal para LWE es la siguiente:

Dado un vector s con coordenadas módulo algún número grande m, dado un número arbitrario de vectores aleatorios a_i del mismo tamaño y cómputo $a_i + e_i$, donde e_i representa un error pequeño, ¿se puede encontrar el valor de s?

Por ejemplo, si se usa el secreto $s = \langle 3, 6\rangle$ y los vectores aleatoreos $a_0 = \langle 5, 2\rangle$ y $a_1 = \langle 2, 0\rangle$, se vuelve a las ecuaciones con las que se explicó LWE. Los esquemas basados en *lattices* no hacen uso de ellos; con los *lattices* se prueba que la seguridad por ejemplo de SVP, se mantiene dura (alguna definición de dura). La reducción se puede apreciar si se platea el problema como matrices. En la figura 2.11.a, las columnas de A representan las bases del lattice, en el cual un punto t es cercano al punto del lattice As (debido al error). Este resultado se ve gráficamente en la figura 2.11.b.

LWE se dice un problema basado en *lattices* debido a la existencia de una reducción a un problema de *lattices*: el CVP. En otras palabras si se encuentra una solución para CVP, entonces también se puede encontrar una solución para LWE. La transformación lineal se ve representada gráficamente al pasar de la figura 2.11.b a 2.11.c.



(a) (b) (c)

Figura 2.11: Learning With Error (LWE) [18]

Ring - Learning With Error (R-LWE): El problema de Anillos - Aprendizaje Con Error (*R-LWE*) es el mismo que el de LWE aplicado a anillos en polinomios definidos sobre cuerpos infinitos.

Un anillo es un sistema algebraico que consiste de: un conjunto, un elemento identidad, 2 operaciones y el inverso de la primera operación. Las operaciones usualmente son suma y multiplicación, siendo el inverso de la suma, la resta [18].

En relación a los cuerpos, estos también son sistemas algebraicos que consisten de: un elemento identidad para cada operación, 2 operaciones y el inverso de las 2 operaciones. En ese caso, cada cuerpo es un anillo, pero no todo anillo es necesariamente un cuerpo [18].

Se dice que R-LWE es de gran importancia en el ámbito dado que se cree es resistente al algoritmo de Shor, por lo tanto conservaría su dureza en ecosistemas cuánticos. Una de las ventajas de R-LWE sobre LWE es el tamaño de sus llaves, por ejemplo

para obtener uns seguridad de 128 bits con LWE se requiren 49000000 bits, mientras que para R-LWE solamente 7000 bits [36].

Module - Learning With Error (M-LWE): LWE posee problemas de eficiencia y R-LWE mejora ese aspecto. Sin embargo, este cambio trae asunciones de dureza y posible debilitamiento de la seguridad. Module-LWE es un puente entre LWE y R-LWE, donde la seguridad de M-LWE es al menos igual de dura que la de LWE, hablando de *lattices* regulares y *lattices* modulares [30].

2.2 Estenografía

Al igual que la criptografía, la estenografía también busca la prevención de que partes *non gratas* sean capaces de ver cierta información. Mientras la criptografía aplica matemática para hacer los mensajes indescifrables, la estenografía intenta asegurar los datos vía la ocultación de estos en otra media inocua.

La estenografía se puede definir como el arte y ciencia de escribir mensajes ocultos de manera que nadie, además del emisor y el receptor, sospechen que el mensaje existe [18].

La ventaja de la estenografía sobre la criptografía es que los mensajes no atraen la atención a sí mismos. Si nadie está consciente de que el mensaje existe, entonces nadie tratará de descifrarlo. En muchos casos, los mensajes encriptados también son escondidos por medio del uso de estenografía.

Existen diferentes acercamientos para poder esconder mensajes en diferentes tipos de archivo. La elección del método a ser utilizado, en algunos casos, va ligado directamente al formato o plataforma en la que se espera hacer uso de los archivos. A menudo los mensajes se ocultan en imágenes, audio, video, texto plano y cualquier tipo de extensión para desafiar la detección.

A como existe la necesidad de aplicar estenografía en diferentes tipos de datos, existen tipos de estenografía, dentro de los que podemos nombrar los basados en:

- Inyección
- Sustitución
- Transformación

2.2.1 Estenografía basada en inyección

Este tipo de métodos se basa en esconder la información en secciones de los archivos los cuales no son usualmente procesados o expuestos por las aplicaciones. La aplicación de este tipo de métodos afecta el tamaño del archivo resultante [18]. Un ejemplo es el uso de comentarios dentro de archivos de código fuente como lo son los que tienen las

extensiones “*.py”, “*.cpp” o “*.html”, las cuales independientemente de ser compiladas o interpretadas, son descartadas del producto final.

2.2.2 Estenografía basada en sustitución

Literalmente implica sustituir ciertos bits dentro de los datos para esconder los mensajes en los archivos. El archivo resultante no cambia en tamaño [18]. Dentro de este tipo de métodos se encuentra el más sencillo y conocido como lo es el de Bit Menos Significativo.

Least Significant Bit (LSB): La técnica más sencilla utilizada en estenografía es conocida como el Bit Menos Significativo, derivado del inglés *Least Significant Bit (LSB)*. A como su nombre lo dicta, este consta de alterar el LSB, donde se puede ocultar información adicional con mínimas alteraciones en el archivo de origen, logrando modificaciones casi imperceptibles [18].

El cómo se determina el LSB depende del formato del archivo. Por ejemplo si se aplica para un archivo gráfico, cada archivo posee un cierto número de bits por unidad del archivo. En el caso de Windows, son 24 bits por pixel (RGB): 8 para el rojo (R), 8 para el verde (G) y 8 para el azul (B). Al modificar el LSB de esta manera, entonces los cambios no son notables a la vista desnuda. Por ejemplo si se tienen los valor de RGB de (91, 16, 10), se ilustra la diferencia de los colores al modificar el LSB en una imagen en la figura (2.12), la cual es casi imperceptible a simple vista.

(a) (b)

Figura 2.12: R=90 en *a* & R=91 en *b*, casi imperceptible a la vista humana

2.2.3 Estenografía basada en transformación

LSB es la más simple de las técnicas estenográficas, pero a su vez sensible y no robusta a operaciones como el difuminado, recorte, compresión con pérdida y adición de ruido.

En las técnicas basadas en la transformación, primero se transforman la imagen de portada y la imagen secreta en un conjunto de coeficientes de dominio de frecuencia. Los coeficientes de frecuencia significativos de la información secreta son entonces empotrados en algún coeficiente de frecuencia menos importante de la imagen de portada. Por lo tanto, la información oculta es menos visible y más robusta a diferentes operaciones procesamiento

de imágenes. Finalmente, los coeficientes de frecuencia modificados son transformados al inverso para construir una imagen estenográfica [10].

Otra manera de verlo es la siguiente, se transforman los archivos del dominio del tiempo al de las frecuencias. Una imagen en su forma digital es básicamente una colección de píxeles. Los píxeles de los bordes son conocidos por tener una mayor frecuencia, mientras que los que no son del borde poseen una frecuencia baja [18]. Existen diferentes técnicas dentro de esta clasificación, por ejemplo Discrete Cosine Transform y Discrete Wavelet Transform.

Discrete Cosine Transform (DCT): Traducido al español, la Transformada Discreta de Coseno es referencia en la mayoría de la literatura relacionada con estenografía. Esta es aplicada en imágenes, audio y vídeo, por lo que es de vital importancia estar familiarizado con esta técnica.

DCT expresa una secuencia finita de puntos de dato en términos de suma de funciones de coseno oscilando a diferentes frecuencias. Expresa una función o señal en términos de suma de sinusoides con diferentes frecuencias y amplitudes. Un sinusoide es una curva similar a las funciones de seno, pero posiblemente corridas en fase, periodo, amplitud o cualquier combinación de ellos.

Los coeficientes de DCT son utilizados, por ejemplo, en compresión JPEG. Separa las imágenes en partes de importancia distinta. Transforma la señal o imagen en componentes de alta, mediana y baja frecuencia [18]. La Figura 2.13 presenta una visualización en 2 dimensiones de la aplicación de DCT.

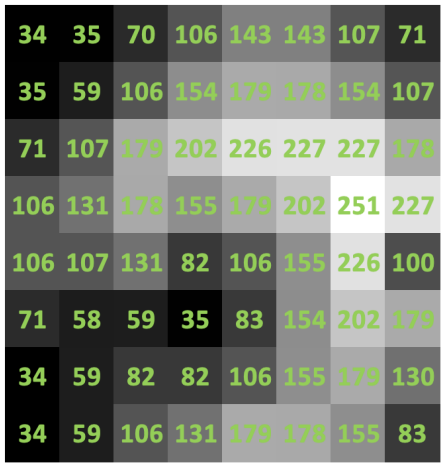


Figura 2.13: DCT en 2D. Tomada de https://shorturl.at/dgkpQ

Discrete Wavelet Transform (DWT): La Transformada de Ondículas Discretas [1] es una manera de transformar del dominio espacial al de frecuencias. Se utiliza en compresión para JPEG el cual es un formato muy popular. Las ondículas son básicamente funciones que se integran a ondas cero por debajo y por encima del

[1] Derivado del inglés Discrete Wavelet Transform.

eje x. Para el procesamiento de señales e imágenes, las ondículas se utilizan como función básica, como senos y cosenos en la transformada de Fourier [10]. En la Figura 2.14 se aprecia el proceso de descomposición a 2 dimensiones en DWT.

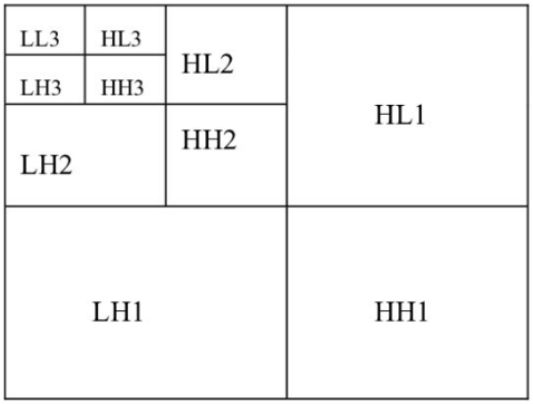


Figura 2.14: Descomposición 2D en DWT [24]

Capítulo 3

Metodología

En este capítulo se exponen las fases de la metodología de investigación y las actividades que corresponden con cada una de ellas. Además se presenta la propuesta de los experimentos para validar las hipótesis.

3.1 Descripción de la metodología

La metodología utilizada en esta investigación es el modelo Investigación de Acción, el cual se basa en una serie de iteraciones para resolver un problema en específico, en donde cada ciclo tiene por objetivo refinar la solución [49]. En la tabla 3.1 se observa que la metodología consiste en 5 fases (plan/revisión del plan, diagnóstico, tomar acción, evaluar, analizar hallazgos). Cuando se completan las fases se realiza un nuevo ciclo del proceso que inicia con la revisión del plan. Esta investigación corresponde al primer ciclo de una serie de iteraciones.

La investigación inicia con la fase **Plan/Revisión del plan** que corresponde al planteamiento del problema, la definición de objetivos y la limitación el alcance del proyecto. Luego continuará con la fase de **Diagnóstico**, en la cual se realizarán la revisión y clasificación de la literatura, se identificarán los métodos de encriptación de *lattices*, su estado, aplicaciones e investigación hecha a su alrededor en conjunto con mecanismos estenográficos.

La siguiente fase, **Tomar acción** para el futuro método de seguridad multinivel, permitirá definir la arquitectura, el diseño y la implementación del mecanismo propuesto para la encriptación y ocultación de los datos. Mientras que en la fase **Evaluar** se diseñarán e implementarán los experimentos para evaluar los métodos propuestos. La fase final de esta investigación corresponde a **Analizar hallazgos**, la cual tiene por fin realizar el análisis de los resultados obtenidos en las fases previas y realizar las conclusiones a partir de los hallazgos.

Fases de la metodología	Actividades
Plan/Revisión del plan	Estado del arte.
	Planteamiento del problema.
	Definición de Hipótesis y objetivos.
	Definición de alcance y limitaciones.
Diagnóstico	Clasificación de la literatura.
	Identificación de métodos y su estado.
	Análisis y discusión de la literatura.
	Revisión detallada de la literatura afín.
Tomar acción	Definición de herramientas.
	Especificación de arquitectura.
	Diseño e implementación de los métodos.
Evaluar	Caso de estudio.
	Diseño de experimentos.
	Aplicación de experimentos.
Analizar Hallazgos	Análisis de resultados.
	Conclusiones.

Tabla 3.1: Propuesta de actividades para cada fase de la metodología de Investigación de Acción.

3.2 Planteamiento de los experimentos

Esta sección detalla un conjunto de experimentos que se realizaran para probar las hipótesis (ver Sección 1.4). La propuesta se basa en el uso de un algoritmo de seguridad multinivel post-cuántico basado en *lattices*, esteganografía y computación paralela. El método de esteganografía se utilizará como mecanismo de seguridad de segundo nivel para empotrar los datos en imágenes y el uso de computación paralela se usará para efectuar la encriptación y el empotrado de forma eficiente.

El algoritmo se denominará *Shinobice*, un nombre compuesto por las palabras *shinobi*[1] y lattice. La selección del nombre es una analogía de la palabra *shinobi* con escabullirse (pasar desapercibido, estenografía) y con secretismos (criptografía), y los *lattices*, que son parte esencial de la propuesta.

La Tabla 3.2 muestra la correspondencia entre los objetivos (ver Sección 1.5), hipótesis y experimentos que se realizarán para evaluar *Shinobice*. El detalle del planteamiento de cada experimento se presenta en la siguientes secciones.

[1] *Shinobi* o *ninja* es una palabra japonesa la cual se utiliza para describir a grupos de mercenarios que se empleaban en épocas de guerra los cuales dominaban el *ninjutsu*, donde *nin* significa escabullirse y *jutsu* se traduce como arte o destreza.

Objetivos	Hipótesis	Experimento	Sección
1 y 2	Hipótesis 1	Experimento 1	3.2.1
1 y 4	Hipótesis 2	Experimento 2	3.2.2
1 y 3	Hipótesis 2	Experimento 3	3.2.3
1, 3 y 4	Hipótesis 2	Experimento 4	3.2.4

Tabla 3.2: Experimentos y metas afines

3.2.1 Comparar la ejecución secuencial de Shinobice y RSA

Objetivo: Comparar la eficiencia del algoritmo utilizando criptografía de *lattices* en conjunto con estenografía basada en DCT, en términos de tiempo de ejecución, en relación con la eficiencia que proporciona la criptografía que proporciona RSA en conjunto con el método estenográfico DCT.

Descripción: Este experimento consiste en la ejecución de *Shinobice* y el método de seguridad multinivel que utiliza RSA con DCT. Este tiene por fin recopilar los datos relacionados a la eficiencia de las ejecuciones para contrastarlos. Este contempla la ejecución de los métodos con las mismas configuraciones y condiciones deben, pero con diferentes mecanismos de encriptación. A continuación se presentan los pasos requeridos para efectuar este experimento:

1. Implementar *Shinobice*.
2. Reemplazar del método de encriptación de *lattices* por RSA.
3. Medir la eficiencia de la ejecución del método que utililiza *lattices*.
4. Cuantificar la eficiencia de la solución que usa RSA cuando se ejecuta el mismo número de veces que en el caso anterior.
5. Contrastar los resultados obtenidos de ambas soluciones.

Este experimento tiene por fin comprobar que si la solución que usa *lattices* proporciona mejores resultados, en relación a la eficiencia, que la solución que utiliza RSA.

3.2.2 Comparar la eficiencia entre las ejecuciones secuenciales y paralelas basadas en multihilo de Shinobice

Objetivo: Contrastar la eficiencia de la ejecución secuencial y paralela de Shinobice con programación multihilo.

Descripción: Los resultados obtenidos en el experimento 3.2.1 con Shinobice y RSA se tomarán como referencia para la realización de la comparación de la eficiencia entre las ejecuciones secuenciales y paralelas con multihilo. Este experimento consiste en modificar el algoritmo propuesto para contar con dos implementaciones: la

secuencial y la paralela (*Shinobice* modificado) que explota el uso de programación multihilo. A continuación se detallan los pasos que serán requeridos para realizar esta comparación:

1. Modificar la solución del algoritmo para contar con una propuesta que utilice la paralelización multihilo, a nivel de datos y tareas.
2. Medir la eficiencia de la solución secuencial mediante su ejecución en múltiples ocasiones para obtener un promedio de estas.
3. Cuantificar la eficiencia de la solución paralela al ejecutarla la misma cantidad de veces que el algoritmo secuencial.
4. Comparar los resultados de los promedios obtenidos con la ejecución de las soluciones secuencial y paralela con multihilos.

Este experimento utilizará diferentes escenarios para realizar las pruebas de ejecución.

3.2.3 Comparar las ejecuciones secuenciales y paralelas con operaciones vectoriales de Shinobice

Objetivo: Analizar los resultados que se obtienen de la ejecución del algoritmo al transformar la propuesta secuencial con el uso de operaciones operaciones vectoriales[2].

Descripción: Este experimento tiene por fin comparar la ejecución de la implementación secuencial de Shinobice con una versión del mismo algoritmo usando operaciones vectoriales. A continuación se detallan los pasos requeridos para efectuar las pruebas:

1. Diseñar e implementar una versión paralela de Shinobice con el uso de vectorización.
2. Medir la solución secuencial en términos de eficiencia al ejecutarla múltiples veces para obtener un promedio.
3. Cuantificar la eficiencia de la solución basada en paralelismo con instrucciones vectoriales con la secuencia al ejecutarla la misma cantidad de veces y promediar sus resultados.
4. Comparar los resultados obtenidos de ambas soluciones.

Este experimento busca definir los escenarios en los cuales es más beneficioso utilizar el algoritmo sin alteraciones o la solución que hace uso de instrucciones vectoriales.

[2]Operaciones vectoriales, también conocidas como *SIMD* el cual deriva de las siglas en inglés *Single Instruction Multiple Data.*

3.2.4 Comparar la ejecución secuencial, paralela con multihilos y paralela con operaciones vectoriales de Shinobice

Objetivo: Contrastar los resultados de la eficiencia del algoritmo propuesto al ejecutarlo de forma secuencial y paralela, utilizando operaciones vectoriales y programación multihilo.

Descripción: Este experimento usa los resultados obtenidos en los experimentos anteriores con las ejecuciones secuenciales, paralelas con multihilos y paralela con instrucciones vectoriales. El fin de este experimento es hacer usar esos resultados para compararlos y recomendar la solución más eficiente.

1. Obtener los resultados de los experimentos 3.2.2 y 3.2.3 y analizar los beneficios de cada uno para aplicarlos a la realización de una solución paralela.
2. Estudiar la eficiencia de la solución secuencial realizada en el experimento 3.2.1 al ejecutarla repetidas veces y promediar sus resultados.
3. Evaluar la eficiencia de las pruebas efectuadas en el experimento 3.2.2 que hace uso paralelización multihilo. Se deben efectuar la misma cantidad de iteraciones que las que efectuadas en la evaluación de la solución secuencial.
4. Cuantificar la eficiencia de la implementación con operaciones vectoriales, efectuadas en el experimento 3.2.3, al ejecutarla el mismo número de veces que la implementación secuencial.
5. Medir el rendimiento de la implementación que contempla el uso de operaciones operaciones vectoriales junto a paralelismo de datos y tareas (multihilo). Realizar la misma cantidad de ejecuciones que en la secuencial para promediar los resultados.
6. Comparar y analizar los resultados obtenidos en los diferentes experimentos.

Este experimento tiene por fin verificar, mediante diferentes escenarios, que el uso de computación paralela contribuye a mejorar la eficiencia de la ejecución del algoritmo propuesto.

Capítulo 4

Calendario propuesto

En este capítulo se presenta la linea de tiempo de todas las tareas a desarrollar durante los tres seminarios de investigación. A continuación se detallará cada una de las etapas y las tareas que incluyen desde la revisión de la literatura hecha para este trabajo hasta llegar al documento final.

4.1 Detalle de tareas

La distribución de las tareas se presenta mediante un calendario detallado, la Figura 4.1 determina en detalle la repartición de las tareas a lo largo de los seminarios. Las tareas propuestas listan las diferentes actividades requeridas para completar este proyecto de investigación.

Como parte fundamental de este proyecto de investigación, se inició con la propuesta de investigación, la cual contempla desde la revisión de la literatura hasta la presentación de la propuesta.

Con respecto al desarrollo, para su confección se toman en cuenta las configuraciones iniciales y el diseño e implementación de lo listado a continuación: marco de pruebas, modelo de seguridad multinivel, modelo de seguridad multinivel con programación multihilo, modelo de seguridad multinivel con vectorización, y modelo de seguridad multinivel con programación multihilo y vectorización.

En relación al tramo final, centrado en la elaboración de la tesis, se detallan las secciones requeridas para completar el trabajo de investigación.

Para la confección de este calendario se utilizaron fechas estimadas para su realización, las cuales se encuentran previstas para finalizar el 2 de junio del año 2024. Para ver el calendario en detalle, este se puede acceder en la página de GitHub de este proyecto.

Task Name	Duration	Start	Finish
Propuesta de tesis	**311 days**	**Mon 7/25/22**	**Wed 5/31/23**
Desarrollo de la investigación	**114 days**	**Mon 7/24/23**	**Tue 11/14/23**
Configuración Inicial del proyecto	**2 days**	**Mon 7/24/23**	**Tue 7/25/23**
Marco de pruebas	**3 days**	**Wed 7/26/23**	**Fri 7/28/23**
Modelo de seguridad multinivel	**9 days**	**Sat 7/29/23**	**Sun 8/6/23**
Diseño e implementación	**7 days**	**Sat 7/29/23**	**Fri 8/4/23**
Pruebas unitarias	2 days	Sat 8/5/23	Sun 8/6/23
Modelo de seguridad multinivel vectorizado	**44 days**	**Mon 8/7/23**	**Tue 9/19/23**
Diseño e implementación	**40 days**	**Mon 8/7/23**	**Fri 9/15/23**
Pruebas unitarias	8 days	Tue 9/12/23	Tue 9/19/23
Modelo de seguridad multinivel multihilo	**44 days**	**Wed 9/20/23**	**Thu 11/2/23**
Diseño e implementación	**40 days**	**Wed 9/20/23**	**Sun 10/29/23**
Pruebas unitarias	8 days	Thu 10/26/23	Thu 11/2/23
Modelo de seguridad multinivel multihilo y vectorizado	**12 days**	**Fri 11/3/23**	**Tue 11/14/23**
Diseño e implementación	**8 days**	**Fri 11/3/23**	**Fri 11/10/23**
Pruebas Unitarias	4 days	Sat 11/11/23	Tue 11/14/23
Tesis	**119 days**	**Mon 2/5/24**	**Sun 6/2/24**
Introducción	17 days	Mon 2/5/24	Wed 2/21/24
Marco teórico	12 days	Thu 2/22/24	Mon 3/4/24
Diseño	24 days	Tue 3/5/24	Thu 3/28/24
Desarrollo	35 days	Fri 3/29/24	Thu 5/2/24
Resultados	17 days	Fri 5/3/24	Sun 5/19/24
Conclusiones	14 days	Mon 5/20/24	Sun 6/2/24

Figura 4.1: Calendario propuesto del 25 de julio del 2022 al 2 de junio del 2024

Bibliografía

[1] NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy — nsa.gov. https://shorturl.at/EHJV2. [Accessed 04-May-2023].

[2] Post-Quantum Cryptography Standardization - Post-Quantum Cryptography — CSRC — CSRC — csrc.nist.gov. https://shorturl.at/PQZ68. [Accessed 13-May-2023].

[3] Round 3 Submissions - Post-Quantum Cryptography — CSRC — CSRC — csrc.nist.gov. https://shorturl.at/pHJZ4. [Accessed 21-Sep-2022].

[4] Round 4 Submissions - Post-Quantum Cryptography — CSRC — CSRC — csrc.nist.gov. https://shorturl.at/ijoxU. [Accessed 21-Sep-2022].

[5] Selected Algorithms 2022 - Post-Quantum Cryptography — CSRC — CSRC — csrc.nist.gov. https://shorturl.at/hLQR4. [Accessed 21-Sep-2022].

[6] Federal information processing standards publication: data encryption standard (DES). Technical report, 1993. URL https://doi.org/10.6028%2Fnist.fips.46-2.

[7] Advanced encryption standard (AES). Technical report, November 2001. URL https://doi.org/10.6028/nist.fips.197.

[8] Ieee standard specification for public key cryptographic techniques based on hard problems over lattices. *IEEE Std 1363.1-2008*, pages 1–81, 2009. URL https://ieeexplore.ieee.org/document/4800404.

[9] Digital signature standard (DSS). Technical report, July 2013. URL https://doi.org/10.6028/nist.fips.186-4.

[10] Ahmed A. Abdelwahab and Lobna A. Hassaan. A discrete wavelet transform based technique for image data hiding. In *2008 National Radio Science Conference*, pages 1–9, 2008. URL https://ieeexplore.ieee.org/document/4542319.

[11] Dorit Aharonov and Oded Regev. Lattice problems in np conp. *J. ACM*, 52(5):749–765, sep 2005. URL https://doi.org/10.1145/1089023.1089025.

[12] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*,

STOC '96, page 99–108, New York, NY, USA, 1996. Association for Computing Machinery. URL https://doi.org/10.1145/237814.237838.

[13] Elaine Barker, Lily Chen, Allen Roginsky, Apostol Vassilev, and Richard Davis. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. Technical report, apr 2018. URL https://shorturl.at/ghMYZ.

[14] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults. In Walter Fumy, editor, *Advances in Cryptology — EUROCRYPT '97*, pages 37–51, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg. URL https://doi.org/10.1007/3-540-69053-0.

[15] Joppe Bos, Leo Ducas, Eike Kiltz, T Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle. Crystals - kyber: A cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367, 2018. URL https://shorturl.at/aoHO8.

[16] Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2018*, pages 282–305, Cham, 2018. Springer International Publishing. URL https://shorturl.at/CKMQ4.

[17] Elena Dubrova, Kalle Ngo, and Joel Gärtner. Breaking a fifth-order masked implementation of crystals-kyber by copy-paste. Cryptology ePrint Archive, Paper 2022/1713, 2022. URL https://eprint.iacr.org/2022/1713.

[18] Chuck Easttom. *Modern cryptography: Applied mathematics for encryption and information security*. McGraw-Hill Education, Columbus, OH, October 2015. URL https://shorturl.at/fqEJM.

[19] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. 2020. URL https://falcon-sign.info/falcon.pdf.

[20] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery. URL https://doi.org/10.1145/1536414.1536440.

[21] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Paper 2007/432, 2007. URL https://eprint.iacr.org/2007/432.

[22] Stuti Goel, Arun Kumar Rana, and Manpreet Kaur. A review of comparison techniques of image steganography. *Global journal of computer science and technology*, 13:41–48, 2013. URL https://shorturl.at/mrBC0.

[23] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery. URL https://doi.org/10.1145/237814.237866.

[24] Baisa L Gunjal and Suresh N Mali. Strongly robust and highly secured DWT-SVD based color image watermarking: Embedding data in all y, u, V color spaces. *Int. J. Inf. Technol. Comput. Sci.*, 4(3):1–7, April 2012. URL http://www.mecs-press.org/ijitcs/ijitcs-v4-n3/v4n3-1.html.

[25] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, pages 267–288, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg. URL https://link.springer.com/chapter/10.1007/BFb0054868.

[26] Yiming Huang, Zhongkui Lei, Zhufu Song, Yueru Guo, and Yihang Li. A video steganography scheme based on post-quantum cryptography. In *2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE)*, pages 83–87, 2021. URL https://ieeexplore.ieee.org/document/9404087.

[27] Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. Ntru-hrss-kem - submission to the nist post-quantum cryptography project, 2017. URL https://shorturl.at/JLT69.

[28] Julian Jang-Jaccard and Surya Nepal. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5):973–993, 2014. URL https://www.sciencedirect.com/science/article/pii/S0022000014000178. Special Issue on Dependable and Secure Computing.

[29] Febrian Kurniawan and Gandeva Bayu Satrya. Future identity card using lattice-based cryptography and steganography. In Sanjiv K. Bhatia, Shailesh Tiwari, Su Ruidan, Munesh Chandra Trivedi, and K. K. Mishra, editors, *Advances in Computer, Communication and Computational Sciences*, pages 45–56, Singapore, 2021. Springer Singapore. URL https://doi.org/10.1007/978-981-15-4409-5_4.

[30] Adeline Langlois and Damien Stehle. Worst-case to average-case reductions for module lattices. Cryptology ePrint Archive, Paper 2012/090, 2012. URL https://eprint.iacr.org/2012/090.

[31] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988. URL https://doi.org/10.1137/0217022.

[32] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming*, pages 144–155, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. URL https://shorturl.at/hlowB.

[33] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, 9(3), 2018. URL `https://shorturl.at/efjl0`.

[34] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. The Springer International Series in Engineering and Computer Science. Springer US, 2012. URL `https://doi.org/10.1007/978-1-4615-0897-7`.

[35] Daniele Micciancio and Oded Regev. *Lattice-based Cryptography*, pages 147–191. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. URL `https://doi.org/10.1007/978-3-540-88702-7_5`.

[36] Marius Iulian Mihailescu and Stefania Loredana Nita. Ring learning with errors cryptography. In *Pro Cryptography and Cryptanalysis with C++20*, pages 287–301. Apress, Berkeley, CA, 2021. URL `https://doi.org/10.1007/978-1-4842-6586-4`.

[37] S. M. Naser. Cryptography: From the ancient history to now, it's applications and a new complete numerical model,. *International Journal of Mathematics and Statistics Studies*, 9(3):11–30, aug 2021. URL `https://shorturl.at/iQTY4`.

[38] Oded Regev. Lattice-based cryptography. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, pages 131–141, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. URL `https://link.springer.com/chapter/10.1007/11818175_8`.

[39] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), sep 2009. URL `https://doi.org/10.1145/1568318.1568324`.

[40] Sayeed Z. Sajal, Israt Jahan, and Kendall E. Nygard. A survey on cyber security threats and challenges in modern society. In *2019 IEEE International Conference on Electro Information Technology (EIT)*, pages 525–528, May 2019. URL `https://ieeexplore.ieee.org/document/8833829`.

[41] Eike Kiltz Tancrède Lepoint Vadim Lyubashevsky Peter Schwabe Gregor Seiler Shi Bai, Léo Ducas and Damien Stehlé. Crystals-dilithium algorithm specifications and supporting documentation (version 3.1). https://pq-crystals.org/dilithium/, feb 2021. URL `https://shorturl.at/gjHX6`.

[42] Mohammad Hadi Shirafkan, Ehsan Akhtarkavan, and Javad Vahidi. A image steganography scheme based on discrete wavelet transform using lattice vector quantization and reed-solomon encoding. In *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, pages 177–182, 2015. URL `https://ieeexplore.ieee.org/document/7436041`.

[43] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, page 124–134, USA, 1994. IEEE Computer Society. URL `https://doi.org/10.1109/SFCS.1994.365700`.

[44] Ravi Srihitha, Yadlapalli Sai Harshini, and V. M. Manikandan. An adaptive multi-level block-wise encryption based reversible data hiding scheme. In *2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS)*, pages 186–191, Nov 2020. URL https://ieeexplore.ieee.org/document/9342695.

[45] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer Abdulsattar Lafta, Mohammed Mahdi Hashim, and Hassanain Mahdi Alzuabidi. Combination of steganography and cryptography: A short survey. *IOP Conference Series: Materials Science and Engineering*, 518(5):052003, may 2019. URL https://shorturl.at/ejnB9.

[46] Ingrid Verbauwhede. Pq crypto contribution. Intel Crypto Frontiers Research Workshop, 2022.

[47] Luis von Ahn and Nicholas J. Hopper. Public-key steganography. In Christian Cachin and Jan L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, pages 323–341, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg. URL https://doi.org/10.1007/978-3-540-24676-3_20.

[48] David Wong. *Real-World Cryptography*. Manning Publications, New York, NY, October 2021. URL https://shorturl.at/txHJ5.

[49] Adrian Zbiciak and Tymon Markiewicz. A new extraordinary means of appeal in the polish criminal procedure: the basic principles of a fair trial and a complaint against a cassatory judgment. *Access to Justice in Eastern Europe*, 6(2):1–18, March 2023. URL https://doi.org/10.33327/AJEE-18-6.2-a000209.