ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO INTRODUCTORIO A LA CRIPTOGRAFÍA CUÁNTICA

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN.

ANDRÉS RONALD LEMA ANDRANGO

andres.lema@epn.edu.ec

DIRECTOR: WILLIAM FERNANDO FLORES CIFUENTES

fernando.flores@epn.edu.ec

QUITO, Septiembre 2022

CERTIFICACIONES

Yo, ANDRÉS RONALD LEMA ANDRANGO declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

ANDRÉS RONALD LEMA ANDRANGO

Certifico que el presente trabajo de integración curricular fue desarrollado por ANDRÉS RONALD LEMA ANDRANGO, bajo mi supervisión.

FERNANDO FLORES CIFUENTES
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

ANDRÉS RONALD LEMA ANDRANGO

FERNANDO FLORES CIFUENTES

DEDICATORIA

Dedico este trabajo principalmente a mis padres Arturo Lema y Magdalena Andrango que siempre han estado conmigo en las buenas y en las malas. A mi hermana Érica que cuento con su apoyo día a día y a mi hermana Belén que lamentablemente ya no está con nosotros físicamente, pero la recordaremos siempre; y a todas aquellas personas que de una u otra manera ha contribuido a que este objetivo se cumpla.

AGRADECIMIENTO

Agradezco principalmente a mi familia por todo el apoyo brindado en este largo camino, agradezco a mi director el Ing. Fernando Flores por su paciencia y dedicación en la realización de este documento.

Finalmente hago extenso mi agradecimiento a todos aquellos maestros de la Escuela Politécnica Nacional que han logrado inculcarme sus sólidos conocimientos para ser un profesional de altura.

ÍNDICE DE CONTENIDO

RESUMEN

PALABRAS CLAVE: criptografía, información, hardware, software, clave pública, clave privada, algoritmo.

La criptografía es un método que nos permite proteger la información por medio de diferentes técnicas o algoritmos matemáticos que se han ido perfeccionando o modificando con el transcurrir del tiempo, y nos han permitido manejar la información de manera confidencial.

En la actualidad la seguridad de los sistemas informáticos se ha visto vulnerada con más frecuencia y cada vez con más facilidad, una de las causas de esto se debe al incremento de sistemas informáticos desarrollados para estos propósitos. El avance tecnológico tanto como en hardware y software de diferentes dispositivos permiten que cada vez sea más fácil vulnerar la seguridad de la información basada en la criptografía tradicional.

La criptografía tradicional utiliza claves públicas las cuales están basadas en algoritmos matemáticos que nos permiten dar un cierto nivel de seguridad a la información, a diferencia de la criptografía cuántica; que tiene como bases a la mecánica cuántica, y utiliza claves privadas que por medio de la luz se distribuyen y se logra enviar información por vías adecuadas como la fibra óptica.

Por medio del estudio de las bases fundamentales de la criptografía cuántica y algunos modelos utilizados en la transmisión de información por medio de luz se plantea determinar las ventajas de la criptografía cuántica con respecto a la criptografía tradicional.

ABSTRACT

KEYWORDS: cryptography, information, hardware, software, public key, private key, algorithm.

Cryptography is a method that allows us to protect information by means of different mathematical techniques or algorithms that have been improved or modified over time, and have allowed us to handle information confidentially.

At present, the security of computer systems has been violated more frequently and with increasing ease, one of the causes of this is due to the increase in computer systems developed for these purposes. Technological advances, as well as in hardware and software of different devices, make it easier and easier to violate the security of information based on traditional cryptography.

Traditional cryptography uses public keys which are based on mathematical algorithms that allow us to give a certain level of security to information, unlike quantum cryptography; which is based on quantum mechanics, and uses private keys that are distributed by means of light and it is possible to send information through appropriate channels such as fiber optics.

Through the study of the fundamental bases of quantum cryptography and some models used in the transmission of information by means of light, it is proposed to determine the advantages of quantum cryptography with respect to traditional cryptography.

1 INTRODUCCIÓN

En la actualidad los ataques informáticos se han convertido en uno de los problemas más comunes en el ámbito tecnológico, el objetivo de estos ataques es vulnerar cualquier tipo de seguridad informática y obtener información, ya sea información personal o información empresarial de relevancia. Por esta razón se plantea hacer un breve estudio de la criptografía cuántica, que haciendo uso de los conceptos fundamentales de la mecánica cuántica introduce nuevas ideas a ser analizadas con respecto a la criptografía tradicional. Se plantea hacer una comparación entre la criptografía tradicional y la criptografía cuántica de tal forma que se pueda determinar cuál de estas dos formas de criptografía nos provee mejores herramientas para poder salvaguardar la información.

En este documento se mencionan las bases y fundamentos teóricos de la criptografía cuántica de tal forma que se puede crear una idea general de cuál es su funcionamiento; además de eso se hace un especial énfasis en temas relevantes como las principales fuentes de fotones y los diferentes canales cuánticos utilizados en esta tecnología.

Como punto de partida y para tener un panorama más claro es necesario conocer cómo fue que la criptografía cuántica dio sus primeros pasos, por lo tanto, en este documento se realiza un resumen en forma de reseña histórica de la criptografía tradicional, pasando por la criptografía moderna y finalmente llegando a la criptografía cuántica.

Se toma como punto de partida los primeros indicios de la criptografía, conocida también como criptografía clásica; se menciona el desarrollo de la criptografía moderna hasta culminar finalmente con el desarrollo de la criptografía cuántica.

En orden cronológico se mencionan eventos y personajes estrechamente relacionados con el tema, así, por ejemplo, quien fue el primer personaje que se atrevió a utilizar los conceptos cuánticos y principios de la mecánica cuántica con la finalidad de transmitir información; como se fueron desarrollando y como se fueron mejorando los métodos para transmitir fotones de luz por un medio guiado y por un medio no guiado.

Se abordan conceptos de la mecánica cuántica como el principio de incertidumbre de Heisenberg y la superposición de estados que son temas en los cuales la criptografía

cuántica tiene su raíz; así también se menciona cómo funcionan y que papel cumplen en los diferentes procesos que se llevan a cabo para poder enviar información de un punto a otro por medio de fotones de luz con la utilización de este método criptográfico.

Este documento está orientado principalmente a dar a conocer de forma breve y resumida las principales fuentes de fotones utilizadas en la criptografía cuántica; así mismo se hace referencia a los canales que se pueden utilizar para transportar dichos fotones de luz con el objetivo primordial de salvaguardar la información encriptada.

Finalmente se plantea realiza una comparación entre la criptografía moderna y la criptografía cuántica en diversos ámbitos partiendo desde las bases de cada una de ellas y concluyendo con sus resultados como método criptográfico.

Adicionalmente se propone mencionar rápidamente aspectos derivados de este documento que nacen como interrogantes en desarrollo de los principales temas abordados y que van más allá de lo mencionado en este texto.

Se llegan a analizar de forma muy breve los dispositivos cuánticos que permiten que esta nueva criptografía sea una realidad, así mismos temas derivados como el costo que implica implementar esta nueva forma de criptografía frente a los costos de la criptografía que todos conocen; ¿es realmente necesario implementarla y hacer uso de esta nueva base científica para salvaguardas nuestra información? o todavía la criptografía moderna tiene las herramientas para brindar seguridad a nuestra información.

Por lo tanto, se brinda una opinión desde el punto de vista del autor de este documento, tratando de ser lo más imparcial posible de tal forma que se puedan obtener resultados valiosos y principalmente se puedan conseguir conclusiones relevantes de este tema.

1.1 Objetivo General

Comparar la criptografía tradicional con la criptografía cuántica mediante conceptos generales de funcionamiento para determinar cuál de estas brinda mayor seguridad a la información.

1.2 Objetivos Específicos

1. Desarrollar una idea general clara del funcionamiento de la criptografía cuántica mediante los conceptos básicos de la mecánica cuántica.
2. Conocer los componentes que la criptografía cuántica necesita para funcionar, así como las fuentes encargadas de generar fotones de luz y los diferentes canales que se manejan para el transporte de la información.
3. Obtener una comparación que nos permita resaltar las ventajas y desventajas de cada criptografía en temas secundarios con la finalidad de determinar cuál es la más conveniente en sentido de seguridad informática.

1.3 Alcance

Se plantea realizar una comparativa entre la criptografía tradicional y la criptografía cuántica basada inicialmente en aspectos fundamentales como las fuentes de fotones de luz y los canales que sirven para transportar estos fotones. Adicionalmente se consideran también de forma muy resumida, y en forma de opinión, algunos aspectos derivados de estos temas como la utilización de dispositivos cuánticos y costos que conlleva esta criptografía; de tal manera que se pueda obtener una mejor visión de cuál de las dos criptografías permiten que información se encuentre mejor protegida.

Se deja marcado el precedente de un par de temas derivados, como el costo y los dispositivos que se utilizan en la criptografía cuántica, para que en un futuro otras personas con los mismos intereses puedan tomar como base este escrito y por ejemplo orienten su estudio al costo–beneficio de estas dos criptografías.

Mediante el breve desarrollo de varios de los conceptos más importantes que se manejan en la mecánica cuántica y por consiguiente en la criptografía cuántica se intenta conseguir las herramientas necesarias para poder evidenciar que tipo de criptografía nos brinda más ventajas ante los diferentes ataques que tornan vulnerable nuestra información.

Conceptos tales como el principio de incertidumbre de Heisenberg, que es la base para la realización de esta criptografía y la superposición cuántica, que es el principio que se utiliza para la generación de los fotones de luz; nos permitirán entender el proceso que se lleva acabo para el propósito mencionado.

Una vez desarrollados estos conceptos el objetivo final es poder tener una idea clara de la criptografía cuántica para poder contrastarla y compararla con la criptografía tradicional con el fin de encontrar puntos de discusión que permitan concluir de forma adecuada cuál de estas es la mejor opción al momento de salvaguarda la integridad de la información.

Para poder comparar estos dos tipos de criptografía también es necesario mencionar algunos conceptos fundamentales de la criptografía tradicional con el objetivo de lograr el cometido de este documento. Se analizará las herramientas que la criptografía tradicional utiliza para cifrar la información y los canales que esta utiliza para transportar la misma.

Para cumplir con el alcance descrito se platea realizar las siguientes actividades siguiendo el cronograma a continuación:

Tabla 1.3.1. Distribución de horas por actividades

No	Actividad	Horas
1	Recolectar información y estudiar los conceptos relacionados con la criptografía tradicional.	20
2	Recolectar información y estudiar los conceptos relacionados con la criptografía cuántica.	20
3	Estudiar los diferentes modelos referidos a la transmisión de señales de luz.	30
4	Analizar brevemente los modelos matemáticos asociados con el manejo de señales de luz.	50
5	Comparar la criptografía tradicional con la criptografía cuántica.	60
6	Redacción del documento.	60
	TOTAL	**240**

Las dos primeras actividades tienen como objetivo adquirir los conocimientos necesarios para comprender cada una de las criptografías mencionadas, partiendo desde la base de cada una de ellas, pero haciendo énfasis la transmisión de señales de luz.

Las actividades tres y cuatro nos permitirán formar una idea clara de las fuentes utilizadas para generar los fotones de luz y cuáles son los canales adecuados para el trasporte de la información codificada, esto depende de cada modelo de transmisión de señales que se esté analizando.

Finalmente se plantea realizar la comparación entre las dos criptografías partiendo inicialmente de los modelos de transmisión de señales de luz para luego mencionar brevemente algunos aspectos secundarios derivados del tema como costos y equipos a utilizar. El resultado de estas actividades será un documento redactado por el autor de aproximadamente 50 paginas cumpliendo con el objetivo general mencionado en páginas anteriores. Así también se cumplirá con los objetivos específicos descritos en la sección correspondiente.

El documento resultante no realiza un estudio a profundidad de los temas tratados, solamente analiza la información pertinente de tal forma que se pueda alcanzar el objetivo general que es realizar una comparación que nos permita concluir que tipo de criptografía es la que brinda mayor seguridad a la información.

1.4 Marco teórico

1.4.1 Criptografía

Definir a la criptografía es verdaderamente complicado, hay autores que afirman que la criptografía es un arte, otro gran grupo de respetables autores fomentan que la criptografía en una ciencia aplicada; por otro lado, hay quienes sostienen que simplemente es una técnica. En este caso se ha tomado la definición dada por la Real Academia de la Lengua que dice:

"La criptografía es el arte de escribir con clave secreta o de un modo enigmático." [11]

Una vez que se ha definido a la criptografía es importante recalcar que para ocultar mensajes o información existen dos maneras, la estenografía que se encarga de ocultar completamente la información y la criptografía que se encarga de que la información o mensajes se vuelva incomprensibles, hecha la aclaración respectiva, este documento hace referencia solamente a la criptografía.

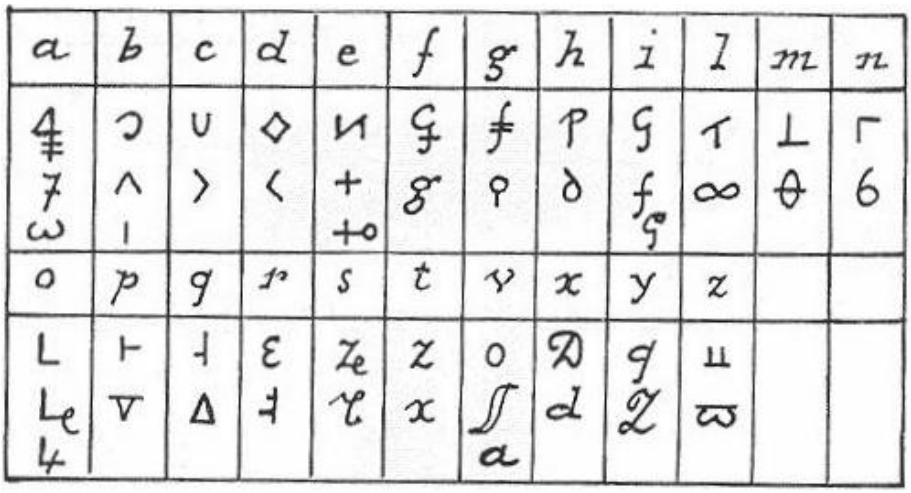

Figura 1.4.1.1. Primera tabla de sustitución.

Fuente: https://gitbooks.io/criptografia-clasica

En primera instancia es necesario mencionar los inicios de la criptografía para poder crear una base teórica sólida que finalmente nos permita llegar hasta la criptografía cuántica la cual es el objetivo de nuestro interés.

Surge la necesidad de aclarar dos conceptos bastante utilizados y muchas veces comprendidos de forma errónea, la criptografía clásica y la criptografía moderna. Por un

lado, la criptografía clásica que es el origen de los métodos de cifrado que luego de mucho tiempo pudieron desarrollarse y se convirtieron en la criptografía moderna o también conocida como criptografía tradicional que se basa en algoritmos computacionales.

Como se mencionó anteriormente el objetivo primordial es hacer una comparación entre la criptografía tradicional y la criptografía cuántica por lo cual se revisará brevemente cada una de ellas.

1.4.2 Criptografía Clásica

La primera noción histórica de la criptografía se remonta a la época de los primeros jeroglíficos donde a pesar de ya tener patrones definidos para la escritura se han hallado indicios de escritura con patrones diferentes que llevaban información entre dos individuos de alto rango en determinadas organizaciones sociales. Es decir, se ocultaba información importante al resto de personas al utilizar diferentes cadenas de caracteres.

No queda la certeza de que este proceso sea realmente el que pensamos, pero es lo más cercano a lo que hoy en día conocemos como criptografía.

Mientras las civilizaciones se desarrollaban en aspectos militares, religiosos y comerciales la necesidad de contar con un método para proteger la información se volvía cada vez más importante. La guerra entre Atenas y Esparta logró finalmente revelar el primer método criptográfico registrado denominado la escitala espartana.

La Escítala Espartana

La escítala espartana se trata de un bastón o palo en el cual se enrollaba una cinta de cuero o papiro, sobre la cinta enrollada se escribía el mensaje en las columnas paralelas al eje de palo, al desenrollar la cinta el texto escrito quedaba cifrado, es decir, el texto perdía cualquier tipo de lógica o sentido.

Para poder descifrar el texto escrito era necesario el intercambio de una clave entre emisor y receptor con la longitud y grosor del bastón utilizado.

Este mecanismo de cifrado se utilizaba en la guerra y era muy efectivo ya que el papiro que transportaban los mensajeros de guerra carecía de sentido en las manos del enemigo.

Figura 1.4.2.1. La escítala espartana

Fuente: https://gitbooks.io/criptografia-clasica

Cifrado César

Otro método de cifrado que en la antigüedad fue muy importante fue el cifrado de César. Para la época de Julio César se creó este método de cifrado que logró su cometido por mucho tiempo. El cifrado Cesar es un método mono alfabético que consiste en desplazar un determinado número de espacios el alfabeto base.

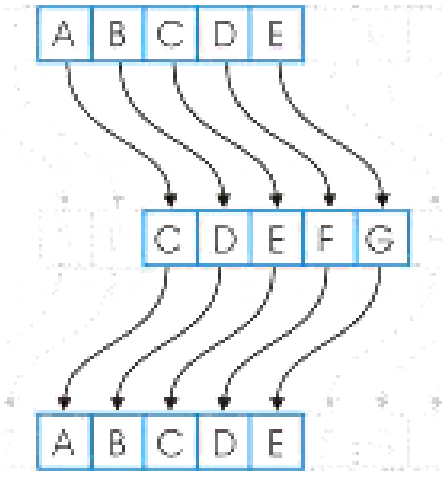

Figura 1.4.2.2 Desplazamiento de alfabeto para encriptar.

Fuente: https://gitbooks.io/criptografia-clasica

Al desplazar una cantidad específica de espacios en el alfabeto original, el mensaje inicial queda completamente sin sentido. La única forma para poder descifrar el mensaje es conocer el número de espacios que fue desplazado el mensaje al momento de ser encriptado. Para la época en la cual este método fue creado se trataba de un sistema de encripción bastante útil ya que no se contaban con dispositivos computaciones que permitan automatizar el proceso de descencripción.

A continuación, se muestra un ejemplo de cómo funciona el cifrado de cesar.

Figura 1.4.2.3 Ejemplo de Cifrado César.

Fuente: https://revistas.uexternado.edu.co

El texto a cifrar es CASA, para esto nuestra clave es desplazarse dos espacios hacia la derecha en el alfabeto para poder obtener nuestro texto cifrado.

Una vez que hemos desplazado dos espacios hacia la derecha nuestra frase encriptada será ECUC que es una palabra que carece de sentido a simple vista.

Para poder desencriptar la palabra es necesario realizar el procedimiento inverso a la inicial. En este caso el alfabeto se debe desplazar dos espacios hacia la izquierda y se obtendrá la palabra CASA.

Con el pasar del tiempo este tipo de método de cifrado se fue quedando obsoleto y el procedimiento para desencriptarlo cada vez se tornó más simple.

1.4.3 Criptografía Moderna o Tradicional

Con el despertar de la era digital se facilitó de gran manera la creación de algoritmos que permitan descifrar los mensajes de manera rápida. No existe la fecha exacta de cuando la criptografía moderna inicio, pero posiblemente se desarrolló basada en el artículo publicado

por los investigadores de la universidad de Standford, W Diffie y M. Hellman. Su artículo vió la luz en 1976 y es considerado el nacimiento oficial de la criptografía moderna, sin embargo, existen comentarios que afirman que algunas asociaciones militares habrían desarrollado métodos similares años atrás con el objetivo de proteger la información que se intentaba transmitir.

El constante desarrollo de la criptografía hacia que se establecieran más condiciones que permitan que la información este completamente segura. Se mencionan varios conceptos que permiten que la criptografía sea capaz de proteger a la información contra espías o ataques informáticos. Por lo tanto, la criptografía de ser capaz de cumplir con:

Integridad

Este concepto hace referencia a la no corrupción de la información, es decir, tener plena certeza que la información que se emitió sea la misma que se recibió una vez aplicado un método de desencripción.

El concepto de integridad de la información abarca varios puntos importantes a destacar, la integridad debe evitar lo siguiente:

Figura 1.4.3.1 Integridad de la Información.

Fuente: https://revistas.uexternado.edu.co

Confidencialidad

La confidencialidad en la información hace referencia a la garantía que esta tiene para no ser divulgada en el proceso de envío hasta el receptor. La información debe ser enviada únicamente al destino especificado sin que sea manipulada en el proceso. Esta confidencialidad se garantiza por medio de reglas o tratados que limitan el acceso a la

información. Algunas recomendaciones para que la información sea confiable es la generación de claves apropiadas las cuales no deben ser compartidas.

Autenticación

La autenticación se trata de seguir un procedimiento adecuado de identificación de tal forma que no todas las personas puedan ingresar a determinada información. Se podría decir que es la forma de verificar que el destino de la información es el correcto y que no se trata de un impostor que podría robar la información. La forma más común de realizar el proceso de autenticación es por medio de un usuario y una contraseña.

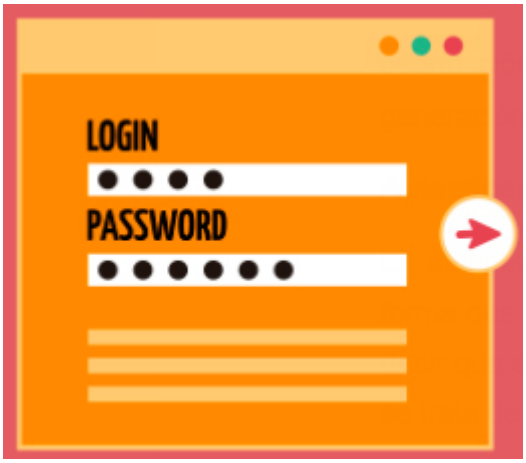

Figura 1.4.3.2 Autenticación.

Autorización

Se trata del otorgamiento de los permisos que permiten la manipulación de la información. Para acceder a la información es necesario tener en consideración que no todos los individuos deben manipularla de la misma manera, es decir, habrá casos que la información solamente debe ser leída mas no modificada; o por otro lado se evidencian casos donde la información puede ser modificada pero no eliminada.

Después de que la criptografía clásica tomó forma, el mayor desarrollo de la criptografía moderna se lleva a cabo durante la segunda guerra mundial, en esta época se establecen criterios que nos permiten visualizar a la criptografía con más claridad. Una de las razones más importantes para que la criptografía haya alcanzado tal nivel se debe al desarrollo tecnológico, específicamente al desarrollo computacional al incluir algoritmos que permiten resolver operaciones matemáticas complejas en muy corto tiempo.

Actualmente se sabe que la criptografía moderna se basa o se divide en dos grades categorías en función del tipo y del número de claves que se han de utilizar.

Sistemas simétricos: Los sistemas simétricos también son conocidos como de clave única o de clave privada, es decir, utilizan la misma clave para encriptar como para desencriptar la información. Estos sistemas al tener una sola clave no se consideran muy seguros y el proceso para romper su seguridad es corto.

Sistemas asimétricos: Los sistemas asimétricos también son conocidos como de clave pública o de dos claves. Estos sistemas hacen uso de un par de claves, una clave es utilizada al momento de cifrar el mensaje y otra clave es utilizada al momento de descifrar el mensaje.

Figura 1.4.3.3 Cifrado Simétrico y Asimétrico

Fuente: https://www.cifrar-descifrar-textos-herramientas

1.4.4 Modelos y Canales de transmisión de la Criptografía Tradicional

El área de la criptografía moderna es un campo inmensamente grande el cual ha sido desarrollado por muchos años de estudios. Se plantea mencionar un par de modelos matemáticos que han dado muy buenos resultados en la transmisión de la información a lo largo de la historia con la finalidad de tener información relevante para poder hacer la comparación al final del documento.

Además, se menciona algunos de los canales más utilizados para poder trasportar la información de un punto a otro sin que existan inconvenientes en el proceso.

1.4.4.1 Modelos de Transmisión de la Información

Es bien conocido que la información viaja de un lado a otro en forma de bits mediante un canal que los transporta intentado ser lo más confiable posible. Para que los millones de bits que transitan las redes interconectadas puedan moverse de forma rápida y eficaz se crearon varios modelos matemáticos que agilizan este proceso.

El primer paso para que la información viaje de un emisor hasta un receptor es convertirla en un paquete de datos, un paquete de datos no es nada más que un conjunto de bits agrupados; estos bits deben ser codificados en la capa física para poder ser transportados por un medio determinado.

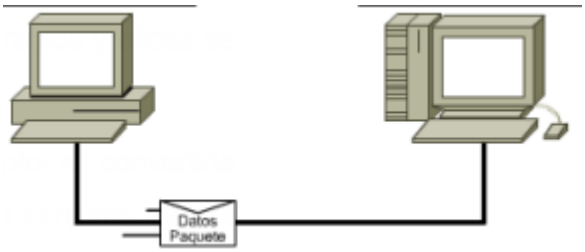

Figura 1.4.4.1.1. Transporte de paquetes

Como se mencionó anteriormente en la criptografía tradicional y todo lo que conlleva su desarrollo existen un sin número de modelos y métodos para transportar la información. A continuación, vamos a mencionar dos de ellos para tener una idea general de cómo funciona.

Codificación Bipolar

La codificación bipolar trabaja con 3 niveles de voltaje a ser detectados los cuales son positivo, negativo y nulo. El nivel 0 se usa para detectar el bit 0 y el bit 1 se detecta alternando el nivel positivo y negativo respectivamente.

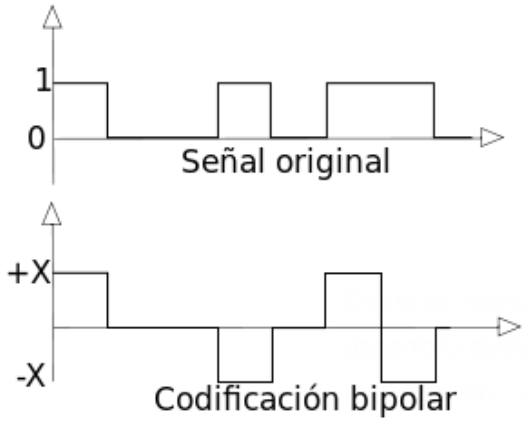

Figura 1.4.4.1.2 Codificación Bipolar

Codificación Bifásica

La codificación bifásica es un método donde la señal cambia justo en medio del intervalo de bit y además nunca vuelve a nivel nulo de tensión porque continua hasta el lado opuesto del nivel en el cual se encontraba. Existen dos variantes para este método de codificación:

La codificación Manchester

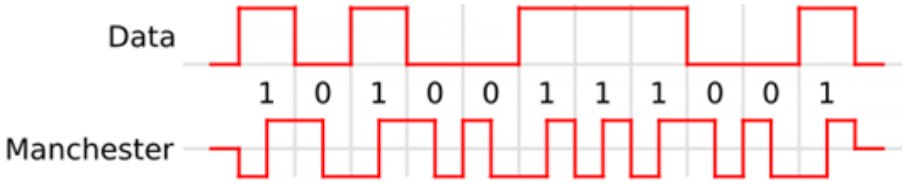

Figura 1.4.4.1.3 Codificación Bipolar

La codificación Manchester Diferencial

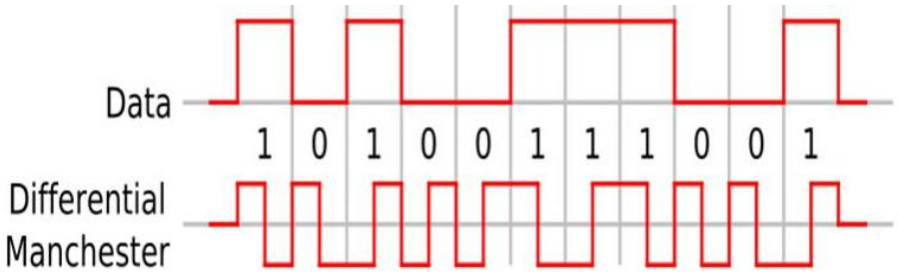

Figura 1.4.4.1.4 Codificación Bipolar

Hasta este punto se ha resumido muy brevemente varios conceptos que nos permiten tener una idea muy general de la criptografía tradicional. Para complementar esta información se mencionan los métodos de cifrado más utilizados en la actualidad.

Cifrado AES 256

AES significa Advanced Encryption Standard que traducido al español es Estándar de Cifrado Avanzado, es uno de los algoritmos actualmente más usados en el medio ya que tiene un gran nivel de seguridad y es de acceso público.

Este algoritmo tiene sus inicios en el año de 1997 cuando el Instituto de Nacional de Estándares y Tecnología comenzó la búsqueda de un nuevo algoritmo que pueda reemplazar al ya desgastado y envejecido algoritmo DES.

En el 2001 AES por fin llega a ser público como el nuevo estándar de cifrado, este método de cifrado se consolida como algo prometedor ya que su justificación matemática maneja operaciones de alto rango que incluso para un computador logran ser dificultosos. A pequeños rasgos el algoritmo consta de sustituciones matemáticas, varias permutaciones y múltiples transformaciones lineales; cada una de esta es un bloque de datos de 16 bytes.

Las operaciones realizadas se ejecutan en ciclos a los cuales se les conoce como rondas, en cada ronda se calcula una clave a partir de la clave de cifrado y se la incluye en los cálculos. Tomando en cuenta el rango de las operaciones se considera que, si existe la alteración de un solo bit en la clave, por ejemplo, se obtiene un bloque completo con datos erróneos; esta característica hace que el algoritmo tenga una gran ventaja sobre los algoritmos de flujo tradicionales.

Conforme se va desarrollando el algoritmo hay cambios notables con respecto al algoritmo inicial, la mayor diferencia está en el tamaño de la clave que se va generando en cada versión de AES. Actualmente se cuenta con AES-128, AES-192 y AES-256, para esta última versión del AES se han realizado cálculos midiendo el tiempo que le llevaría a un supercomputador poder vulnerarlo y el resultado es sorprendente ya que le tomaría nada más que la conocida edad del universo.

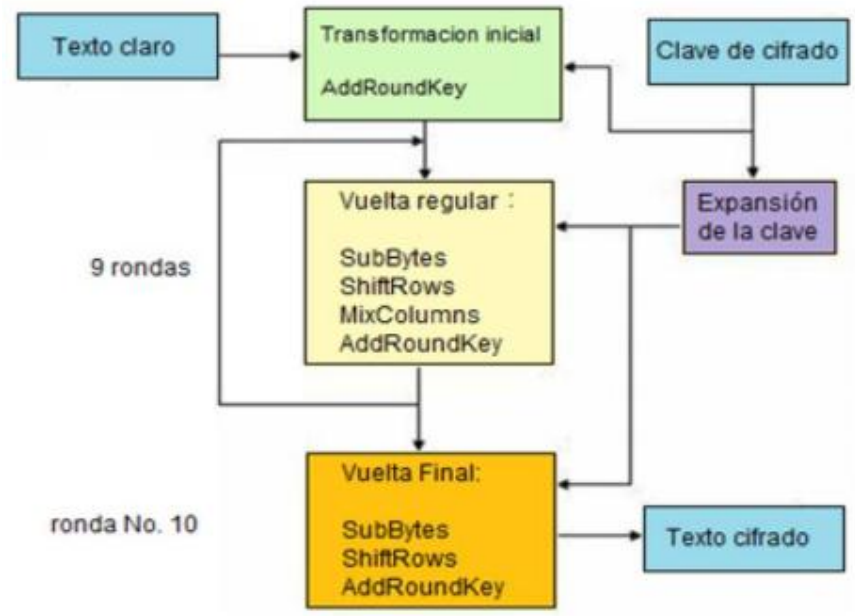

Figura 1.4.4.1.5 Esquema General AES-128

Este método de cifrado se ha convertido en el más seguro actualmente y por esta razón es utilizado en ámbitos militares, financieros y de gobierno.

Cifrado RSA

El cifrado RSA tiene ese nombre debido a sus desarrolladores Rivers, Shamir y Adleman; estos 3 investigadores lograron redescubrirlo en el año de 1977 ya que originalmente era propiedad de la inteligencia militar Britanica.

Este método de cifrado trabaja con una clave pública y con una clave privada las cuales deben relacionarse y complementarse; es decir que una que si un mensaje es cifrado con una de estas claves la única forma de poder descifrar el mensaje en poseer la clave complemento. Este cifrado es ampliamente utilizado en las firmas digitales y su nivel de seguridad es muy alto ya que matemáticamente está basado en la factorización entera que es un procedimiento mediante el cual el mensaje a cifrar es considerado un gran numero el cual es elevado a la equivalencia de la clave generada para luego ser dividido por un producto fijo de dos números primos.

1.4.4.2 Canales de Transmisión

De la misma forma que en las codificaciones y en los métodos de cifrado el tema de los canales de transmisión es un aspecto muy extenso, en este documento se plasman los conceptos fundamentales de tal forma que se pueda cumplir con el objetivo planteado inicialmente.

Existen varios medios por los cuales se puede transportar la información, a continuación, enlistamos algunos:

- Cable Telefónico
- Cable Coaxial
- Cable UTP
- Fibra Óptica

Se tratan brevemente los dos últimos medios ya que en la actualidad son los más usados, además de esto la fibra óptica es un canal común entre la criptografía tradicional y la criptografía cuántica.

Cable UTP

UTP viene de las siglas Unshielded Twisted Pair que en español significa Par Trenzado No Blindado, es el medio conductor más utilizado en el ámbito de las redes de datos y telecomunicaciones.

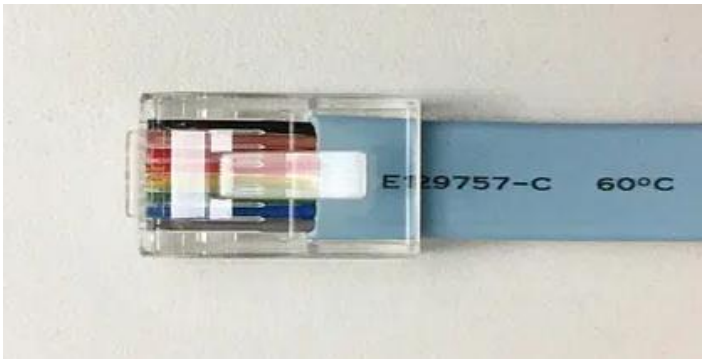

Figura 1.4.4.2.1 Cable UTP

Este cable de par trenzado fue creado por Alexander Graham Bell y se trata de un par de conductores eléctricos que se entrelazan con la finalidad de eliminar la interferencia con otros cables y medios externos.

Con el transcurrir del tiempo el cable UTP ha ido evolucionando y en la actualidad se tienen varios pares de conductores entrelazados en mismo empaque, además se ha incluido

conectores que nos permiten realizar conexiones de manera más simple ya que estos se rigen a un estándar ya establecido y aceptado.

Los conectores RJ45 nos permiten hacer conexiones a redes de datos de forma sencilla y sin tener realizar conexiones no habituales. Para incluir un conector RJ45 en un cable UTP es necesario seguir los colores normalizados para que no existan problemas posteriores a la instalación. La siguiente figura nos muestra las conexiones que deben realizarse al momento de implementar el conector mencionado.

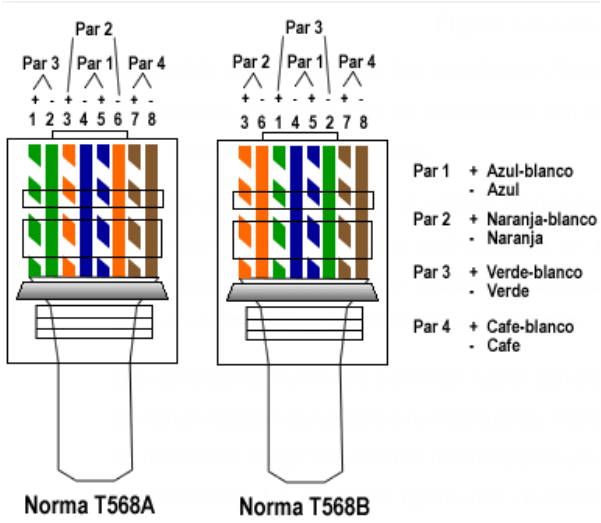

Figura 1.4.4.2.2 Normativa para Conector RJ45

Fibra Óptica

La fibra óptica es un medio de transmisión de datos muy utilizado actualmente ya que nos brinda mayor velocidad, la fibra óptica utiliza pulsos fotoeléctricos para transportar los bits. Está estructurada principalmente de vidrio o plástico que permiten q la luz rebote y pueda desplazarse a través del conductor.

Figura 1.4.4.2.3 Normativa para Conector RJ45

La gran ventaja de la fibra óptica es que es inmune a las interferencias electromagnéticas e interferencias externas. Dependiendo de sus características la fibra óptica puede clasificarse en fibra monomodo y fibra multimodo, la utilización de cada una de ellas depende de las características de la conexión como la distancia y el lugar donde se va a desplegar.

La longitud de onda que maneja la fibra óptica también varía dependiendo la estructura de la misma, es importante tener presente que al ser un medio guiado tambien cuenta con varias limitaciones por ejemplo en despliegue en distancias muy grandes. Al tener una estructura interior mas delicada implica tambien mayores cuidados para que funcione adecuadamente, adicional a eso hay que tener en cuenta que los conectores seran completamente diferentes ya que deben manejar señales de luz. Las fuentes mas comunes para generar los pulsos fotoelectricos en la fibra optica son los laseres y leds.

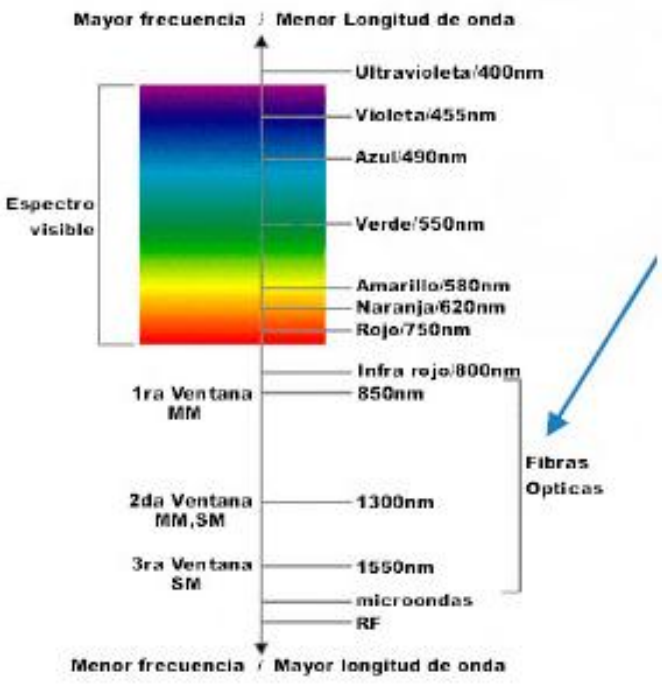

Figura 1.4.4.2.4 Normativa para Conector RJ45

2 METODOLOGÍA

En esta sección del documento detallaremos el proceso que se siguió para la realización del mismo, describiremos el diseño o el planteamiento que ha sido utilizado en su desarrollo dependiendo del método que ha sido utilizado.

Este documento tiene como objetivo principal hacer una comparación de la criptografía cuántica, en este documento detallada, con la criptografía tradicional; haciendo uso de conceptos básicos que conlleva este tipo de criptografía.

Para la realización de este documento se utilizará un método investigativo inductivo lo que significa que, partiendo del caso particular, como lo es la criptografía cuántica, se llega a un caso general que para este documento se trata de la comparativa de las dos criptografías mencionadas anteriormente.

Teniendo en cuenta el contexto y la temática para el documento se optó por un enfoque cualitativo, de esta manera el tipo de trabajo será descriptivo utilizando el análisis documental y principalmente las referencias bibliográficas para recolectar la información pertinente para poder cumplir con el objetivo principal.

Teniendo en cuenta los tiempos descritos para cada actividad mencionados en el alcance se realiza la distribución de actividades que en líneas más adelante se explicaran por fases.

La tabla a continuación muestras las horas designadas para cada actividad planificada:

Tabla 2.1 División de actividades por horas

No	Actividad	Horas
1	Recolectar información y estudiar los conceptos relacionados con la criptografía tradicional.	20
2	Recolectar información y estudiar los conceptos relacionados con la criptografía cuántica.	20
3	Estudiar los diferentes modelos referidos a la transmisión de señales de luz.	30
4	Analizar brevemente los modelos matemáticos asociados con el manejo de señales de luz.	50
5	Comparar la criptografía tradicional con la criptografía cuántica.	60
6	Redacción del documento.	60
	TOTAL	**240**

2.1 Fase Teórica

En la primera fase para la realización de este documento, como se lo dijo anteriormente, se recolectó la información por medio de análisis documental y referencias bibliográficas.

Para esto se estructuró un procedimiento que nos permitió llegar a fuentes bibliográficas confiables.

El procedimiento consiste en:

1. Buscar cualquier tipo de documento, ya sean papers, revistas, libros, etc; relacionados con el tema, es importante no exagerar con la cantidad de documentos que se están obteniendo.
2. Una vez que se tengan almacenados estos documentos se deben analizar cada uno de ellos para poder descartar los que menos información efectiva contengan. En este punto es importante tomar el tiempo necesario para revisar con el mayor detalle la documentación con la finalidad de no volver a realizar este paso.
3. Finalmente, una vez filtrada la información se procede a realizar un análisis documental, es decir, realizar el proceso de interpretación de la información adquirida mediante los documentos que quedaron después del filtro y sintetizarla de tal forma que sea útil para el objetivo de documento.

Figura 2.1.1. Tratamiento de la información

2.2 Fase de Diseño

En esta fase se analizó varias opciones para definir una metodología que se ajuste a las necesidades del documento con la finalidad de alcanzar el objetivo principal sin mayores contratiempos.

Inicialmente se tomaron en cuenta las metodologías agiles, que en la actualidad están siendo muy utilizadas, ya que estas nos permiten obtener resultados de forma rápida, con procedimientos estructurados y siendo bastante efectivas y eficaces.

Algunas de las metodologías agiles que se planearon utilizar fueron las metodologías Kanban, Lean y Scrum las cuales, aunque son muy atractivas, no fueron de utilidad al momento de realizar el diseño del documento.

Figura 2.2.1 Metodologías.

Fuente: http://comunidad.iebschool.com/metodologias

La metodología Kanban, por ejemplo, no se pudo acoplar en este proyecto ya que esta metodología se orienta a la mejora continua, para lograr esto se basa en una lista de acciones que se va realizando en un proceso de trabajo continuo. El proceso que se llevó a cabo en este proyecto no fue continuo por lo que su implementación se descartó. De la misma forma se encontraron inconvenientes con las otras metodologías agiles mencionadas. Las metodologías agiles tienen la ventaja de realizar correcciones o iteraciones en el proceso y si es necesario retroceder en el mismo con la finalidad de obtener mejores resultados.

Para la realización de este documento se optó por una metodología tradicional, la metodología investigativa, ya que se trata de un proceso de investigación y recolección de información con el fin de solventar algo. Para el fin pertinente de este documento se recolectará información en primera instancia, luego se la procederá con el análisis de la información recolectada con la finalidad de obtener información adecuada y finalmente se obtendrá un resultado; que para este caso es poder concluir que criptografía nos permite asegurar de mejor manera nuestra información.

Se realizará la comparación mediante una tabla que permita visualizar de mejor manera los aspectos más importantes entre los dos tipos de criptografía; teniendo en cuenta la información primordial que permita alcanzar el objetivo principal planteado inicialmente.

2.3 Fase de Resultados

Para la fase final, es importante recalcar que este proyecto no cuenta con una fase de implementación, ya que se trata de un análisis netamente teórico por lo cual una vez concluida la fase de diseño, y con la información adquirida, se procederá a concluir sobre el tema descrito anteriormente.

Los resultados obtenidos en este documento es información concluida a partir de los conceptos compartidos en el mismo, y netamente realizados por el autor; tratando de solventar la principal premisa de este documento que es, ¿qué criptografía es más segura para mantener a salvo nuestra información?

En esta fase se planteó realizar la comparación de la criptografía tradicional con la criptografía cuántica de tal forma que el lector no necesite conocimientos muy profundos sobre la mecánica cuántica. Inicialmente se hará una comparativa de los aspectos desarrollados en este documento como lo son las fuentes de fotones y los canales cuánticos utilizados, para luego también mencionar de forma breve algunos aspectos derivados como equipos y costos relacionados.

Tabla 2.3.1. Diseño de Tabla Comparativa

	Criptografía Tradicional	Criptografía Cuántica
Aspecto 1		
Aspecto 2		
Aspecto 3		
Aspecto n		

Después de la elaboración de la tabla comparativa se procederá a redactar los resultados obtenidos para proceder a verificar que el objetivo de este documento se haya cumplido de manera satisfactoria.

Se termina haciendo una corta mención a temas derivados que podrían ser abarcados con más profundidad en la realización de un documento del mismo tipo que este escrito. Se procede a redactar conclusiones y recomendaciones del tema tratado.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1 Resultados

3.1.1 Análisis Introductorio A La Criptografía Cuántica

La criptografía cuántica tiene sus inicios de la mano de Richard Feynman físico teórico estadounidense que realizo estudios y desarrolló modelos orientados a la mecánica cuántica [1]. La criptografía cuántica usa los principios básicos de la mecánica cuántica para cifrar la información mediante algoritmos criptográficos que hacer que la información cifrada sea imposible de descifrar sin la clave de encriptación. De esta manera el nivel de seguridad de la información que hace uso de esta metodología se incrementa en gran medida y es prácticamente invulnerable.

El avance de la tecnología hace que cada vez sea más fácil realizar métodos que vulneren la seguridad de nuestra información, por esta razón nacen los métodos de criptografía cuántica que están orientados directamente a luchar contra este tipo de amenazas. Las maquinas actuales tienen una gran capacidad de almacenamiento y sobretodo gran capacidad de computo, es decir, pueden realizar miles y hasta millones de operaciones en pocos segundos lo que permite vulnerar con facilidad la mayoría de los algoritmos de la criptografía tradicional.

La criptografía cuántica trae consigo una gran cantidad de consideraciones ya que es relativamente nueva y casi no fomentada en la actualidad. La criptografía cuántica no se limita a ser usada solamente por computadores cuánticos, sino también que se puede utilizar en los computadores convencionales acondicionándolos con el hardware y software adecuado para ello.

Inicios De La Criptografía Cuántica

La primera idea de la criptografía cuántica de manera formal se da con la presentación del escrito “Codificación Cuántica Conjugada” propuesta por Stephen Wiesner, físico investigador norteamericano, a principio de la década de 1970 la misma que fue rechazada por la IEEE; este documento termina siendo publicado en el año de 1983 por SIGACT News [2, p. 2].

Wiesner propuso almacenar y transmitir dos mensajes codificándolos en dos “observables conjugados”, es decir, dos cantidades físicas que podrían ser medidas a posteriori. Dichos observables eran la polarización lineal y circular de los fotones, de forma que cualquiera de los dos, pero no ambos (debido al entrelazamiento cuántico), se podrían recibir y decodificar.

Años después, en 1979 Gilles Brassard y Charles Bennett lograron utilizar los descubrimientos de Wiesner al darse cuenta que los fotones podían transmitir la información y no almacenarla; basándose en esto y después de trabajar en este tema por varios años en 1984 propusieron un método de comunicación segura, considerado como el primer método de criptografía cuántica, el BB84. El objetivo de este método es la distribución de claves, generar claves aleatorias entre dos usuarios y compartirlas de forma segura; así nace el primer algoritmo de compartición de claves cuánticas Quantum Key Distribution (QKD) [2, p. 7]

Este algoritmo utiliza filtros de polarización y ángulos de 0, 45, 90 o 135 grados respecto a la vertical, se envían fotones polarizados en ángulos entre 0 y 45 grados que representan un valor binario equivalente a 0 mientras que los fotones polarizados en otros ángulos representan un valor binario de 1.

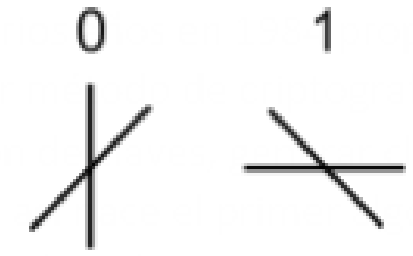

Figura 3.1.1.1 Polarizaciones posibles de la luz en BB84.
Fuente: M. Baig, *Criptografía Cuántica.*

Artur Ekert físico británico en 1991 diseñó el protocolo E91 o también conocido como EPR que toma este nombre de la paradoja de Einstein-Podolsky-Rosen que involucra el entrelazamiento cuántico para la generación de claves [2 p. 9]. A diferencia del protocolo

BB84 este no cuenta con estados de polarización predefinidos, al contrario, las claves son generadas al momento de la transmisión. A la hora de generar la clave tanto emisor como receptor comparten pares de fotones entrelazados que tienen la misma polarización tratándose de un método puramente cuántico.

Un año más tarde Charles Bennett propone un nuevo algoritmo denominado B92 que básicamente se trata del algoritmo BB84 simplificado, es decir, solo utiliza dos posibles direcciones ortogonales para la polarización.

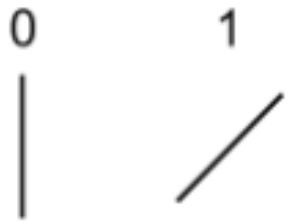

Figura 3.1.1.2 Polarizaciones posibles de la luz en B92
Fuente: M. Baig, *Criptografía Cuántica*.

3.1.2 Algunos Conceptos Básicos de la Criptografía Cuántica.

La criptografía cuántica abarca un sin número de conceptos relacionados principalmente con la mecánica cuántica, a continuación, se hace referencia a las bases fundamentales que permiten que sea posible la encriptación de información por medio de fotones de luz. Recordemos que la criptografía tradicional se basa fundamental en métodos probabilísticos matemáticos que permiten cifrar la información pero que cada vez son más “sencillos” de descifrar.

3.1.2.1 Principio de Incertidumbre de Heisenberg

Uno de los principios básico que la criptografía cuántica toma es el principio de incertidumbre de Heisenberg que a continuación será descrito de forma simplificada. Cabe recalcar que no es el único principio en el cual la criptografía cuántica se rige o utiliza para su desarrollo, sin duda existen muchos principios y métodos cuánticos que permiten el desarrollo de la criptografía cuantica; “The Feynman Lectures on Physics” es un libro que nos permite tener una vista más detallada de todos estos conceptos relacionados [4].

El principio de incertidumbre o principio de indeterminación de Heisenberg afirma que no se puede determinar con precisión la posición y el momento lineal de una partícula observable [6].

3.1.2.2 Fotones de Luz

El universo está compuesto enteramente de átomos, que fue considerada la partícula más pequeña por mucho tiempo, en la actualidad se han dado a conocer varias partículas que, así como los átomos se han convertido en la base de toda la materia.

Hasta hace algunos años la división de algunas partículas no se creía posible, pero mientras la tecnología continúe avanzando y nuevos estudios físicos se desarrollen es posible que la ciencia siga en un cambio continuo. Se establece entonces el término “cuanto”, que representa en términos de física cuántica, el valor más pequeño que una magnitud física puede tomar en un sistema físico. Dentro de la física cuántica y orientados netamente a la criptografía cuántica es indispensable mencionar a la partícula fundamental de la luz, el fotón, es la partícula elemental de la luz. Algunos grandes científicos como A. Einstein denominaban al fotón con el nombre de “cuanto de luz”.

La luz se ve afectada por la superposición cuántica, además, la dualidad onda – partícula hace que la luz adquiera una propiedad derivada de las ondas electromagnéticas denominada polarización. La polarización de la luz es la inclinación que se le puede dar a sus ondas de tal forma que pueden viajar de forma horizontal, vertical o con un ángulo determinado respecto a un sistema de referencia.

3.1.2.3 Superposición Cuántica o Superposición de Estados

A nivel cuántico las partículas no cumplen con las leyes tradicionales de la física, cuando nos referimos a física cuántica existen nuevas leyes a las cuales debemos regirnos, entre estas leyes se denota la superposición de estados que es de gran importancia para entender la criptografía cuántica.

La superposición de estados o superposición cuántica manifiesta que una partícula cuántica observable tiene varios estados superpuestos y definidos por una función de onda específica, una vez que la partícula cuántica observable entra en un medio de interacción su función de onda colapsa y por consecuencia toma un estado específico y sale de su estado de superposición cuántica.

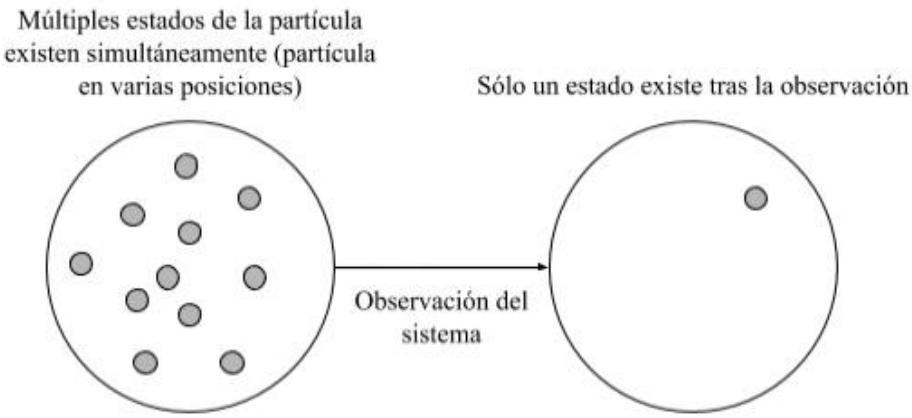

Figura 3.1.2.3.1 Colapso de la superposición cuántica
Fuente: S. Miguéns y P. Gonzalez, *Introducción a la Criptografía Cuántica.*

Una vez que una partícula cuántica observable sale de su estado de superposición es imposible saber los estados iniciales que esta partícula tenía antes de la interacción, a esta particularidad se la conoce como el teorema de no clonación [5]; esto nombre es bastante lógico ya que para que el sistema inicial de las partículas observables pueda ser clonado se debe realizar mediciones para conocer su estado inicial. Sin embargo, cualquier interacción provocará que el sistema colapse y adopte un estado definido haciendo imposible clonarlo en su estado inicial, esto no ocurre con su estado final que al haber colapsado el sistema su función de onda toma valores específicos y es posible realizar mediciones sobre este.

3.1.2.4 QUBITS

Aparece un concepto importante en la criptografía cuántica y más aún en la propagación de la luz, el qubit tiene un concepto análogo al del bit en la criptografía tradicional; el qubit es un sistema cuántico que consta de 2 estados observables [10] que se rigen bajo las leyes de a mecánica cuántica y más específicamente se basan en el principio de superposición cuántica que ya fue brevemente explicado en páginas anteriores. Al qubit se denominan también como la mínima unidad de información cuántica.

A continuación, presentamos algunas de las razones por las que los qubis son utilizados para codificar la información mediante los fotones de luz:

- El entrelazamiento entre los fotones es sencillo por el número limitado de estados que tienen.
- Utilizan fuentes de fotones de bajo costo como infrarrojos o láseres.

- Pueden desplazarse grandes distancias sin ser afectados por el entorno que los rodea ya sea en aire libre o por medio de fibra óptica.

3.1.3 Fuentes De Fotones De Luz

En el proceso de distribución de claves cuánticas un punto importante es la generación de fotones, idealmente las fuentes para realizar una distribución de claves cuánticas son las fuentes deterministas de fotones individuales. Este tipo de fuente solamente se encuentra a nivel de laboratorios experimentales por lo que se trata de obtener el mismo resultado por diferentes caminos.

Las dos formas que mayormente han sido aceptadas por su afectividad son las fuentes de estados coherentes y las fuentes de fotones anunciados.

3.1.3.1 Fuentes De Estados Coherentes De Luz

Las fuentes de estados coherentes de luz describen paquetes de ondas no dispersivos de mínima incerteza, estas fuentes son las que mejor desempeño muestran ya que aproximan las trayectorias en el espacio de fases óptico de los estados clásicos del campo electromagnético, comúnmente trabajan con intensidades de pocas fotos sobre láseres pulsados y láseres monomodo continuos [7].

La emisión de los fotones que presentan estas fuentes tienen bases estadísticas por lo que se las denomina fuentes poissonianas, estos estados coherentes vienen dados por la siguiente expresión:

$$\alpha = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} n$$

Ecuación 3.1.3.1.1 Numero de estados coherentes con distribución Poissoniana.

Donde n representa el número de estados de la superposición y α es un numero complejo relacionado con el operador de aniquilación [7].

Como se mencionó se sigue la distribución de Poisson para lo cual la probabilidad de encontrar n fotones está dada por:

$$Pn(\mu) = |\langle n|\sqrt{\mu}\rangle|^2 = e^{-\mu}\frac{\mu^n}{n!}$$

Ecuación 3.1.3.1.2 Probabilidad de encontrar n fotones con distribución de Poisson.

Donde μ es el valor medio de fotones para un estado coherente dado.

Haciendo un análisis de las expresiones matemáticas dadas anteriormente se puede observar que una buena fuente de fotones individuales es aquella que tiene los estados coherentes con valor medio de fotones por pulso cercano a 0.1, sin embargo, esto solo funcionará correctamente el 10% de las veces.

La grafica a continuación muestra un detalle de diferentes valores para μ y cuál es el efecto que este produce en la fuente.

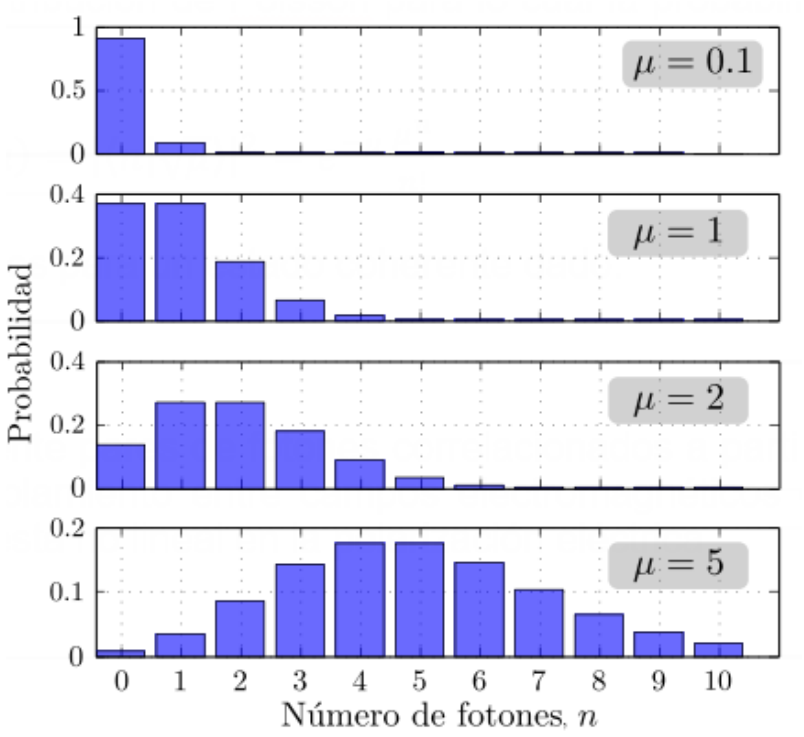

Figura 3.1.3.1.1 Distribución de probabilidad de detección del número de fotones para fuentes Poissonianas. Fuente: I. López, “Distribución cuántica de claves criptográficas”.

Entonces, a medida que μ aumenta su valor la fuente de fotones individuales es mejor pero su eficiencia decrece, es decir, si es necesario una fuente de fotones que emita fotones de buena calidad pero que no trabaje todo el tiempo al 100% debemos disminuir μ. Si nosotros aumentamos μ obtenemos una fuente la cual trabaja más tiempo, pero la calidad de los fotones que genera no es buena por lo que la información puede sufrir contratiempos considerables.

3.1.3.2 Fuentes De Estados Anunciados

Las fuentes de estados anunciados actualmente son las más utilizadas ya que trabajan en el rango de frecuencia visible - infrarrojo.

Estas fuentes generan aleatoriamente pares de fotones correlacionados a partir de un único fotón, al producirse un acoplamiento entre campos electromagnéticos que se muestran en materiales con respuesta no lineal en la polarización eléctrica.

La representación para un par de fotones correlacionados se la puede ver de la siguiente manera:

$$\langle Np, 0s, 0i| \rightarrow |(N-1)p, 1s, 1i\rangle$$

Ecuación 3.1.3.2.1 Par de fotones correlacionados

Donde N representa los fotones con longitud de onda inicial o de bombeo, el subíndice viene de la palabra en ingles pump. Por un proceso de parametrización descendente se obtiene un par de fotones los cuales son 0s y 0i, que toman los nombres de signal e iddler respectivamente.

Para este proceso de se hace referencia a la conservación de la energía, por tanto, haciendo uso de la física clásica y el concepto de la conservación del momento lineal podemos describir la siguiente expresión:

$$\rho_p = \rho_s + \rho_i$$

Ecuación 3.1.3.2.2 Conservación de la cantidad de movimiento lineal

Esto quiere decir que los fotones que se generan está estrechamente relacionados por su momento lineal y además por su energía, además de encontrarse correlacionados en polarización y en tiempo. Así se obtienen los fotones anunciados y cada vez que se detecta un fotón del par generado se crea una ventana determinada por el valor μ que como ya se explico es el número medio de fotones en el tiempo de duración de la misma; probabilísticamente esto se basa en una distribución de Poisson [8].

Existe una gran diferencia con respecto a las fuentes de estados coherentes ya que gracias a la producción de un par de fotones y a la conservación del momento lineal en cada uno de ellos esta fuente tiene una eficiencia máxima para cualquier intensidad de luz.

3.1.4 Medios De Transmisión Cuántica

En este documento principalmente mencionaremos dos medios de transmisión de fotones, sin embargo, no son los únicos que existen con este fin. Los sistemas de distribución de claves cuánticas generalmente utilizan la fibra óptica o aire libre para la transmisión de la información independientemente de las fuentes de fotones que se utilizan. Los canales de comunicación dependen de varias propiedades como la longitud de onda, tipo de medio, reflexión, distancia, etc. A continuación, se mencionan algunos conceptos de los medios de transmisión para tener una pequeña idea de sus características y particularidades.

3.1.4.1 Fibra Óptica

La fibra óptica como canal cuántico es excelente ya que tiene las propiedades adecuadas para propagar la luz, en el mercado actual se pueden encontrar con diferentes características como por ejemplo fibras ópticas con pérdidas muy bajas como de 0.2 dB/Km para 1550 nm, esto significa que la luz que las atraviesa es capaz de recorrer grandes distancias sin atenuarse.

El principio básico de la fibra óptica se basa en encerrar los fotones de luz en un medio con un determinado índice de refracción que hace que los fotones de luz reboten de un extremo a otro. Existen dos características importantes a ser consideradas, estas son el tamaño del núcleo de la fibra y la longitud de onda con la que viaja la luz, dependiendo de la relación que estas dos características tengan se desarrollan uno o más modos de propagación que clasifican a la fibra óptica como fibra monomodo y fibra multimodo [9].

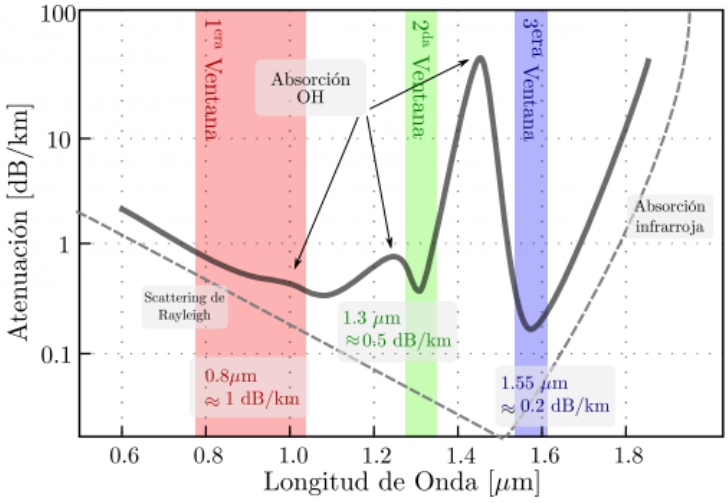

Figura 3.1.4.1.1 Atenuación de las fibras monomodo en función de la longitud de onda utilizada. Fuente: I. López, *"Distribución cuántica de claves criptográficas"*.

Otra característica a ser considerada en los protocolos de distribución de claves cuánticas es el grado de libertad de la luz en los que se codifica la información, ya que de esto depende también la atenuación que refleja el canal cuántico utilizado [7, pag. 19-21].

3.1.4.2 Aire Libre

El aire libre es el canal cuántico que existe naturalmente y permite el transporte de los fotones de luz, tiene un gran espectro y gran ancho de banda utilizable. El aire libre no cuenta con un medio que guie la luz entre dos puntos por lo que la dispersión de los fotones es muy grande y es difícil que exista comunicación en grades distancias.

Este canal al no tener protección del medio exterior es muy fácil que se vea afectado por la atenuación e interferencia; el solo cambio de temperatura afecta las condiciones del canal. Sin embargo, el aire libre como canal de transmisión de fotones es muy utilizado en comunicaciones satelitales, la distribución de claves cuánticas se podría realizar a muy largas distancias con la ayuda de satélites que funcionan como repetidores de señales; pero existen algunos fenómenos que ocurren en la propagación por aire y sin duda tienen un efecto sobre la comunicación.

En la figura 6 se muestra el espectro electromagnético de la luz, cuando se hace referencia a fuentes de fotones que trabajan en el aire libre generalmente se habla de fuentes de luz infrarrojas.

La siguiente tabla nos muestra algunos de los fenómenos más comunes y el efecto que causan en el canal de transmisión.

Tabla 3.1.4.2.1. Principales fenómenos que perturban la propagación de la luz en el aire y los efectos que generan. Fuente: I. López, *"Distribución cuántica de claves criptográficas".*

Fenómeno	**Efecto**
Difracción	Expansión de haz de luz.
Absorción	Atenuación de la luz.
Scattering	Atenuación y distorción de la polarización de la luz
Turbulencia	Centelleo, atenuación dependiente del tiempo, distorsión de la polarización y la fase.
Disperción	Ensanchamieto temporal de pulsos.

Radiación de fondo	Ruido de detección o intermitencia en el funcionamiento del dispositivo

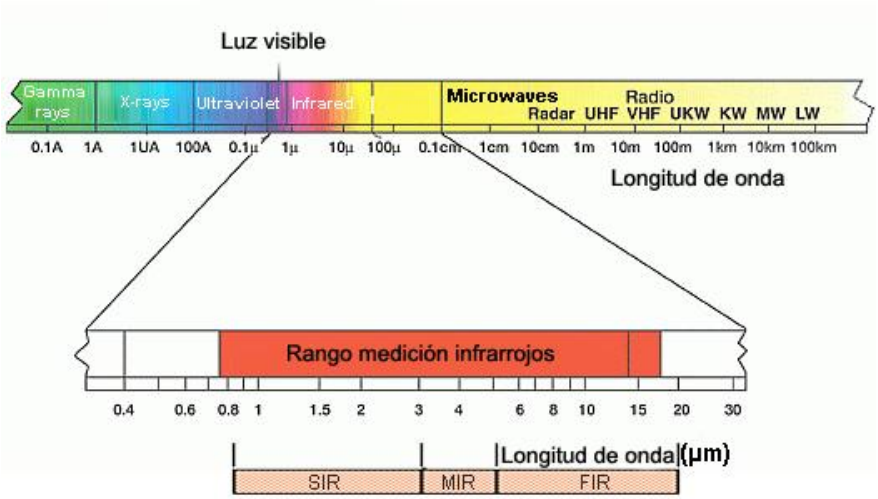

Figura 3.1.4.2.1. Espectro Electromagnético de la luz.
Fuente: http://www.academiatesto.com

3.1.5 El Futuro Y La Criptografía Cuántica

El futuro de la criptógrafa cuántica hasta el momento es incierto, todavía no se ha desarrollado este tipo de criptografía de tal forma que se pueda afirmar que es el método más seguro y confiable; a leves rasgos la criptografía cuántica muestra un gran desempeño y es aceptada sin mayores inconvenientes. Claro está que no se consideran temas de implementación y los valores económicos que esto conlleva. La criptografía cuántica es un método para salvaguardar nuestra información de una manera eficiente, ¿pero tiene un costo adecuado?; o es suficiente con las herramientas que la criptografía tradicional nos provee.

Más adelante se plantea abordar estos temas con el objetico de hacer una comparativa entre la criptografía cuántica aquí brevemente explicada y la criptografía tradicional que se conoce hasta el día de hoy.

Si hablamos de los dispositivos que nos permiten gozar de los beneficios de la criptografía este documento se haría muy extenso. En un breve resumen en la actualidad es posible proveer a cualquier dispositivo de las características necesarias para la utilización de la criptógrafa cuántica, la facilidad que la tecnología nos brinda para dotar a cualquier dispositivo tanto de hardware y como software es increíble pero una vez más ¿es

completamente necesario hacerlo? ¿Tiene un costo adecuado? o es suficiente con la criptografía tradicional y su desarrollo.

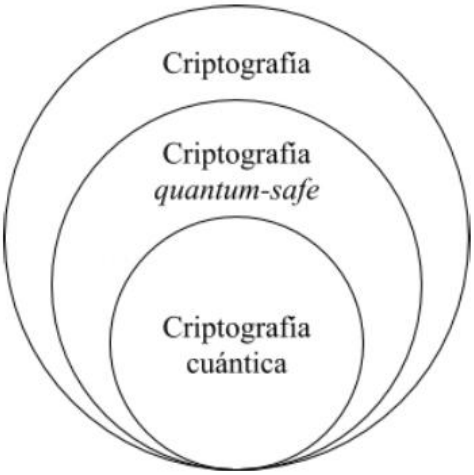

Figura 3.1.5.1 Tipos de criptografía. Fuente: S. Miguéns y P. Gonzalez, *Introducción a la Criptografía Cuántica.*

3.1.6 Comparativa De La Criptografía Cuántica Y La Criptografía Tradicional

La criptografía tradicional nos ha permitido proteger nuestra información de diferentes maneras haciendo uso de diferentes algoritmos matemáticos. Una consideración importa entre la criptografía cuántica y la criptografía tradicional es la cantidad de algoritmos que cada una maneja, por un lado, está la criptografía tradicional que con el pasar del tiempo ha podido desarrollar un sin número de métodos que nos permiten encriptar nuestra información; sin embargo, el mismo desarrollo matemático ha revelado varios métodos que nos permiten desencriptar esta información y vulnerar las seguridades informáticas.

Por otro lado, está la criptografía cuántica que nos muestra una ventana hacia el futuro haciendo uso de los conceptos básicos de la mecánica cuántica pero su desarrollo todavía está iniciando, no existe una gran cantidad de métodos como en la criptografía tradicional que nos permitan realizar la encriptación de la información; es más ni siquiera existe un método que nos permita encriptar la información a nivel cuántico.

En la criptografía cuántica como se ha visto en este documento lo único que se hace, a nivel cuántico, es la compartición de llaves utilizando el método más común y aceptado que es el QKD (Distribución de Llaves Cuánticas); la encriptación de la información se lo hace utilizando un método de la criptografía tradicional como por el ejemplo el RSA que es un método criptográfico de llave pública.

La figura 3.1.6.1 muestra un esquema sistemático general que recalca las diferencias entre la criptografía clásica y la criptografía cuántica de forma muy resumida para dar una idea a nivel general de cómo funcionan cada una de ellas.

Basándose en la criptografía tradicional la información es emitida en forma de bits que es la unidad de medida de la información, esta información es encriptada en el emisor utilizando un algoritmo matemático bien conocido y desencriptada en el receptor utilizando el mismo algoritmo matemático. Al saber con exactitud cuál es el algoritmo utilizado la información se vuelve vulnerable, esto no ocurre en la criptografía cuántica ya que no se conoce como fue encriptada la información en el emisor, por el principio de superposición cuántica, asegurando así la integridad de la información.

En cuanto a medios o canales de transmisión de datos se trata, no existen grandes diferencias, la criptografía tradicional también hace uso de la luz para transmitir la información.

La mayor diferencia radica en cómo es utilizada la luz, la criptografía tradicional utiliza la luz para transmitir la información mientras que la criptografía cuántica utiliza los fotones de luz para crear llaves o claves que son indescifrables. El proceso para encriptar y transmitir la información en la criptografía cuántica es el mismo que se utiliza en la criptografía tradicional.

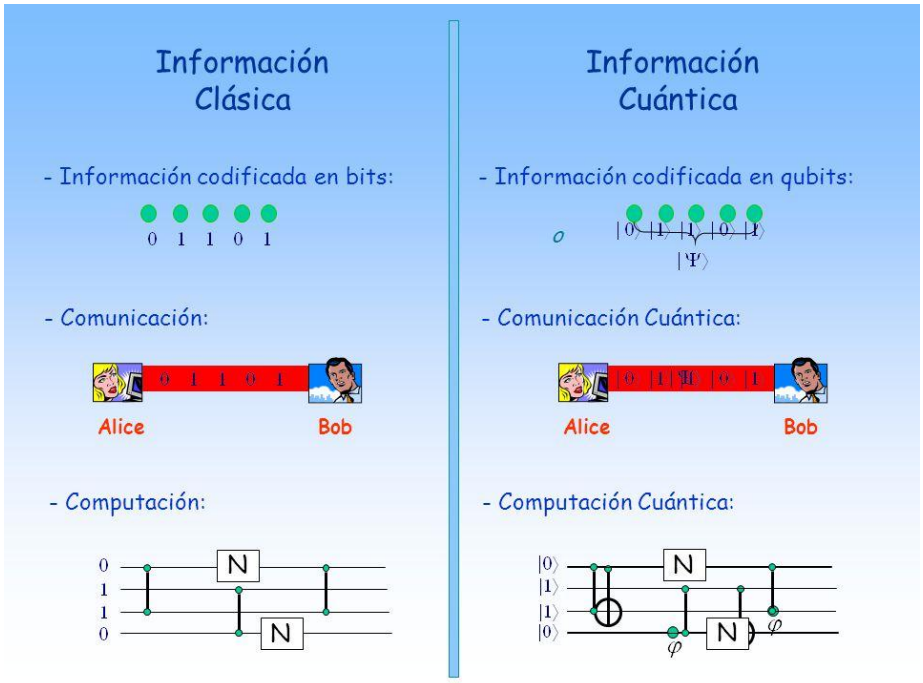

Figura 3.1.6.1 Criptografía cuántica vs criptografía tradicional. Fuente: https://slideplayer.es/slide/6162544/18/images/4

Los algoritmos matemáticos utilizados en la criptografía tradicional son predecibles, es decir, que el proceso y los resultados de cada algoritmo son calculables; sin embargo, estos procesos matemáticos no son nada fáciles de lograr y requieren de sistemas computacionales bastante avanzados para su ejecución.

Para la criptografía cuántica en cambio tenemos el principio de superposición cuántica que parte de varios estados desconocidos de los fotones, los estados iniciales de estos fotones son imposibles de conocer; de esta manera la criptografía cuántica hace que las llaves que se compartirán entre emisor y receptor sean completamente seguras.

De esta manera la criptografía cuántica se ha convertido en la forma más segura de proteger nuestra información, hasta el momento no se ha podido desarrollar un método que vulnere el principio de la superposición cuántica.

Existen puntos adicionales, resultado del proceso de desarrollo de este documento, que son necesarios mencionar para establecer un precedente de tal forma que puedan ser motivo de estudio en un futuro.

Se encuentra importante hacer una comparativa entre estos dos tipos de criptografía a nivel computacional, ya que es inevitable mencionar cómo es posible hacer para que una computara convencional logre trabajar a nivel cuántico. La respuesta a esta inquietud se la puede solventar mencionando que en la actualidad cualquier dispositivo computacional puede hacer uso de la mecánica cuántica implementado un hardware y software adecuado. La diferencia entre los computadores tradicionales y los computadores cuánticos radica principalmente en el poder de procesamiento, es decir, cuantas tareas por segundo son capaces de hacer; sin duda también una gran diferencia se tiene en que los computadores cuánticos son capaces de manejar los conceptos básicos de la física cuántica y todo el tratamiento que conllevan los fotones de luz utilizados.

Figura 3.1.6.2. Computador cuántico de Google. Fuente: https://cnnespanol.cnn.com

El computador cuántico desarrollado por Google tiene como objetivo ser 100 millones de veces más potente que un computar tradicional y actualmente se encuentra trabajando en la Nasa.

Otras de las inquietudes que surgen después de analizar un computador cuántico se refieren a su precio y su tamaño, un computar cuántico tiene un precio promedio de 15 millones de dólares y no son nada pequeños; aunque en algunas partes de este documento se menciona que cualquier computador es susceptible de implementarle tecnología cuántica esto se convierte en algo muy difícil y fuera de lugar por su precio y tamaño.

La tabla a continuación recoge los aspectos más importantes tratados en este documento con la finalidad de mostrar de forma clara y precisa la información; y compararla con la finalidad de cumplir el objetivo general.

Tabla 3.1.6.1 Tabla Comparativa

ASPECTOS GENERALES	CRIPTOGRAFIA TRADICIONAL	CRIPTOGRAFIA CUANTICA
Llaves	Públicas y Privadas	Públicas
Método de distribución de llaves	Depende del método de encriptación utilizado	Un solo método, denominado Distribución de Llaves Cuánticas
Encriptación de la información	Varios métodos para realizar la encriptación.	No se puede encriptar la información, lo único que se encriptan son las llaves
Fuentes que generan luz	Cualquier fuente de luz que trabaje con fibra óptica o aire libre	Fuentes de estados anunciados y fuentes de estados coherentes

Medio de transmisión	Cable UTP, fibra óptica, aire libre, etc.	Fibra óptica y aire libre
ASPECTOS RELACIONADOS		
Equipos o dispositivos computacionales	Dispositivos computacionales tradicionales	Dispositivos computacionales cuánticos
Costo	Bajo	Muy alto

Sin duda la criptografía cuántica es la más segura para salvaguardar cualquier tipo de información, ¿pero vale la pena implementarla? Desde el punto de vista del autor la criptografía cuántica todavía no alcanza el desarrollo necesario para poder migrar hacia ella, es una alternativa brillante que debe seguir desarrollándose y que sin duda en un futuro no muy lejano tomará su lugar y desplazará a los métodos tradicionales de criptografía.

3.2 Conclusiones

- Este documento cumple con el objetivo general planteado, es decir, se concluye que al realizar la comparación de varios aspectos desarrollados en páginas anteriores entre la criptografía tradicional y la criptografía cuántica; la criptografía cuántica es la más confiable y segura. Esto se debe al principio de superposición cuántica que hace inclonable las llaves que utilizan entre el emisor y receptor para encriptar la información.

- Así como la criptografía cuántica ha sido desarrollada para cifrar o encriptar la información es muy probable que en un futuro cercano esta misma tecnología se utilice para vulnerar la información. Este es un aspecto que se debe tener muy en cuenta para permanecer alerta e informados con la finalidad de superarlo o contrarrestarlo.

- La criptografía tradicional no se encuentra obsoleta ni mucho menos se puede pensar que llegó su fin, al contrario, la criptografía tradicional se mantendrá vigente por muchos años más gracias al desarrollo que ha obtenido a lo largo de su historia.

- Se afirma que la criptografía cuántica es la más segura, por el estudio realizado en este documento, pero el costo para implementarla es muy elevado. Por lo tanto, la criptografía tradicional sigue siendo la mejor opción para salvaguardar la integridad de nuestra información.

- El avance tecnológico, en todos los ámbitos, es abrumador por lo cual el futuro de la criptografía cuántica es bastante próspero y sin duda con el pasar del tiempo estará al alcance de todas las personas. Actualmente no existen en el mercado dispositivos computacionales cuánticos que estén disponibles al público, pero ya existen planes de varias empresas con respecto a esto.

- Es importante mencionar que los métodos criptográficos tradicionales que se manejan actualmente aún no han podido ser vulnerados a pesar de conocer con exactitud el algoritmo que tienen de base. El algoritmo más seguro hasta la fecha es el AES en sus diferentes versiones.

- La mecánica cuántica es una ciencia muy extensa y compleja, las leyes fundamentales de la física clásica no rigen este campo, por lo que es imprescindible analizar la información de tal forma que no se vuelva incomprensible para poder transmitirla de la forma más clara y concisa.

- Recolectar información de cualquiera sea el tema se puede convertir en un verdadero problema si no se estructura un plan. Descargar, conseguir o encontrar información de un determinado tema es relativamente sencillo, pero lograr que esta información recolectada se convierta en información útil es un verdadero reto. En este documento se utilizó información que se obtuvo después de realizar varios filtros para luego sintetizar los principales conceptos de tal forma que sea amigable para el lector.
- Temas derivados como costos y elementos computacionales cuánticos son importantes por cual fueron mencionados y analizados brevemente. Se abordó estos temas con la finalidad de dejar un precedente y una interrogante que permita en un futuro realizar un análisis y se obtenga algún tipo de resultado.
- La administración de los tiempos y la organización de las actividades en cualquier tipo de trabajo es una tarea compleja ya que es necesario definirlos y cumplirlos con exactitud de tal forma que el objetivo planteado se pueda cumplir.

3.3 Recomendaciones

- Dirigido a los lectores, se recomienda realizar un análisis con los temas derivados de este documento como lo fueron costos y dispositivos computacionales cuánticos de tal forma que se permita visualizar las ventajas y desventajas de cada uno de ellos.

- Dependiendo de las necesidades de cada persona o empresa se recomienda realizar un estudio que permita visualizar que tan factible es incorporar la criptografía cuántica en sus labores, ya que como se había mencionado en páginas anteriores los equipos para este fin son muy costosos y no están disponibles en el mercado.

- Es recomendable disponer de varias opciones en cuanto a metodologías se refiere e ir probando cada una de ellas con la finalidad de obtener la que más se acerque o cumpla con nuestras expectativas de trabajo.

- Se recomienda actualizar los conocimientos periódicamente con respecto a temas de seguridad informática en especial con relación a la criptografía cuántica porque como se mencionó en líneas anteriores la mecánica cuántica por el momento es nuestra aliada, pero quien sabe el día de mañana talvez sea un dolor de cabeza al vulnerar nuestra información.

- Finalmente se recomienda tener claro el panorama correspondiente a la criptografía cuántica, ya que, a pesar de ya tener varios años de desarrollo, todavía no se ve cerca su implementación al mundo; netamente se la utiliza con fines investigativos por el momento.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] M. Baig. *Criptografía Cuántica.* España: Universidad Autónoma de Barcelona. 2001.

[2] S. Miguéns y P. Gonzalez, *Introducción a la Criptografía Cuántica.* [Online]. Available: github.io

[3] F. Grasselli, *Quantum Cryptography*. Alemania: Heinrich Heine University Düsseldorf. 2020.

[4] R. Feynman., et al, *The Feynman Lectures on Physics*, Basic Books. Estados Unidos. 2010.

[5] W. Wootters y H. Zurek, *"A Single Quantum Cannot Be Cloned."* Nature, vol. 299, 2018

[6] Y. Zao, *"Quantum Cryptography in Real-Life Applications: Assumptions and Security."* Canada, Universidad De Toronto, 2009.

[7] I. López, *"Distribución cuántica de claves criptográficas"*. Ph.D. dissertation, Facultad de Ciencias Exactas, Universidad de Buenos Aires, Buenos Aires, AR, 2018.

[8] C. Hong and L. Mandel, *"Experimental realization of a localized one-photon state"*, Physical Review Letters.

[9] F. Mitschke, *Fiber optics: physics and technology*, Springer, 2016.

[10] Sheng-Kai , Liao, et al. *"Satellite-Relayed Intercontinental Quantum Network."* Physical Review Letters. 2018.

[11] REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.5 Online]. Available: https://dle.rae.es.