LA COMPUTACION CUANTICA Y LAS IMPLICACIONES SOBRE LA CRIPTOGRAFIA MODERNA.

MARTHA LUCIA LARA PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C, COLOMBIA
2019

LA COMPUTACION CUANTICA Y LAS IMPLICACIONES SOBRE LA CRIPTOGRAFIA MODERNA.

MARTHA LUCIA LARA PEREZ

MONOGRAFÍA

Proyecto de Grado para optar al título de:
Especialista en Seguridad Informática

Director de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C, COLOMBIA
2019

Nota de aceptación:

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C, de 2019

A Dios que guía siempre mis pasos y me da su luz en todo momento y a mi perro Rocco que ha sido mi fiel compañía en estos años.

Martha Lucia Lara Pérez

AGRADECIMIENTOS

Le doy gracias a Dios por siempre estar en los momentos más difíciles dándome su voz de aliento y a mis dos ángeles guardianes que me han protegido y brindado la amistad más sincera y noble que he podido tener en la vida, Dracco y Rocco

.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

En esta monografía se realiza un estudio sobre las implicaciones que la física cuántica realiza sobre la criptografía moderna, desarrollada sobre la metodología investigativa, tomando como base publicaciones especializadas sobre Física Cuántica. En ella se abordan conceptos sobre los sistemas de cómputo tradicionales, la criptografía moderna, su historia y los mayores aportes que ha hecho a la tecnología actual.

De Igual manera se resalta la importancia del desarrollo y la implementación de la computación cuántica y las ventajas en el aumento de la velocidad de análisis y transaccionalidad sobre los negocios actuales.

En el estudio monográfico también se abarca los fundamentos de la criptografía cuántica, como ha evolucionado con el pasar de los años, los estudios que se han realizado y las aplicaciones comerciales existentes. Este estudio monográfico está enfocado hacia los profesionales especializados en seguridad informática y al público en general que se interese en los temas de seguridad que ofrece la criptografía.

“La criptografía cuántica es una nueva área dentro de la criptografía que hace uso de los principios de la física cuántica para transmitir información de forma tal que solo pueda ser accedida por el destinatario previsto” [1]

[1] Textos Científicos. Criptografía cuántica - Conceptos de criptografía [En línea]. Disponible en: https://www.textoscientificos.com/criptografia/quantica

Con este estudio se pretende analizar el impacto de la criptografía cuántica en los procesos de las comunicaciones modernas, sirviéndose de las leyes de la naturaleza y aprovechando los estudios realizados sobre el principio de incertidumbre de Heisenberg y temas cuánticos desarrollados.

ABSTRACT

In this monograph a study will be made about the implications that quantum physics will make on modern cryptography, developed on research methodology, based on specialized publications on Quantum Physics. It will deal with concepts about traditional computing systems, modern cryptography, its history and the major contributions it has made to current technology.

Likewise, the importance of the development and implementation of quantum computing and the advantages in increasing the speed of analysis and transaction on current business will be highlighted.

This monographic study will also cover the basics of quantum cryptography, how it has evolved over the years, the studies that have been conducted and the existing commercial applications. This monographic study is focused on professionals specialized in computer security and the general public who are interested in the security issues offered by cryptography.

"Quantum cryptography is a new area within cryptography that makes use of the principles of quantum physics to transmit information in a way that can only be accessed by the intended recipient"

This study aims to analyze the impact of quantum cryptography on the processes of modern communications, using the laws of nature and taking advantage of studies conducted on the Heisenberg uncertainty principle and quantum issues developed.

INTRODUCCIÓN

Con el transcurrir del tiempo, la seguridad de la información ha tomado una gran importancia y de ahí que se realicen todos los procedimientos y métodos necesarios para asegurar que la transmisión de los datos a través de Internet sea totalmente seguro, para que esto se cumpla desde la antigüedad se han venido desarrollando una variedad de investigaciones todos enfocados en la encriptación, desde métodos rudimentarios hasta complejos logaritmos criptográficos, para esta monografía tomaré como base las investigaciones que se han realizados sobre la física cuántica y sus aplicaciones en la computación moderna y en los criptogramas.

Así mismo, tiene como fin dar un insumo a la comunidad académica y a los interesados, el material de investigación y las implementaciones que se han realizado hasta la fecha sobre la criptografía cuántica.

1. DEFINICIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad toda la información debe cumplir con los tres pilares de la seguridad, como lo son la confidencialidad, integridad y autenticidad, esto ha ocasionado que las organizaciones, hayan convertido toda la información en un bien valioso generando tareas específicas de seguridad en el área de TI, como la implementación de herramientas y métodos que permita mantener los pilares de la información.

Gracias a la necesidad de proteger la información, nacen varios sistemas de protección, entre ellos los criptográficos; estos sistemas de protección cuentan con algoritmos y funciones matemáticas que permiten “cifrar y proteger” la información y nos “asegura” que estas transmisiones son seguras entre el emisor y el receptor.

De esta manera podemos tener la “seguridad” de que los mensajes que transmitimos son seguros y fiables y si en algún punto de la comunicación son intervenidos o robados, esta información se convierta en ilegible y el atacante no logre decodificar el mensaje original. "El objeto de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación" [2]

Pero en la actualidad, esta “seguridad” se ha vuelto vulnerable y solo un pequeño grupo de sistemas criptográficos son considerados “seguros”, dentro de las pruebas

---

[2] . PABON, Jhonny, La criptografía y la protección a la información digital [En Línea]. Disponible en: https://www.minjusticia.gov.co/InvSocioJuridica/DboRegistros/GetPdf?fileName=La%20criptografia%20y%20la%20proteccion%20a%20la%20informacion.pdf.

encontradas de esas vulnerabilidades fue realizada en el 1998 por “La Electronic Frontier Foundation con una inversión de 210.000 dólares diseñó un computador capaz de realizar un criptoanálisis efectivo en un mensaje cifrado con sistema DES, el DES Cracker, mediante el sistema de búsqueda exhaustiva logró probar todas las claves en nueve días” [3]

Otro de los riesgos con los sistemas actuales es el criptosistema RSA, ya que es uno de los más utilizados nivel mundial y de los más seguros, su problema radica en la baja velocidad en encriptar datos de gran volumen, lo que nos hace pensar en otros sistemas criptográficos modernos, con otras capacidades de procesamiento, velocidad y con diferentes criptosistemas conocidos por los atacantes, “La criptografía cuántica, a diferencia de la criptografía clásica, resuelve los problemas de cifrado de los mensajes para ocultar la información, así como la distribución de la clave, donde cada bit puede estar en un estado discreto y alternativo a la vez; la unidad fundamental de almacenamiento es el bit cuántico, cada uno de los cuales puede tener múltiples estados simultáneamente en un instante determinado, con lo que se reduce el tiempo de ejecución de algunos algoritmos de miles de años a apenas segundos” . [4]

En la actualidad, estamos cerca a esta implementación cuántica, ya que un equipo de investigadores del MIT (Massachusetts Institute of Technology) y la Universidad de Innsbruck diseñaron y construyeron una computadora cuántica de cinco átomos, gracias a esta computadora y con la ayuda de pulsos láser, se implementó el algoritmo de SHOR, que puede considerarse como la llave maestra que permitiría

---

[3] CADAVID, Pabón, La criptografía y la protección a la información digital [En Línea]. Disponible en: http://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

[4] MOLINA, María, Criptografía Cuántica: Un Nuevo Paradigma [En línea], Disponible en: http://www.redalyc.org/pdf/4026/402640449006.pdf

abrir cualquier clave criptográfica, lo que nos hace pensar **¿QUÉ TIPO DE IMPLICACIONES TIENE LA COMPUTACIÓN CUÁNTICA SOBRE CRIPTOGRAFÍA MODERNA?**, cuantos cambios se podrán aplicar sobre nuestra información actual, en qué porcentaje aumentará la seguridad informática, como podremos protegernos antes este nuevo descubrimiento y lo más importante, nosotros estamos listos para este cambio.

2. JUSTIFICACIÓN

Con el nacimiento de la informática, la información ha evolucionado y se ha convertido en un factor de gran importancia en las organizaciones, esto debido a que en la actualidad necesitamos gran rapidez en las transacciones, con el uso del internet, los servicio ofrecidos en la nube, las nuevas tecnologías y los nuevos sistemas de información han hecho que las organizaciones cambien su negocio, la seguridad se haya convertido en la palabra clave y que los equipos de cómputo sean confiables, fiables y disponibles en todo momento para que salvaguarde la información que se ha convertido en uno de las activos más preciados.

Estos cambios han obligado a que las organizaciones presten más atención a la seguridad de la información, sin dejar de lado estar actualizados con la tecnología, se debe avanzar conociendo la importancia de la seguridad informática, de esta manera surgen los diferentes sistemas de protección como los firewalls, IDS, protocolos de conexión segura y la criptografía.

Esta monografía se realiza para entender el concepto de que, “La criptografía cuántica se presenta como la gran esperanza para la Ciberseguridad. En un campo en pleno crecimiento, el “salto cuántico” se vislumbra como la única posibilidad de convertir Internet en un lugar realmente seguro. Es la obsesión por la seguridad en la red la que está impulsando la Ciberseguridad como una de las materias con mayor proyección”[5].

[5] NEXT IBS, La criptografía cuántica, el futuro de la Ciberseguridad [En línea], Disponible en: http://www.nextibs.com/criptografia-cuantica-ciberseguridad/

Aunque esta información puede ser cierta, también es importante considerar el desarrollo del computador como una amenaza para la seguridad del mundo de la información ya que la criptografía moderna resultaría insegura y se podrían descifrar los criptosistemas actuales de cualquier organización como un banco, los sistemas de salud, ejercito, gobernación, la Nasa entre otro, en cuestión de milisegundos. “Desde el punto de vista de los investigadores en criptografía cuántica, después del advenimiento de los ordenadores cuánticos de altas prestaciones, si tales ordenadores llegan a construirse algún día, la criptografía convencional resultaría totalmente insegura. Estos afirman que los ordenadores cuánticos, junto con nuevos algoritmos de cálculo y búsqueda que exploten sus posibilidades, abreviarían dramáticamente las tareas de criptoanálisis[6].

Las comunidades en general desconocen que es imposible hacer que la seguridad informática se encuentre protegida al 100%, pero si es importante que las personas conozcan e identifiquen los nuevos métodos de protección de la tecnología y los beneficios que traería y las amenazas que esto generaría.

[6] MONTOYA, Fausto, La criptografía cuántica, ¿realidad o ficción? [En línea], Disponible en: https://www.researchgate.net/publication/255601730_La_criptografia_cuantica_realidad_o_ficcion1

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis de los beneficios de la computación cuántica aplicados a las técnicas criptográficas.

3.2 OBJETIVOS ESPECÍFICOS

- Describir de manera general la mecánica cuántica y los aspectos más importantes sobre su uso en la criptografía
- Documentar los aportes más importantes de la computación cuántica y los elementos que la constituyen.
- Realizar un análisis sobre la evolución desde los inicios de la criptografía cuántica y sus aspectos importantes.
- Presentar una infografía sobre la criptografía cuántica y sus principales ventajas.

4. ALCANCE Y LIMITACIONES

4.1 ALCANCE

La presente monografía es un proyecto de seguridad de la información y lo que pretende es analizar las implicaciones que tendría la criptografía con la aplicación de la física cuántica sobre la misma, basada en las publicaciones sobre la física cuántica utilizando la metodología investigativa.

4.2 LIMITACIONES

La presente monografía es un trabajo de investigación que se basará en las experiencias y resultados publicados por los especialistas, ya que al no contar con acceso a los centros de investigación no se podrán realizar las pruebas diseñadas para tal fin, por esta limitante no se incluirán.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES TEÓRICOS

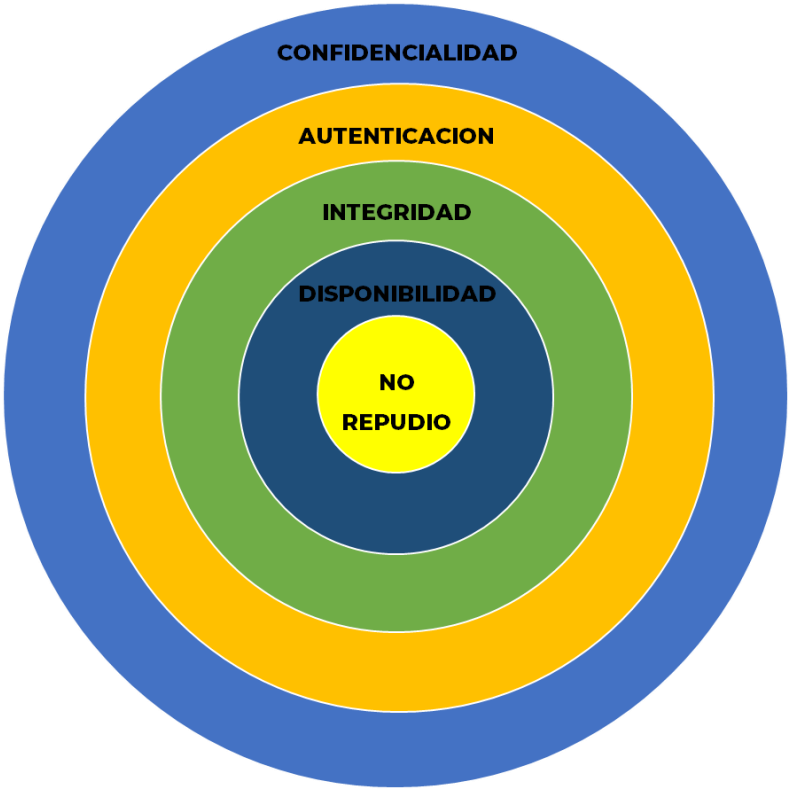
Con base al tema y el planteamiento expuesto es importante definir el concepto de seguridad informática, la seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

En síntesis, consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Al tener presente que debemos proteger nuestra información surge la necesidad de encriptarla, aunque se han implementado muchos protocolos de seguridad que garantizan que la conexión es segura, no estamos exentos a que una persona no autorizada logre conectarse y robarse nuestra información, la criptografía asegura que la información se encuentre “codificada” en el origen, esto hace que se requieran la aplicación de códigos y algoritmos precisos en el destino para que la información sea visible.

La criptografía es una disciplina que estudia los métodos que transforman los datos asegurando los cinco pilares fundamentales que se deben cumplir en la seguridad Informática, conocidos como CIDAN, como se muestra en la siguiente imagen.

Figura 1 Pilares de la Seguridad Informática



Fuente: Autor.

- **Confidencialidad**: Cualidad que debe tener cualquier archivo para que solo sea entendido y comprendido por la persona autorizada. En la confidencialidad se pueden aplicar técnicas de cifrado.
- **Autenticación**: Proceso de verificación de que un documento elaborado sea de la persona quien dice, del origen indicado y que no haya tenido modificaciones.
- **Integridad**: Cualidad de los archivos que garantiza que la información no ha sido alterada en el transcurso del envió y que además pueda ser verificado frente al archivo original.
- **Disponibilidad**: la información debe ser recuperada en el menor tiempo posible si ha sido robada.

- **No Repudio**: También conocida como irrenunciabilidad, este fundamento corresponde a la autenticidad del envió de información de terceras personas.

La criptografía "... el estudio de técnicas matemáticas relacionadas con aspectos de la seguridad de la información tales como la confidencialidad, integridad de datos, autenticación de entidades, y autenticación de origen de los datos. La criptografía no es el único medio de proveer seguridad de la información, sino un conjunto de técnicas"[7], en otras palabras, la criptografía se encarga de realizar un modelo con las instrucciones para que la información sea cifrada.

El criptoanálisis, está encargado de realizar la destrucción de estas instrucciones del cifrado para recuperar la información original, esto se realiza a través de criptosistemas o "llaves".

Los criptosistemas, son los procedimientos que permiten asegurar la información, son conocidas como las "llaves" o "claves".

Los criptosistemas se componen de:
T: Texto en claro: Información original la cual va a ser cifrada.
C: Texto cifrado: Información encriptada con un algoritmo de cifrado.

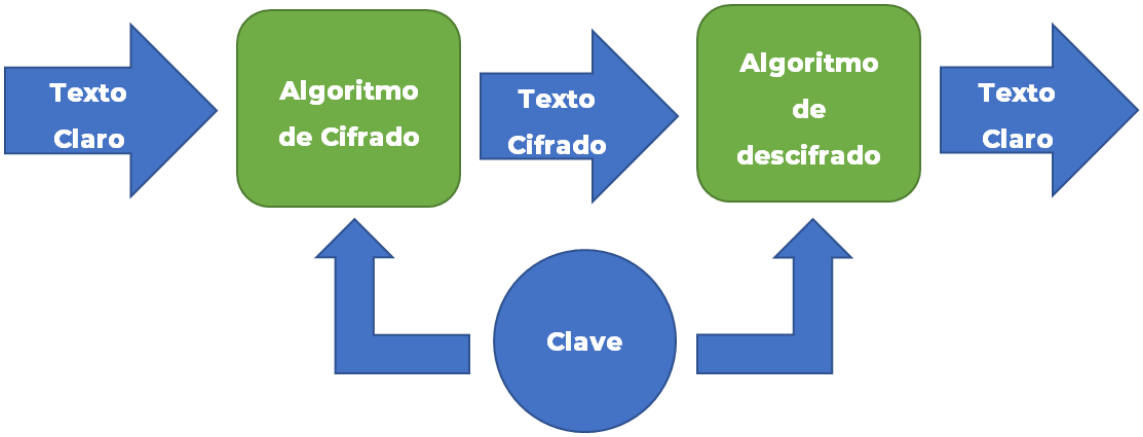
Algoritmos de cifrado.

El proceso de un criptosistema inicia con el texto claro, este texto contiene la información que se va a cifrar.
Este texto pasa por un algoritmo de cifrado y viaja por el canal ya codificado, una

[7] MENEZES, OORSHOT Y VANSTONE, Handbook of Applied Cryptography [En línea], Disponible en http://cacr.uwaterloo.ca/hac

vez llega al destino se decodifica con las claves correspondientes y se convierte nuevamente en texto claro, como lo muestra la siguiente imagen.

Figura 2 Muestra de un Criptosistema



Fuente: Autor.

5.2 MARCO HISTORICO

La criptografía es una disciplina bastante antigua desde el inicio de la escritura, las primeras civilizaciones iniciaron con el desarrollo de técnicas especiales para lograr enviar mensajes en las luchas militares. El primer método fue conocido como "Escítalo". El segundo fue un sistema de sustitución sobre las letras en una tabla. Los romanos utilizaron el sistema de sustitución conocido como César este “es un cifrado de sustitución mono alfabética. Este sistema consiste en desplazar el alfabeto una cantidad determinada de posiciones y alinearlo con el alfabeto sin desplazar”[8], los griegos utilizaron la “escítala espartana”, este método de trasposición se encontraba basado en un cilindro donde se enrollaba el mensaje y que contenía la clave.

[8] CORRALES, Héctor, Criptografía y Métodos De Cifrado [En línea], Disponible en: http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

En el inicio de la Primera Guerra Mundial sobre el año 1914 se realizaron varios cambios sobre las comunicaciones que permitieron cambiar las estrategias de combate y la transmisión de las comunicaciones, la transmisión de la información se realizó de forma segura y se utilizaron criptosistemas que hacían que la información fuera segura, intentar captar la información del enemigo y des encriptarla impulso el desarrollo de la matemática y la informática en este campo.

Después de la segunda guerra mundial, el aumento del desarrollo y del estudio monográfico de la criptografía, tanto en los investigadores como en la gente del común, ya que descubrieron que la codificación de las comunicaciones puede salvar la vida de muchas personas en el momento de estar en una guerra.

> Es importante tener en cuenta que la criptografía, se desarrolló por primera vez en vísperas de Primera Guerra Mundial, con el advenimiento de las comunicaciones por radio. Alcanzó gran importancia durante la II guerra Mundial, con los esfuerzos para romper el código alemán Enigma y el código púrpura japonés. Después de la guerra los EE.UU. creó la Agencia Nacional de Seguridad (NSA), como el principal código de decisiones y la agencia de descifrar códigos. Durante los años 50 y los años 60 era un tema de poca discusión. Durante la década de 1970 los avances tecnológicos en el procesamiento de información hacen de la criptografía un tema de importancia para la población civil, nace en las empresas la necesidad de proteger la información, que transfieren electrónicamente de un sitio a otro. El siguiente acontecimiento importante fue la criptografía "clave pública", que tomó a la NSA un tanto por sorpresa. El uso de cifrado de clave pública tiene aplicaciones comerciales obvias (por ejemplo, se permite el uso de "firmas digitales" para autenticar mensajes), pero con poca aplicación militar. En 1977 se desarrolló el esquema de clave pública RSA para hacer frente a este nuevo desarrollo.[9]

Con la creación del primer computador moderno ENIAC “se empezaron a convertir los mensajes en códigos binarios, es decir en ceros y unos, utilizando protocolos,

---

[9] RIVEST, Ronald, Cryptography and the Limits of Secrecy [En línea]. Disponible en: http://web.mit.edu/ssp/seminars/wed_archives99fall/rivest.pdf

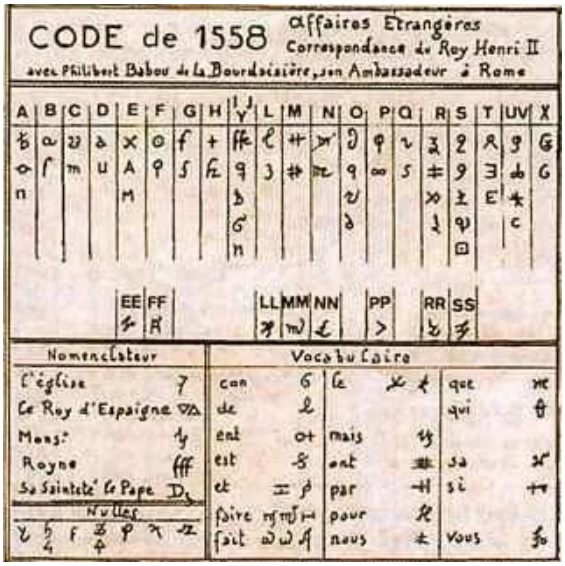
como el ASCII. Cada letra de cada palabra para su transmisión se convierte en series de ceros y unos, a los cuales para cifrar el mensaje se les aplica el criptosistema"[10]

En los años 70, operaba el esquema de clave privada, en el cual el emisor y el receptor debían tener la misma clave, el emisor la utilizaba para cifrar el mensaje y el receptor para descifrarla este sistema de criptografía no garantizaba la autenticidad del mensaje. Este sistema utiliza dos operaciones fundamentales: la sustitución y la permutación, estas dos operaciones han sido los métodos utilizados en la mayoría de las antiguas civilizaciones.

La sustitución consiste en establecer una correspondencia entre los símbolos del alfabeto en el que está escrito el mensaje original y otro alfabeto, de esta manera las letras del texto origen, es sustituido por un símbolo del otro alfabeto para elaborar el criptograma, cuando el destinatario recibía el mensaje, cambiaba los símbolos por letras para decodificarlo, un ejemplo de este método es el cifrado de Babeó.

[10] CADAVID, Pabón, La criptografía y la protección a la información digital [En Línea]. Disponible en: http://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

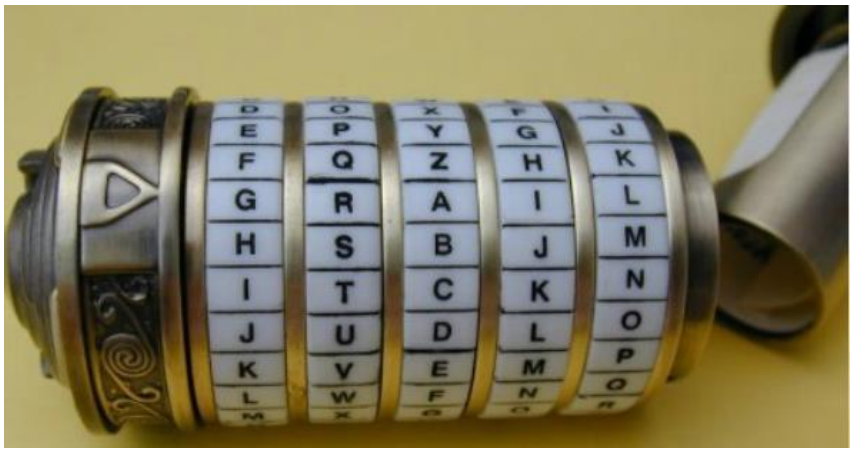
Figura 3 Cifrado utilizado por Babeó, cifrado por sustitución



Fuente: [Fotografía], Cifrado Babeó [Consultado: 01 de noviembre de 2018] Disponible en internet: https://earchivo.uc3m.es/bitstream/handle/10016/6173/PFC_Patricia_Xifre_Solana.pdf?sequence=1

El método de la transposición, consistía en entremezclar algunos símbolos del mensaje original, lo que ocasionaba que el texto no fuera claro para cualquier persona, solo podía ser descifrado por el receptor con los conocimientos de transposición, que ubicaba los símbolos mezclados en su posición original. Este método de cifrado por transposición en la actualidad puede ser aplicado en escribir al revés las palabras, a continuación, la imagen de un equipo de transposición.

Figura 4 Muestra de un equipo que utiliza la Transposición



Fuente: [Fotografía]**,** Transposición método de cifrado [Consultado: 01 de noviembre de 2018] https://aminoapps.com/c/investigacion_amino/page/blog/transposicion-metodo-de-cifrado/4pwb_kBTYulaGYYaKVBDPz2ojX12mnXon

Algunos ejemplos históricos del cifrado por sustitución:

Cifrado de César: Este cifrado consistía en "sustituir la primera letra del alfabeto por la cuarta; la segunda por la quinta, y así sucesivamente con todas las demás estableciendo un ciclo con las últimas letras. Los términos matemáticos y un ejemplo ya están expuesto en un apartado anterior. La debilidad de este método radica en que la frecuencia de aparición de cada letra en el texto en claro se refleja exactamente en el criptograma.

Conociendo la letra de mayor frecuencia en el tratamiento utilizado, queda automáticamente establecida la correspondencia."[11]

[11] XIFRE, Patricia, Antecedentes y perspectivas de estudio en historia de la Criptografía [En línea], Disponible en: http://www.cnv.gob.ar/infoadicional/rsafaq.htm

5.3 CRITPOGRAFIA MODERNA

Dos acontecimientos importantes cambiaron el curso de la criptografía, uno de ellos fue el estudio que realizo Claude Shannon con la teoría de la información y la criptología, en esta define un marco de trabajo y de matemáticas donde propone convertir las imágenes, los sonidos a dígitos binarios (0 y 1) y que sean transmitidas por cualquier medio de comunicación, reduciendo el ruido o corrigiéndolo, de esta manera al llegar al destinatario se convertiría nuevamente los códigos binarios en la información enviada, por estos y más contribuciones a Shanon se le considera el padre de las comunicaciones digitales.

En el campo de la criptografía, también realizo importantes aportes uno de ellos es el documento “Communication Theory of Secrecy Systems en el año 1949, donde “establece una base teórica para la Criptografía y para el criptoanálisis y define las estructuras matemáticas básicas de los sistemas de seguridad”[12]. Con este nuevo documento de Shannon la criptología es considerada como una de las ramas de las matemáticas y deja de estar rodeada de escepticismo y misterio.

El siguiente acontecimiento importante en la historia de la criptología fue la publicación de un ensayo realizado por Whitfield Diffie y Martin Hellman en el año 1976 que marca un antes y un después de la clave pública, este ensayo lleva por nombre New Directions in Cryptography, en el que proponen el cifrado asimétrico. “Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring lOloo

[12] MARTÍNEZ, Evelio, Claude Shannon: el padre de la teoría de la información [En línea], Disponible en: http://www.eveliux.com/mx/Claude-Shannon-el-padre-de-la-teoria-de-la-informacion.html

instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D”[13].

Este concepto de asimetría consiste básicamente en tener que el receptor tenía ahora dos claves, una publica (Puede ser conocida por todo el mundo) y una privada, las dos claves son distintas, pero con la ayuda de las matemáticas, el mensaje se cifra con la clave pública y solo se descifra con la clave privada.
La seguridad cambia radicalmente con el uso de estas dos claves, ya que, si se intentaba descifrar el mensaje con la clave privada, el mensaje sería totalmente incomprensible. La distribución de estas claves era segura ya que el emisor del mensaje difundía la clave pública y se la enviaba al receptor.

A continuación, un ejemplo del envió de un mensaje utilizando la criptografía simétrica.

Figura 5 Diagrama del funcionamiento de la Criptografía Asimétrica

Fuente: [Fotografía], Criptografía Asimétrica [Consultado: 01 de noviembre de 2018] Disponible en internet:

[13] DIFFIE, whitfield and HELLMAN, martin, New Directions in Cryptography [En línea], Disponible en: https://ee.stanford.edu/~hellman/publications/24.pdf

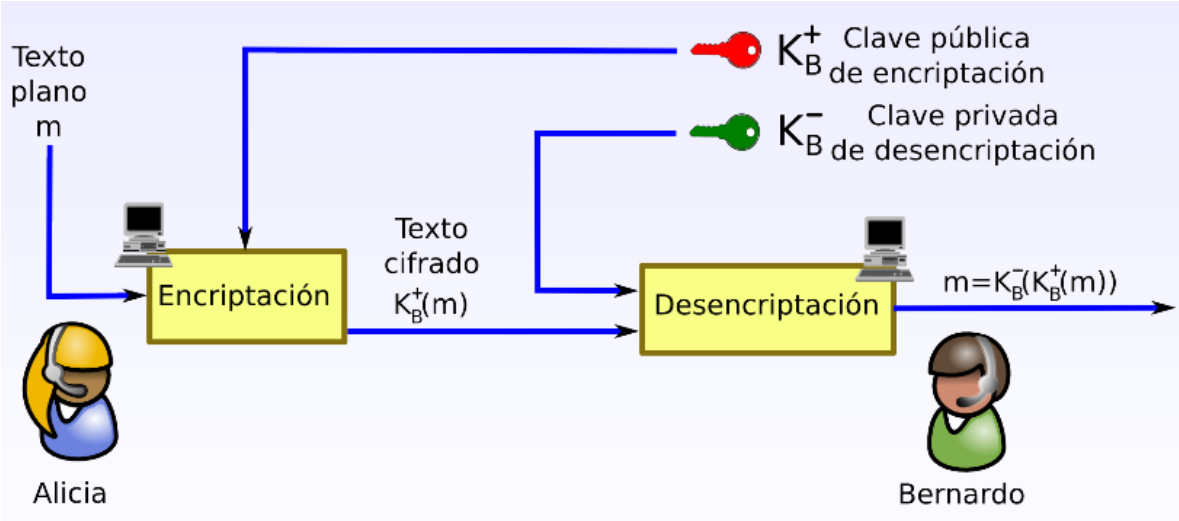
https://ethicalhackneox.wordpress.com/2015/09/29/criptografia-llaves-publicas-y-privadas-tarea-3/

Con estas bases realizadas por Diffie y Hellman, se desarrolló el sistema uno de los criptosistemas de clave pública más utilizados en la actualidad el RSA, inventado en 1978 por Ronald Rivest, Adi Shamir y Leonard Adleman, el criptosistema está basado en la *factorización* de enteros "Funciona de la siguiente manera: se toman dos números primos grandes, p y q, y se calcula su producto n = pq; n se denomina módulo. Elija un número e, menor que n y primo relativamente de (p-1) (q-1) y halle el inverso d, mod (p-1) (q-1), que significa que de = 1 mod (p-1) (q-1); e y d se denominan el exponente público y privado, respectivamente. La clave pública es el par (n, e) y la privada es d. Los factores p y q deben mantenerse en secreto o ser destruidos.[14]

A continuación, un ejemplo del funcionamiento del criptosistema RSA en la transmisión de un mensaje.

Figura 6 Diagrama del funcionamiento de RSA

[14] FAHN, Paul, Respuestas A Las Preguntas Más Frecuentes Sobre Criptografía Actual [En línea], Disponible en: http://www.cnv.gob.ar/infoadicional/rsafaq.htm



Fuente: [Fotografía], Historia y definición de sra, md5, sha1 y sha2 [Consultado: 01 de noviembre de 2018] Disponible en internet: https://www.mindomo.com/mindmap/algoritmo-rsa-3bd2e41be346485a8d76fa4a3eb2ce86

5.4 MARCO TEORICO

La física cuántica es compleja, aunque entendiendo dos conceptos clave, podemos socializarnos más fácil a ella. “El primer concepto clave es el que propuso Schrödinger con su famoso experimento mental: El gato de Schrödinger. Un gato que está encerrado dentro de una caja en la que hay un veneno mortal que tiene un 50% de posibilidades de abrirse, sin saber si se ha abierto el veneno, ¿está vivo o está muerto? La física cuántica nos dice que el gato se encuentra vivo y muerto a la vez, en un estado de superposición, hasta que se abra la caja.”[15]

El segundo concepto, Principio de Incertidumbre de Heisenberg, “Para las cosas pequeñas, desde electrones, hasta partículas subatómicas o fotones, la incidencia

[15] NEXT IBS, La Criptografía Cuántica, El Futuro De La Ciberseguridad [En línea], Disponible en: http://www.nextibs.com/criptografia-cuantica-ciberseguridad/

de la observación resulta clave. Al intentar observar una partícula de este tipo, resulta físicamente imposible determinar su velocidad y su posición al mismo tiempo, ya que para observarla deberías impactar fotones que variarían su velocidad y trayectoria."[16]

5.4.1 Principio de incertidumbre de heisenberg

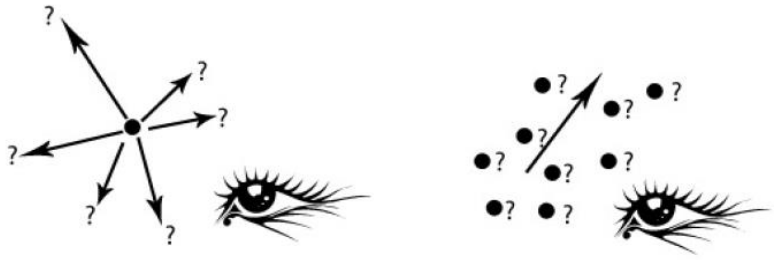
Werner Heisenberg en el año 1927, descubrió un principio fundamental de la mecánica, "El hecho de que cada partícula lleva asociada consigo una onda, impone restricciones en la capacidad para determinar al mismo tiempo su posición y su velocidad"[17],, Heisenberg indica que algunas de las propiedades físicas se encuentran relacionadas, de esta forma cuando queremos alguna información sobre una propiedad, disminuye la información de otra.

Como lo podemos visualizar en la imagen, cada vez que nos enfocamos en un objeto perdemos la relación de los demás objetos.

[16] NEXT IBS, La Criptografía Cuántica, El Futuro De La Ciberseguridad [En línea], Disponible en: http://www.nextibs.com/criptografia-cuantica-ciberseguridad/

[17] LOPEZ, Juan Carlos, El Principio De Incertidumbre De Heisenberg [En línea], Disponible en: https://www.nucleares.unam.mx/~vieyra/node20.html

Figura 7 Principio de incertidumbre de Heisenberg



Fuente: [Fotografía], El principio de Incertidumbre de Heisenberg [Consultado: 01 de noviembre de 2018] Disponible en internet: https://www.nucleares.unam.mx/~vieyra/node20.html

Entropía de Von Neumann

Esta entropía es referida como una propiedad del sistema que se puede medir, por ejemplo, la energía o posición si conocemos el estado de cierta partícula del sistema cuántico y se calcula con la siguiente formular:

$$S(\rho) = -\mathrm{tr}(\rho \log \rho),$$

Donde tr, significa la traza de la partícula. [18]

5.4.2 Mecánica cuántica

La física cuántica es un modelo que nos permite realizar una descripción del comportamiento que realizan las partículas subatómicas. Con la física cuántica se

[18] QUEZADA, Roberto, Entropía Relativa De Von Neumann [En línea], Disponible en: http://www2.izt.uam.mx/newpage/contactos/revista/90/pdfs/entropia.pdf

verifica a niveles microscópico ya que estas toman otro compartimento diferente a lo observado a nivel macroscópico.

A nivel macroscópico gracias a las leyes de Newton, podemos realizar experimentos que nos permiten visualizar el comportamiento de estas partículas, como por ejemplo podemos seguir una trayectoria de una pelota de futbol, pero gracias a la física cuántica podemos capturar niveles que no son percibidos por nuestros sentidos, como por ejemplo polarizar un fotón o el movimiento de un electrón. La diferencia de los niveles de revisión tanto microscópicos como macroscópicos nos permite visualizar en detalle los movimientos y comportamientos a niveles superiores.

Los fundamentos de la física cuántica se establecieron en el año 1924 por el científico Louis de Broglie, quien notifico al mundo el término de partícula "muy pequeña" que es entendido por el tamaño ya que en estas escalas se notan diferentes efectos que imposibilitan conocer la posición y la velocidad que lleva esta partícula, estos son conocidos como "efectos cuánticos". La mecánica cuántica describe los movimientos y las interacciones que realizan las pequeñas partículas.

5.4.3 Polarización de un fotón

Los fotones son considerados como un medio por el cual se transporta la información cuántica en escalas grandes de distancia, estas partículas sin masa, sin carga eléctrica, se mueven a la velocidad de la luz.

Los fotones son campos electromagnéticos que trabajan perpendicularmente a la dirección en la que se propagan, los fotones se mueven sobre el eje Z.

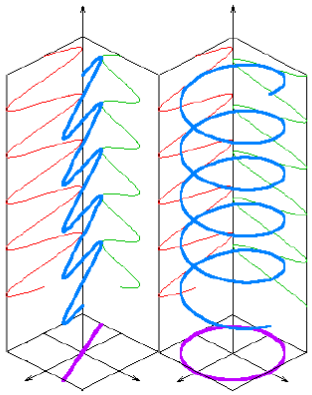
La criptografía cuántica utiliza esta propiedad específica de los fotones (polarización) para codificar el bit y se refiere al plano en el que se mueve el fotón

en el campo eléctrico.

Cabe destacar que el hecho de que el electrón tenga espín implica que debería estar hecho de cargas girando, pero la física actual no se pronuncia sobre este hecho, quedando relegado a teorías de nueva física.

A continuación, como podemos visualizar los patrones de polarización son posibles oscilaciones en el plano perpendicular.

Figura 8 Polarización circular de un fotón



Fuente: [Fotografía], Polarización de fotones [Consultado: 02 de noviembre de 2018] Disponible en internet: http://www-revista.iaa.es/content/%C2%BFondas-gravitatorias-primordiales

5.4.4 Qubits

La computación cuántica opera como estados de polarización de un fotón, este término qubit fue introducido por primera vez por Benjamín Schumacher en los años 90 y se pronuncia “ket φ “.

Como se puede ver en la imagen, la polarización de los fotones se encuentra en

varios estados que se representan de la siguiente manera:

Figura 9 Estados de polarización de un fotón

ESTADO	POLARIZACION RECTILINEA	POLARIZACION DIAGONAL
Polarizado en 0° o 45°		
Polarizado en 90° o 135°		

Fuente: Autor.

“Matemáticamente, “un qubit (bit cuántico) es un estado cuántico φ =α 0 +β 1 donde α, β ∈□ y 2 2 α + β =1”. Al hacer la medición del qubit, se obtiene 0 con probabilidad 2 α y 1 con probabilidad 2 β”[19]

5.4.5 Teorema de no-clonación

Este teorema es importante para la criptografía cuántica ya que nos demuestra que es imposible copiar los estados cuánticos que se estén enviando en una comunicación por el emisor y el receptor lo que asegura que un tercero si llegara a interceptar la transmisión no podría descifrar el mensaje, lo que hace a la criptografía cuántica indescifrable.

[19] ROJAS, Hernan, Fundamentos De Criptografía Cuántica [En línea], Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/2367/OrtizRojas_Hernan_2007.pdf;sequence=1

Lo que enuncia este teorema es que no puede copiarse un estado cuántico y que este sea exacto.

> Consideramos que el estado del sistema a copiar viene dado por un ket de estado $|\alpha\rangle$. Disponemos un sistema físico idéntico al primero en el cual tenemos la intención de copiar el estado del primer sistema. El inicial estado de este segundo subsistema, $|\beta\rangle$, no nos interesa, lo único que nos interesa es que el estado final del sistema en su conjunto sea de la forma $|\alpha\rangle \otimes |\beta\rangle$.
>
> Consideremos una base de estado $|a_i\rangle$, según la cual podemos descomponer el estado a copiar,
>
> $$|\alpha\rangle = \sum_i a_i |a_i\rangle \ .$$
>
> El procedimiento de copiado vendrá representado mediante un operador U unitario y lineal. Si el procedimiento de clonado ha de funcionar, el operador U debe ser capaz de duplicar los vectores de la base,
> $U |a_i\rangle \otimes |\beta\rangle = |a_i\rangle \otimes |a_i\rangle \ .$
>
> Veamos, pues, el resultado de aplicar el operador de clonado al estado completo.20
>
> $$\begin{aligned} U |\alpha\rangle \otimes |\beta\rangle &= \sum_i a_i U |a_i\rangle \otimes |\beta\rangle \\ &= \sum_i a_i |a_i\rangle \otimes |a_i\rangle \ . \end{aligned}$$

La computación cuántica, nos permite explotar las propiedades de la materia a escalas demasiado pequeñas para realizar operaciones lo que permitirá que las operaciones fueran mucho más rápidas que la de los computadores tradicionales, realizar un crecimiento exponencial de procesamiento de datos como lo hace una supercomputadora en la actualidad. La construcción de los computadores cuánticos se ha enfocado en la utilización de fotones (partículas de luz) atrapados en el campo

---

[20] TARRIO, Javier, Teorema De No Clonado [En línea], Disponible en: http://www.lawebdefisica.com/dicc/noclonat/

eléctrico, lo que permite aprovechar la propiedad de " superposición ", ya que se puede aprovechar una partícula cuántica en varios estados.

En la computación cuántica este gran procesamiento de información puede ser aplicado en el mejoramiento de respuesta en las bases de datos, ya que se reducirían los tiempos de realizar una consulta dentro de millones de registros, también puede ser aplicado en la precisión de los cálculos para predecir fenómenos biológicos y químicos en menor tiempo.

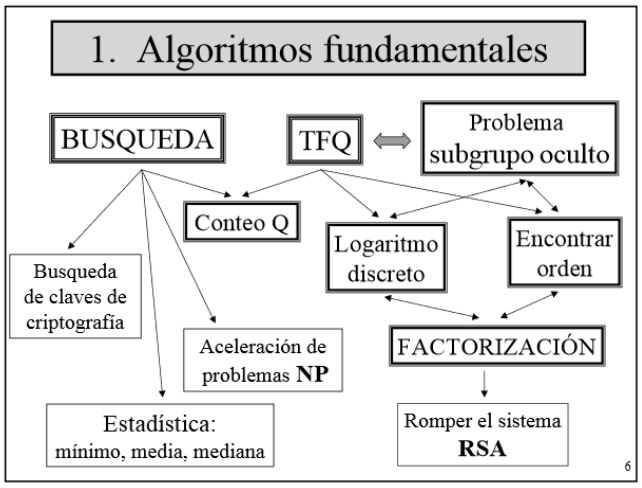
La computación cuántica incrementará la velocidad del procesamiento gracias a los QKD, de las siglas quantum key distribution, una de las grandes ventajas será la distribución de la clave cuántica, ya que el comportamiento de las partículas cuánticas nos garantizará que ninguna persona puede interferir en una comunicación privado sin que pase desapercibido.

“QKD (distribution): BB84, B92, etc. Sistemas de clave secreta (simétrica). Realmente QKG (growing), ya que se requiere autenticación.”[21]

Existen muchos algoritmos que se basan en la física cuántica, los dos algoritmos más importantes para el mundo cuántico son el algoritmo del orden y el algoritmo utilizado para factorizar, estos dos algoritmos se basan en la Transformada de Fourier Cuántica, un resumen de estos algoritmos se visualiza en la imagen.

[21] LANCHO, Daniel, Criptografía Cuántica Aplicada [En línea], Disponible en: http://gicc.fis.ucm.es/teaching/master/SeminarioUCM-19Ene07-web.pdf

Figura 10 Resumen de los algoritmos fundamentales de la cuántica



Fuente**:** [Fotografía], Algoritmos fundamentales de la cuántica [Consultado: 02 de noviembre de 2018] Disponible en internet: https://francis.naukas.com/2008/05/06/lenguajes-de-alto-nivel-para-la-computacion-cuantica-o-computacion-cuantica-para-informaticos/

El algoritmo de factorización fue presentado en el año 1994 por Peter Shor, este algoritmo conocido como el algoritmo SHOR algoritmo polinomial plantea una solución para el problema de factorizar enteros: "Dado un número entero impar N, encontrar un factor propio de N[22]"

Este algoritmo es importante para la computación cuántica ya que demostró que con la ayuda de un computador cuántico se realizan cálculos para factorizar números muy grandes en periodos cortos, es decir pasaría de millones de años a cuestión de segundos.

[22] CARREÑO, Juan, Algoritmo De Factorización De Shor [En línea], Disponible en: http://www.dma.eui.upm.es/MatDis/Seminario4/AlgoritmoShor.pdf

El riesgo que pone este algoritmo, con la criptografía cuántica es sobre RSA ya que al ser implementado este computador la función de factorizar con RSA quedaría vulnerable y podría llegar a decodificar millones de archivos en menos tiempo.

La Criptografía cuántica está basada en las propiedades de la interacción entre las partículas subatómicas, en la superposición paralela de dos estados de una sola partícula subatómica, gracias a esta propiedad se realizan los desarrollos teóricos de los algoritmos cuánticos, lo que permite tener una capacidad de procesamiento exponencial.

La criptografía cuántica utiliza más la física que la matemática para crear sus criptosistemas, lo que hace que los códigos encriptados sean casi imposibles de decodificar, ya que se crearía una "clave cuántica" conformada por qubits (En la cuántica, no existen los bits binarios (unos y ceros) ya que lo que observamos puede ser modificado en su estado, por eso existen los qubits, conformados por varios estados de los unos y ceros), si algún atacante quisiera observar la clave (esta clave viaja por fotones a través de la fibra óptica), los fotones cambiarían de estado y la clave que conseguirían no sería la misma que la clave original, esto nos puede ayudar a verificar si se ha tratado de acceder a la comunicación.

"La criptografía cuántica, se basa en el uso de partículas/ondas luminosas (fotones) individuales y sus propiedades cuánticas intrínsecas, para desarrollar un criptosistema inquebrantable (porque es imposible medir el estado cuántico de cualquier sistema sin perturbarlo)."[23]

[23] BANAFA, Ahmed, ENTENDER LA CRIPTOGRAFÍA CUÁNTICA [En línea], Disponible en: https://www.bbvaopenmind.com/entender-la-criptografia-cuantica/

Como es bien conocido, la criptografía cuántica es una evolución del criptosistema Vernam, este criptosistema fue desarrollado por Joseph Mauborgne y Gilbert Vernam en 1920 aproximadamente, es utilizado ampliamente en las comunicaciones que implementan las fuerzas militares, esto debido a que su seguridad puede ser demostrada gracias a las matemáticas.

Este sistema utiliza una “cinta” con una secuencia aleatoria de números binarios (1-0), que se agrega al mensaje final que también es convertido en binario, módulo 2 (XOR). Cuando llega el mensaje al receptor este también cuenta con una “cinta” idéntica, se realiza un proceso de la sumatoria de los mensajes cifrados y así se decodifica el mensaje original, para realizar una decodificación sin las cintas apropiadas tardaría alrededor de millones de años.

Figura 11 Representación gráfica del criptosistema Vernam

Fuente: Autor.

Una de las ventajas que tiene la aplicación de la criptografía cuántica, es él envió de la clave o “cinta” ya que esta se realizaría por una transmisión fotónica (por fibra óptica) y no a través de correo seguro, lo que significa que realiza una distribución cuántica de cintas o claves, como sus siglas quantum key distribution (QKD).

> “Los criptosistemas de clave pública, basados en la dificultad de factorizar números enteros grandes o en hallar su logaritmo discreto, pueden ser rotos, con los actuales ordenadores convencionales, en un periodo de tiempo exponencialmente creciente con el número de dígitos del número. Pero mediante un ordenador cuántico, que ejecutase el algoritmo de factorización propuesto en 1994 por Shor, de los laboratorios AT&T Bell,

> este tipo de problemas se podrían resolver en un período de tiempo creciente solamente cuadráticamente con el número de dígitos del número”[24]

De esta manera, es posible asegurar que descifrar un mensaje en clave cuántica resulta literalmente imposible de descifrar.

[24] MONTOYA, Fausto, La criptografía cuántica, ¿realidad o ficción?... ([En línea], Disponible en: https://www.researchgate.net/publication/255601730_La_criptografia_cuantica_realidad_o_ficcion1.

5.5 ESTADO ACTUAL DE LA CRIPTOGRAFIA

Actualmente el sistema RSA tiene una gran expansión y puede ser utilizado por varios años más, es utilizado por una gran variedad de plataformas en el mundo, este sistema criptográfico está incluido en varios sistemas comerciales como Microsoft, Apple, Sun y Novell y es aplicado para muchos organismos estatales estadounidenses, grandes compañías, laboratorios y universidades, también es aplicado a las conexiones https y los servicios de la nube.

Las aplicaciones de la criptografía de clave pública son:

Autenticación del mensaje: Los mensajes deben ser fiables, es decir, los mensajes deben tener la seguridad de que no pueda modificarse ninguna parte del contenido.

Identificación del usuario: A través de las autoridades de certificación (CA), se expiden certificados donde se valida el proceso de las claves, de este modo se puede asegurar la garantía de la clave pública.

Como hemos verificado los sistemas de cifrado actuales se basan en operaciones matemáticas, que básicamente ocultan el mensaje original hasta que el destinatario aplique las claves correctas y descubre el mensaje. Uno de los riesgos es que en el transcurso de la información las claves pueden ser interceptadas sin que el destinatario o el emisor lo descubran. “La criptografía cuántica supera en teoría ambas limitaciones, ya que la información se sitúa en las partículas de luz o fotones que son emitidos, de uno en uno, en un estado previamente conocido por el destinatario, quien de esta forma puede recuperar el mensaje, si uno de los fotones es interceptado, su estado queda alterado y el receptor detecta el ataque al

mensaje."[25]

La factorización es un factor importante en la criptografía moderna (RSA), y el tiempo en que requeriría el realizar la factorización se estima en aproximadamente 4x1016 años y se estima que con los algoritmos cuánticos esta factorización se realizaría en cuestión de segundos.

La criptografía actual tanto de llave pública como de llave privada (RSA o clave Diffie y Hellman) pueden recibir ataques o intentos de des-encriptamiento no autorizado, aunque los hackers encuentran en la factorización de números un problema grande, estos problemas con la computación cuántica podrían ser resueltos y decodificar la información del mensaje en menor tiempo.

Lo que nos puede llegar a hacer pensar la importancia de desarrollar nuevos métodos que nos permita asegurar las comunicaciones con la aplicación de nuevos algoritmos de encriptación cuántica.

[25] MOLINA, María, Criptografía Cuántica: Un Nuevo Paradigma [En línea], Disponible en: http://www.redalyc.org/pdf/4026/402640449006.pdf

6. DISEÑO METODOLOGICO

La metodología de este trabajo es investigativa con el fin de conocer y divulgar las implicaciones que la criptografía cuántica traerá a la tecnología actual. En ella se abordarán conceptos sobre los sistemas de cómputo tradicionales, la criptografía moderna, su historia y los mayores aportes que ha hecho a la tecnología, tomando como base publicaciones especializadas sobre Física Cuántica, entrevistas y videos científicos.

Dicha investigación se desarrolló sobre una pregunta central del cual se desglosan los objetivos generales y específicos que se persiguen solucionar en la investigación.

Para el desarrollo de la presente monografía se llevó a cabo varias lecturas científicas, videos sobre física cuántica, entrevistas a empresas tecnológicas que me permitieron obtener información importante sobre el tema tratado.

Con la información obtenida sobre esta investigación se realizó la monografía.

7. ASPECTOS DE LA CRIPTOGRAFÍA CUANTICA.

La mecánica cuántica es una base importante de la física y del conocimiento humano ya que explica el comportamiento tanto de la materia como de la energía. Con la aplicación se han realizado grandes descubrimientos y desarrollos a nivel tecnológico como los transistores.

La mecánica cuántica básicamente nos da una explicación sobre la existencia del átomo y la estructura atómica que la física clásica no puede explicar en detalle.

La mecánica cuántica es un modelo con el que se puede especificar de manera detallada la conducta natural de las partículas subatómicas, esto se realiza con el fin de visualizar lo que sucede en realidad a niveles microscópicos, como se comportan las partículas viéndolas desde un nivel más detallado que lo que se visualiza en el nivel macroscópico.

La física clásica y las leyes de Newton, nos permiten guiarnos realizando varias pruebas experimentales sobre lo que sucede a nivel macroscópico, esto lo vemos en el ejemplo más básico como lo es la trayectoria de un balón de futbol, ya que es visible para nosotros y de esta manera podemos calcular su velocidad, trayectoria, aceleración entre otros, esto lo podemos tanto calcular como visualizar a través de nuestros sentidos. La física cuántica trabaja en la parte que los sentidos no pueden ver, como lo es la polarización de un fotón.

La teoría cuántica incluye varios fenómenos que no son descritos en la física clásica como la superposición, el principio de incertidumbre, entre otros, lo que genera que se realice un nuevo foco para profundizar sobre estos fenómenos, estos fenómenos son las bases de la criptografía cuántica.

“La Teoría Cuántica es una teoría netamente probabilista: describe la probabilidad de que un suceso dado acontezca en un momento determinado, sin especificar cuándo ocurrirá. A diferencia de lo que ocurre en la Física Clásica, en la Teoría Cuántica la probabilidad posee un valor objetivo esencial, y no se halla supeditada al estado de conocimiento del sujeto, sino que, en cierto modo, lo determina. ”[26]

Hablando un poco sobre la historia de la cuántica, partimos de la relatividad de Einstein, ya que empezó con las ecuaciones correctas por el físico Max Plank donde el asumía que la materia alcanza a absorber y exponer luz en pequeñas partes de acuerdo a la formula *E=hv*

Aunque esta teoría fue cuestionada en aquella época, no fue sino hasta que Albert Einstein la aprovecho llevándola a su tesis del efecto fotoeléctrico (ganadora de un Premio Nóbel en el año 1921), donde el asumía que la luz no era solamente ondas si no que podían comportarse como un fajo dé partículas que llamo fotones y replanteo la ecuación de Plank sobre la relación entre la frecuencia de la luz y la energía del fotón, así *v=E/h*.
El físico Louis de Broglie aprovecho los estudios realizados por Max Planck y Albert Einstein sobre las bases de la física cuántica y presentó su tesis en el año 1924 donde realiza un nuevo descubrimiento, la dualidad onda-partícula, indicando que el comportamiento de los electrones es como ondas y que las partículas llevan asociada una onda de materia.

De allí surge la hipótesis de Broglie, combinando las ecuaciones de Plank (cuantización de la energía: E= hv) y de Einstein (relatividad especial: E=mc2),

[26] TOBOSO, Mario, La Teoría Cuántica, una aproximación al universo probable ([En línea], Disponible en: https://www.tendencias21.net/La-Teoria-Cuantica-una-aproximacion-al-universo-probable_a992.html

proponiendo la formula hv/c^2.

Otro de los descubrimientos fundamentales de la Mecánica Cuántica es el Principio de Incertidumbre, por Werner Heisenberg, este principio nos dice que en la mecánica cuántica cuando nos acercamos a un objeto especifico, se pierde la información sobre otro objeto cercano, conocido como el caso de la superposición de las partículas del momentum.

En la actualidad el método criptográfico más utilizado, resistente a varios ataques y fiable es el RSA, ya que su algoritmo base se debe a números primos. Una de las ventajas que tiene que es que no existe aún un computador que sea capaz de descifrar un mensaje sin que tenga la clave privada en un lapso de tiempo corto.

Aunque es sabido, con la aplicación de ciertas formulas y algoritmos inventado por Shor no es tan remota la posibilidad del desarrollo de un computador cuántico que podría llegar a destruir la seguridad de todos los algoritmos actuales y el desarrollo de algoritmos y criptosistemas de nivel cuántico.

Con el tiempo si los experimentos a nivel cuántico se convierten en una realidad, la situación a nivel computacional cambiará de forma drástica, ya no hablaríamos a nivel de bits sino a nivel de qubits (bits cuánticos) y los computadores cuánticos estarían en la capacidad de solucionar problemas con mayor eficiencia y rapidez que uno digital.

Dentro del campo de la criptografía, al usar los qubits se podrán realizar cálculos exponenciales mucho más rápidos y eficientes, a un nivel superior que los que realizan los computadores convencionales, también se puede utilizar gracias a la teoría cuántica de la información el diseño de algoritmos que permitirán realizar la distribución de claves cuánticas y la teleportación cuántica.

Básicamente utilizando los fenómenos cuánticos podemos cifrar información o destruir cualquier sistema criptográfico y de manera hipotética se podría llegar a vulnerar algún método de claves públicas que utiliza RSA.

Otra de las ventajas que tiene la criptografía cuántica es que se puede llegar a detectar algún tipo de intrusión o espionaje que se haga en el medio, ya que, al tratar de espiar una clave cuántica, gracias a los estados del qubits el mensaje será cambiado y el receptor puede validar inmediatamente si el mensaje fue interceptado, algo que no se puede realizar en la comunicación clásica.

8. COMPUTACIÓN CUÁNTICA Y SUS PRINCIPALES APORTES.

Un ordenador cuántico realizaría lo mismo que hace un computador convencional, pero con un procesamiento diferente de datos, este procesamiento se basaría en las leyes de la física cuántica.

Desde la época de los 90, existen las bases teóricas de un computador cuántico que ha sido el resultado de la investigación de varios años de diferentes personalidades de la ingeniera. La presentación de este modelo comercialmente se ha dilatado con el tiempo, ya que puede llegar a romper los modelos estandarizados de la computación tradicional.

En la actualidad los computadores realizan varios procesos utilizando sus capacidades físicas, estas operaciones tienden a durar minutos, aunque dependiendo de la complejidad de la operación puede tardar incluso horas, con la computación cuántica se espera una velocidad de procesamiento superior sobre las mismas operaciones complejas que llegarían a tardar segundos y de esta manera desarrollar una nueva era en el mundo cuántico.

Aprovechando las características de la física cuántica que indica que un átomo puede estar en dos lugares diferentes en el mismo tiempo, la base del computador cuántico indica que cualquier objeto puede estar en varios estados a la vez, lo que permite hacer que el computador cuántico sea mucho más eficiente.

Los computadores cuánticos denominados como QC (Quantum Computer) tienen una característica sobre las computadoras convencionales, como sabemos la computación convencional procesa a través del lenguaje binario, es decir 1-0, estado apagado o encendido y solo lee uno de los estados a la vez, las computadoras QC operan con la cualidad física de los átomos llamada la superposición que le permite tener dos valores a la vez, lo que permite que se

realicen varias actividades al tiempo, como por ejemplo buscar en archivos muy grandes, representar varios sistemas o solucionar operaciones matemáticas complejas o realizar factores de números grandes en menor tiempo.

8.1 ELEMENTOS DE LOS COMPUTADORES CUÁNTICOS.

Al realizar un análisis visual de un computador cuentico podemos descubrir que no cuenta ni con memoria RAM ni con un disco duro, solo tiene un procesador al que le llegan las señales de los microondas que le permiten gestionar los estados de los qubits, por esta razón los dos elementos que constituyen un computador cuántico son:

8.2 BIT CUÁNTICO.

Los Qubits representa una unidad básica de información cuántica. Los qubtis utilizan el comportamiento de la dualidad onda-partícula, que utiliza la superposición, en la que un átomo puede tener un estado de 0 y de 1 y además puede adoptar ambos estados al mismo tiempo, para que esta propiedad funcione los qubits deben estar separados uno de otros y solo interactúan cuando el proceso lo requiera.

A continuación, se muestra en la imagen los diferentes estados de un Qubit.

Figura 12. Estados de un Qubit

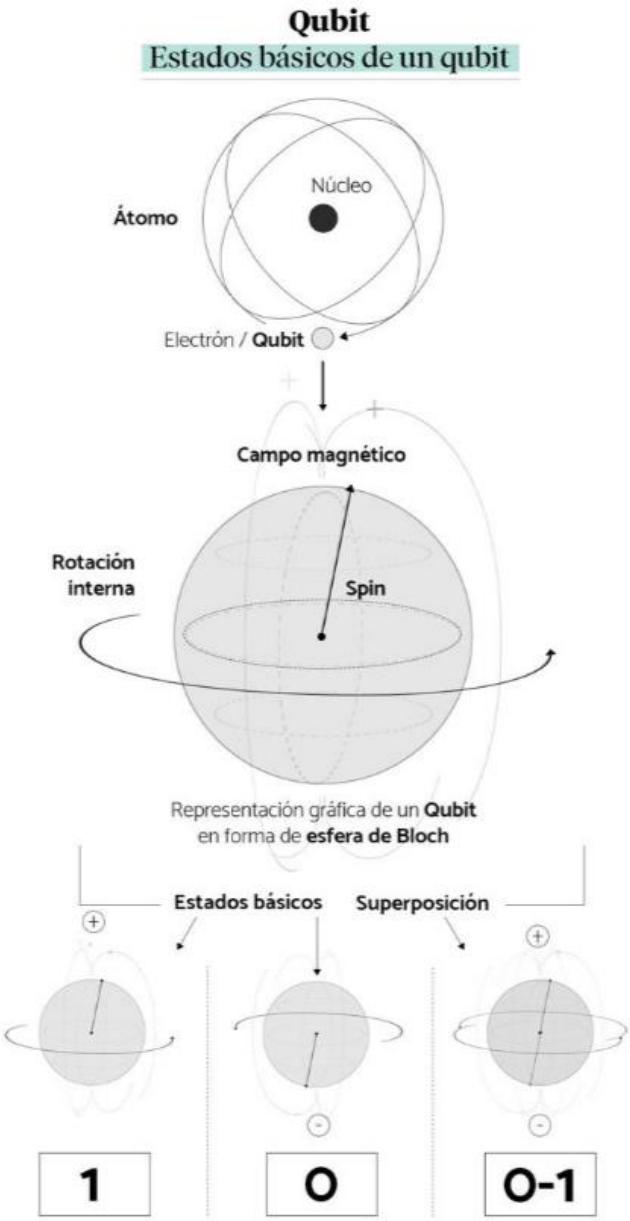


Figura 13. Estados de un Qubit

Fuente: [Fotografía], Computación cuántica: el futuro de los ordenadores [Consultado: 15 de noviembre de 2018] Disponible en internet: https://www.lavanguardia.com/tecnologia/20170521/422764114392/computacion-cuantica-ordenadores-qubits.html

Como podemos observar en la imagen, tenemos 3 bits en un estado específico (0,1) los cuales pueden ser mezclados de ocho formas posibles:

000

001

010

011

100

101

110

111

Lo que significaría que, si aumentamos el número de bits, tendríamos como resultado mayor número de combinaciones como por ejemplo si contáramos con 6 bits serían 64 posibles combinaciones, contrario a lo que pasaría si tuviéramos 3 qbits ya que puede realizar las mismas ocho combinaciones al mismo tiempo.

Lo que determina el estado de un Qubits es la observación, lo que significa que a niveles interno un computador cuántico no puede ser visto, si es visto se pierde los efectos cuánticos, con ello el estado y función de la onda y la información que contiene.

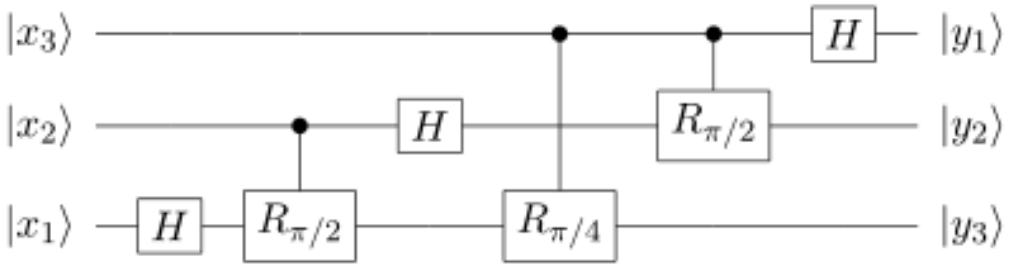
Los Qubits trabajan a temperaturas muy bajas, llegando a requerir el cero absoluto que se encuentran sobre los -273,15° C o 0° Kelvin.

8.3 PUERTAS LÓGICAS CUÁNTICAS

Las compuertas cuánticas operan en el principio de reversibilidad y universalidad, lo que indica que cuando se trabaja con una compuerta cuántica si conocemos el resultado de los estados se puede llegar a conocer los estados ingresados.

A continuación, un diagrama sobre el funcionamiento de computación cuántica.

Figura 14 Componentes de un computador cuántico.



Fuente: [Fotografía], Computación cuántica: el futuro de los ordenadores [Consultado: 17 de noviembre de 2018] Disponible en internet: https://www.lavanguardia.com/tecnologia/20170521/422764114392/computacion-cuantica-ordenadores-qubits.html

8.4 APORTES DE LA COMPUTACIÓN CUÁNTICA

Estos computadores cuánticos pueden complementar a los supercomputadores que existen en varios países del mundo, pueden llegar a realizar las mismas tareas que realiza los supercomputadores como predicciones de tiempo, diseño de compuestos químicos o estudio de los materiales en un menor tiempo utilizando mucho menos energía.

Los métodos de criptografía actuales serian inseguros con estos computadores cuánticos, ya que ellos podrían llegar a decodificar una comunicación realizando factorización de números grandes de manera rápida.

Los ordenadores cuánticos serán más rápidos en la búsqueda de datos en base de datos, ya que realizara la búsqueda de manera eficiente, realizarán aplicaciones de optimización.

Los fabricantes que le han apostado al desarrollo de estos computadores cuánticos

son Google, IBM, Intel, Microsoft y ya han realizado varios prototipos conocidos como Quantum Supremacy para los próximos dos años.

Los ordenadores que están desarrollando en la actualidad no tienen corrección de errores, solo está realizando pruebas para que los Qubits no tengan interacción con nada y den un resultado correcto, aunque para que realice tareas más complejas como factorización, requiere tener corrección de errores.

Con las correcciones de errores se pueden tener resultados efectivos del tiempo para que se pueda trabajar con los estados cuánticos.

8.5 ¿EN QUE VAMOS?

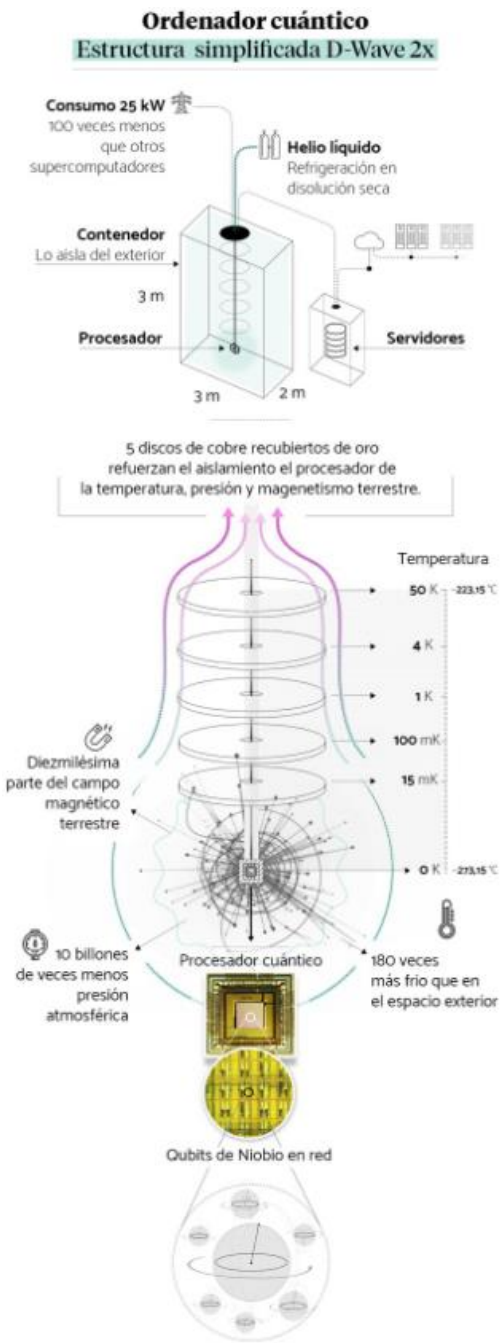
Intel junto con el instituto de investigación cuántica dentro de la Delft University of Technology (TU Delft) y TNO, realizaron un acuerdo desde el 2015 con una duración de 10 años y una inversión de 50 millones de dólares en QuTech con el objetivo de sentar las bases de una muestra computacional que sea capaz de solucionar problemas de la computación.

Google y la Nasa se unieron y compraron la empresa D-Wave Systems, esta empresa ha desarrollado dos computadores cuánticos. El primero llamado D-Wave 2X, trabaja con 1.000 qubits y es capaz de ejecutar operaciones de 100 millones de veces más rápido que los computadores usuales.

El nuevo ordenador cuántico de la firma, bautizado como D-Wave 2000Q, puede presumir de tener el doble de qubits. La nueva versión llamada D-Wave-2x trabaja con 2.000 qubits.

A continuación, en la imagen se presenta la estructura física de un D-Wave 2X.

Figura 15. Ordenador Cuántico



Fuente: [Fotografía], D-Wave lanza un ordenador cuántico de 2.000 qubit [Consultado: 17 de noviembre de 2018] Disponible en internet: https://www.computerworld.es/innovacion/dwave-lanza-un-ordenador-cuantico-de-2000-qubits

Google también cuenta con Quantum Playground, este experimento usa WebGL27 en el cual simula registros de hasta 22 qubits, se pueden ejecutar algoritmos cuánticos (Shor y Grover28), y cuenta con una variedad de puertas cuánticas incorporadas.

IBM Q por su parte se encuentra trabajando en el diseño de un prototipo de 50 qubit del ordenador cuántico y la elaboración de ordenadores cuánticos para el mercado de la investigación, los cuales operan con 20 qubits y un promedio de 90 microsegundos.

El 4 de mayo del 2016 IBM lanzo el proyecto “IBM Q Experience” o computador cuántico en la nube con un prototipo de 5 qubits y hace algunos meses instauró otro ordenador con 16 qubits. Este proyecto ofrece un camino práctico a la computación cuántica experimental y se encuentra basado en qbits superconductores y se encuentra enfocado a estudiantes y ya cuenta con cerca 60.000 usuarios y se han realizado aproximadamente 1,7 millones de experimentos.

A continuación, una imagen del computador cuántico de IBM.

Figura 16. IBM Q

Fuente: [Fotografía], IBM Q [Consultado: 17 de noviembre de 2018] Disponible en internet: https://www.research.ibm.com/ibm-q/

9. CRIPTOGRAFÍA CUÁNTICA Y SU EVOLUCION.

La criptografía actual utiliza un sistema que permite encriptar la información entre el emisor y el receptor y que solo ellos puedan “entender” el mensaje, utilizando un sistema de claves. Aunque este método no es 100% seguro ya que en la actualidad los computadores pueden descifrar estos mensajes en horas y si es interceptado ni el emisor ni el receptor pueden percatarse.

Debido a esto se ha ido desarrollando la criptografía cuántica aprovechando los dos principios más importantes de la física cuántica, el entrelazamiento cuántico y el principio de incertidumbre.

Los inicios del estudio de la criptografía cuántica inician en la Universidad de Columbia, en los años 60, con Stephen Wiesner quien tenía la idea de que dos mensajes fueran transmitidos por canal cuántico donde solo pudiera ser extraído uno de los dos mensajes por el receptor, estas ideas en su época eran un tanto locas así que no fueron tenidas en cuenta hasta los 80.

En el año 1984 Gilles Brassard y Charles Bennett desarrollaron el protocolo BB84 (Brassard-Bennett-1984), conocido como el primer protocolo de la criptografía cuántica y tomando las ideas expuesta por Wiesner propusieron que no debería almacenarse información si no que deberían usar las propiedades físicas de los fotones para transmitir información.

Este protocolo tuvo su primera aplicación práctica a través de un canal de 30 cm gracias a un prototipo construido por IBM. Otro experimento práctico lo realizarón en los laboratorios de Telecom en Inglaterra con Paul Towersend y Christophe Marand en el año 1994, modificando el protocolo BB84 demostraron la primera

distribución real de claves cuánticas a una distancia de 30 km dentro de una misma habitación.

En el año de 1997, el siguiente experimento fue realizado por un equipo de la Universidad de Geneva quienes realizaron el experimento real con una distancia mayor de 23 Km de separación del emisor y el receptor, en este experimento una señal fue transmitida por una fibra óptica que se encuentra bajo el lago Geneva, utilizando una técnica especializada para cancelación de ruido.

Unos años más tarde Richard Hughes y su grupo de trabajo realizaron otra prueba de transmisión aumentando la distancia a 48 Km. Y en el año 2007 ellos mismos lograron realizar una distribución de claves cuánticas a una distancia de 148.7 km. Estos experimentos se limitaban en espacio geográfico debido al repetidor ya que, al restaurar una seña débil, esta entraba en contacto con la señal del repetidor se modificaba, corrompiendo los datos. Por eso los repetidores no eran los óptimos para este tipo de pruebas y la distancia era corta, con el pasar de los años los investigadores encontraron otras alternativas para poder ampliar el rango de distancia, una de estas es la de transmitir fotones por el aire en vez de utilizar un medio fisco como la fibra óptica.

Con esta idea, se han realizado varios experimentos, estos se han realizado en las montañas, donde gracias a la altitud se reduce la turbulencia atmosférica. El laboratorio Nacional de Los Alamos, logro establecer una conexión de 10 km por el aire y más adelante QinetiQ en Farnborough en colaboración con la Universidad Ludwing Maximilian de Munich, lograron establecer un enlace de 23 km entre dos cimas de los Alpes meridionales.

Y en el 2007, se realizó una distribución de clave cuántica segura transmitida por el aire entre dos telescopios que se encontraban separados a 144 Km, entre dos de las Islas Canarias.

9.1 PROTOCOLOS DE LA CRIPTOGRAFÍA CUÁNTICA.

9.1.1 Protocolo BB84

Este protocolo Brassard y Bennett involucra el envío de fotones en diferentes estados de polarización con la ayuda de un filtro de polarización, donde se seleccionará el ángulo de polarización con respecto a la horizontal.

La información se transmite en código binario (0 y 1) y estos puede transmitirse por fotones con dos polaridades vertical, horizontal y su orientación inclinado hacia la izquierda, hacia la derecha, vertical y horizontal y puede agregarse incertidumbre cuántica para encriptar la información.

Cuando los fotones se encuentran polarizados en “ángulos de 0 y 45 representan el valor binario 0, y los fotones polarizados en ángulos de 90 y 135 representan el valor binario 1; una vez hecha esta correspondencia, una secuencia de bits puede ser convertida en una secuencia de fotones polarizados[27]”.

Este protocolo funciona usando dos canales de comunicación entre el emisor y receptor. El primer canal cuántico es privado y con una sola dirección, en el cual se pasarán las claves donde serán transmitidos los qubits, el segundo es un canal público y es bidireccional que se usara para transferir la información que se requeriría para realizar la construcción de la clave compartida.

El emisor envía una secuencia de qubits por el canal cuántico, generando y registrando la polarización para que el fotón tenga diferentes orientaciones, al llegar el mensaje el receptor no sabe que polarización uso el emisor y para decodificar

---

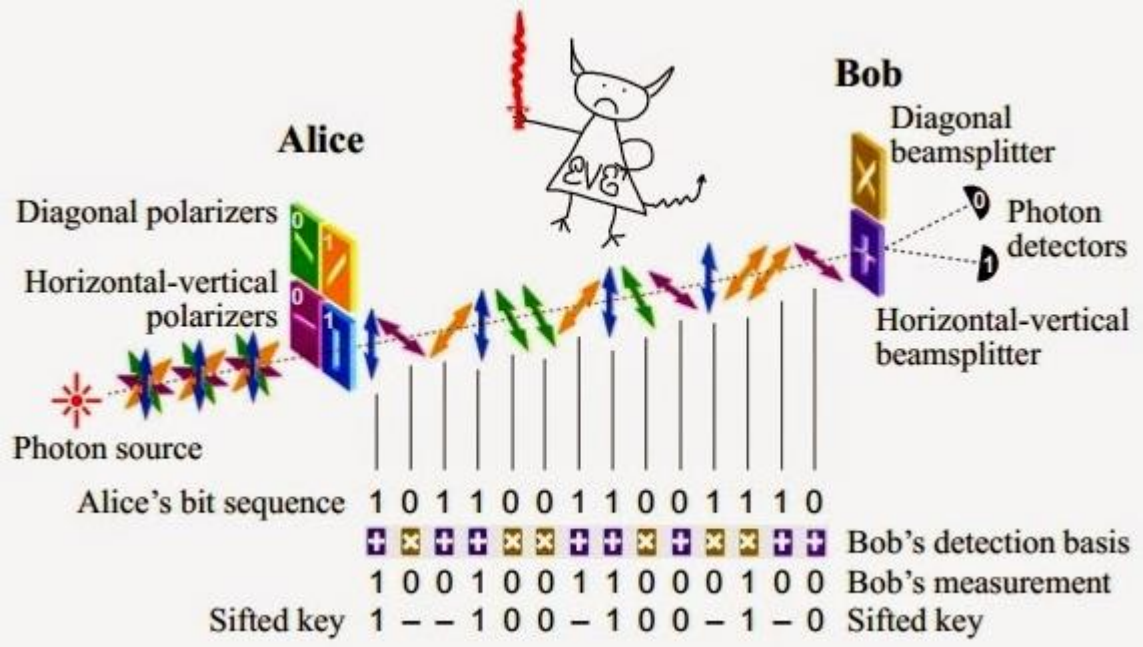
[27] . ROJAS, Hernan, FUNDAMENTOS DE CRIPTOGRAFÍA CUÁNTICA, {En línea}. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/2367/OrtizRojas_Hernan_2007.pdf;sequence=1

debe generar unas posibles polarizaciones que puede medir las orientaciones y con esto obtendrá el valor de los qubits.

Cuando un fotón llegue donde el emisor pasa por las polarizaciones, si la orientación es la correcta, se obtendrá el valor del qubit, si no es correcta se tendrá un valor diferente, ya que el fotón cambia su orientación si pasa por una polarización que no tiene la orientación con la que el atravesó el canal cuántico.

Gráficamente, se explica el funcionamiento del protocolo:

Figura 17. Funcionamiento de BB84



Fuente: [Fotografía], El protocolo BB84 [Consultado: 17 de noviembre de 2018] Disponible en internet: https://www.research.ibm.com/ibm-q/

9.1.2 Protocolo B92

Charles Bennett propuso la versión simplificada de BB84, la principal diferencia entre estos dos protocolos es que la clave en B92 solo necesita dos estados en lugar de los 4 estados de polarización posibles en BB84.

Donde la polarización en 0° representa un “0” y en 45° un “1”

9.1.3 Protocolo EPR

El físico Arthur Eckert en 1991, elaboro un sistema de criptografía basada en el efecto denominado EPR, concebido en las predicciones contra intuitivas del fenómeno de acción a distancia, que fueron inicialmente discutidas en 1935 por Albert Einstein, Boris Podolsky y Nathan Rosen.

> “Este efecto tiene lugar cuando un átomo con simetría esférica, emite dos fotones en direcciones contrarias. El estado de polarización inicial de cada fotón es indefinido. Solo cuando se midan bajo la misma base, se obtendrán resultados siempre opuestos. A continuación, se muestra un ejemplo del protocolo EPR en el cual los usuarios A y B miden con filtros de polarización rectilínea al par de fotones que surgen entrelazados. Ambos tienen la misma probabilidad de registrar un 1 o un 0, pero inmediatamente el primer usuario registre un 1 en su medición, es 100% seguro que el usuario B registrará un 0 en la suya”[28]

[28] LAVERDE ALFONSO, Sebastian, ESTUDIO COMPARATIVO Y EVALUACIÓN DE UTILIDAD DE PROTOCOLOS DE TRANSMISIÓN DE DATOS USANDO CRIPTOGRAFÍA CUÁNTICA T.G. 1612, {En línea}. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/21443/LaverdeAlfonsoSebastian2016.pdf?sequence=1&isAllowed=y

Figura 18. Funcionamiento de protocolo EPR

Fuente: https://repository.javeriana.edu.co/bitstream/handle/10554/21443/LaverdeAlfonsoSebastian2016.pdf?sequence=1&isAllowed=y

La criptografía cuántica en la actualidad ya cuenta con productos comerciales ya que no es necesario un computador cuántico para obtener una clave cuántica.

> "Las compañías Id Quantique y MagiQ Technologies, ofrecen al público él envió de una clave de criptografía cuántica a una distancia de 30 centímetros, también ofrece " Cerberis (que combina el cifrado a alta velocidad basado en el estándar AES, con la seguridad de una Distribución de Clave Cuántica), Vectis (un hardware para cifrado de enlaces punto a punto en redes de fibra óptica que también usa AES y Distribución de Clave Cuántica), Clavis (un sistema para investigación y desarrollo de aplicaciones de Distribución de Clave Cuántica), y Quantis (un generador cuántico de números aleatorios reales que se puede conectar al puerto USB)"29

Existe una aplicación web creada por por Arash Atashpendar, llamada QKD SIMULATOR, que permite realizar simulaciones y análisis de los aspectos de distribución de clave cuántica, donde se pueden realizar personalizaciones de los

[29] ROJAS, Hernan, FUNDAMENTOS DE CRIPTOGRAFÍA CUÁNTICA, {En línea}. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/2367/OrtizRojas_Hernan_2007.pdf;sequence=1

ajustes iniciales y definir componentes del sistema, como el canal cuántico, la tamización, la corrección de errores y trabaja con un máximo de 600 qbits.

10. INFOGRAMA DE CRIPTOGRAFIA CUANTICA.

Como resultado final sobre la monografía, se presenta una infografía sobre la criptografía actual, enfocándonos en la criptografía cuántica y sus principales ventajas.

La estructura del infograma es:

- Criptografía actual.
- Que es la criptografía cuántica.
- ¿Por qué la criptografía cuántica?
- ¿Cómo se transmite la información?
- Ventajas de la criptografía cuántica.

La criptografía cuántica nos asegura un futuro con una seguridad en la transmisión de datos mucho más segura que permitirá contribuir a una implementación más segura y ágil para el mundo.

(Ver Anexo 1)

11. CONCLUSIONES

Aplicando las fórmulas propuestas por los físicos más destacados de la historia en el mundo cuántico y aplicándolas a la criptografía cuántica se puede llegar a imaginar un futuro con una seguridad mucho más fiable en cuanto a la transmisión de datos lo que permitirá contribuir a un mundo seguro.

Los experimentos realizados hacia la computación cuántica en los últimos años, nos permite realizar un panorama alentador para conocer y desarrollar los ordenadores cuánticos, en especial por las capacidades superiores que tendrán sobre la resolución de tareas complejas como lo es la factorización de números, búsqueda de moléculas, entre otros.

En la actualidad solo se tiene en papel los diseños de hardware, la construcción de un ordenador cuántico está limitada por las capacidades físicas y técnicas disponibles de los equipos y materiales disponibles.

Cuando los ordenadores cuánticos sean desarrollados serán muy útiles para diferentes tareas en diferentes áreas tanto en diseño de fármacos, diseño de materiales, optimización, resolver ecuaciones, en la criptografía, etc. IBM y Google, le están apostando al desarrollado de estos ordenadores, y es muy probable que ellos sean los pioneros en esta tecnología.

La computación cuántica puede llegar a acabar con la criptografía actual ya podrá descifrar los mensajes que ya se han enviado y los que se están enviando, en menor tiempo, por esta razón los científicos esta implementado “post quantum cryptography” que consiste en utilizar otras operaciones diferentes a la factorización para encriptar mensaje.

La criptografía cuántica, se origina como una solución a una falla de seguridad en la distribución de las claves entre el emisor y el receptor. El uso de un canal cuántico utilizado por el protocolo BB84 permite hacer un monitoreo en tiempo real y permite validar si la transmisión está siendo interceptada, su seguridad parte del uso de fenómenos físicos.

La criptografía cuántica no está siendo aprovechada al 100% sobre las comunicaciones por el rango geográfico que puede cubrir, pero con el tiempo se puede pensar que con la ayuda de la implementación de redes de comunicación se llegaran a transmitir mensajes codificados a distancias superiores.

BIBLIOGRAFIA

1. ABELIUK, Andres, Computación Cuántica {En línea}. Fecha {19 de Mayo de 2018} disponible en: https://users.dcc.uchile.cl/~aabeliuk/documents/computacion_cuantica.pdf

2. ARENAS, Manu, Así es el ordenador cuántico de 49 Qubits de Intel por dentro. CUÁNTICA {En línea}. Fecha {15 de Noviembre de 2018} Disponible en: https://www.xataka.com/ordenadores/asi-ordenador-cuantico-49-qubits-intel-dentro

3. BANAFA, Ahmed, Entender La Criptografía Cuántica, {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: https://www.bbvaopenmind.com/entender-la-criptografia-cuantica/

4. BANCO DE ESPAÑA, Aplicación De Obtención De Certificados A Través De Internet Con Acceso Autenticado, {En línea}. Fecha {19 de Mayo de 2018} disponible en: http://pki.bde.es/f/webpkibde/INF/Secciones/Solicitudes/Archivos/OCIAUTE-MU2007.19-V07.pdf

5. BUENDIA, Jose, Diffie y Hellman, los abuelos de RSA y el cifrado asimétrico {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: https://www.muycomputerpro.com/2016/03/03/diffie-martin-rsa-cifrado-asimetrico

6. CADAVID, Pabón, La criptografía y la protección a la información digital {En línea}. Fecha {19 de Mayo de 2018}. Disponible en:http://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

7. CARREÑO, Juan, Algoritmo De Factorización De Shor, {En línea}. Fecha {24 de Mayo de 2018} Disponible en: http://www.dma.eui.upm.es/MatDis/Seminario4/AlgoritmoShor.pdf.

8. CORMICK, Paz, Estimación de fase y algoritmo de Shor {En línea}. Fecha {24 de Mayo de 2018} Disponible en: http://users.df.uba.ar/paz/pag_comp_cuant/resumenes/clase12.pdf

9. CORRALES, Héctor, Criptografía y Métodos De Cifrado digital {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

10. DIFFIE, whitfield and HELLMAN, martin, New Directions in Cryptography {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: https://ee.stanford.edu/~hellman/publications/24.pdf

11. GÓMEZ Cárdenas, Roberto, Criptosistemas, {En línea}. Fecha {19 de Mayo de 2018} Disponible en: http://cryptomex.org/CursoCriptoTec/criptosistemas.html

12. JIMÉNEZ, Javier, ¿El principio del fin de la criptografía actual? Crean la primera computadora cuántica escalable {En línea}. Fecha {19 de mayo de 2018}, Disponible en: https://www.xataka.com/investigacion/el-principio-del-fin-de-la-criptografia-actual-crean-la-primera-computadora-cuantica-esclable

13. LANCHO, Daniel, Criptografía Cuántica Aplicada [En línea], Disponible en: http://gicc.fis.ucm.es/teaching/master/SeminarioUCM-19Ene07-web.pdf

14. LAVERDE ALFONSO, Sebastian, Estudio Comparativo Y Evaluación De Utilidad De Protocolos De Transmisión De Datos Usando Criptografía Cuántica T.G.

1612, {En línea}. Fecha {18 de Noviembre de 2018}. Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/21443/LaverdeAlfonsoSebastian2016.pdf?sequence=1&isAllowed=y

15. LOPEZ, Juan Carlos, El Principio De Incertidumbre De Heisenberg {En línea}. Fecha {19 de Mayo de 2018} disponible en: https://www.nucleares.unam.mx/~vieyra/node20.html

16. MARTÍNEZ, Evelio, Claude Shannon: el padre de la teoría de la información Criptografía {En línea}. Fecha {19 de Mayo de 2018}, Disponible en: http://www.eveliux.com/mx/Claude-Shannon-el-padre-de-la-teoria-de-la-informacion.html

17. MENEZES, OORSHOT Y VANSTONE, Handbook of Applied Cryptography digital {En línea}. Fecha {19 de Mayo de 2018}, Disponible en http://cacr.uwaterloo.ca/hac

18. MOLINA, María, Criptografía Cuántica: Un Nuevo Paradigma digital {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: http://www.redalyc.org/pdf/4026/402640449006.pdf

19. MONTOYA, Fausto, La criptografía cuántica, ¿realidad o ficción? digital {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: https://www.researchgate.net/publication/255601730_La_criptografia_cuantica_realidad_o_ficcion1

20. MORET BONILLO, Vicente, Principios Fundamentales De Computación Cuántica {En línea}. Fecha {15 de Noviembre de 2018} Disponible en: http://www.lidiagroup.org/images/descargas/varios/011_ccuantica.pdf

21. MORALES-LUNA, Guillermo, Un poco de computación cuántica: Algoritmos más comunes, {En línea}. Fecha {24 de Mayo de 2018} Disponible en: https://www.fceia.unr.edu.ar/~diazcaro/QC/Tutorials/Un%20poco%20de%20computacion%20cuantica%20-%20Algoritmos%20mas%20comunes.pdf

22. NEXT IBS, La criptografía cuántica, el futuro de la Ciberseguridad digital {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: http://www.nextibs.com/criptografia-cuantica-ciberseguridad/

23. PABON, Jhonny. Revista La Propiedad Intelectual. La criptografía y la protección a la información digital {En línea}. Fecha {19 de mayo de 2018}. Disponible en: https://www.minjusticia.gov.co/InvSocioJuridica/DboRegistros/GetPdf?fileName=La%20criptografia%20y%20la%20proteccion%20a%20la%20informacion.pdf

24. QUEZADA, Roberto, Entropía Relativa De Von Neumann {En línea}. Fecha {24 de mayo de 2018} Disponible en: http://www2.izt.uam.mx/newpage/contactos/revista/90/pdfs/entropia.pdf

25. QUEZADA, Roberto, Mecánica Cuántica {En línea}. Fecha {24 de Mayo de 2018} Disponible en: https://www.ecured.cu/Mec%C3%A1nica_cu%C3%A1ntica.

26. RIVEST Ronald, Cryptography and the Limits of Secrecy. {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: http://web.mit.edu/ssp/seminars/wed_archives99fall/rivest.pdf

27. ROJAS, Hernan, Fundamentos De Criptografía Cuántica, {En línea}. Fecha {24 de Mayo de 2018} Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/2367/OrtizRojas_Hernan_2007.pdf;sequence=1

28. TARRIO, Javier, Teorema De No Clonado, {En línea}. Fecha {24 de Mayo de 2018} Disponible en: http://www.lawebdefisica.com/dicc/noclonat/

29. TEXTOS CIENTÍFICOS. Criptografía cuántica - Conceptos de criptografía {En línea}. Fecha {19 de mayo de 2018}. Disponible en: https://www.textoscientificos.com/criptografia/quantica

30. TOBOSO, Mario, La Teoría Cuántica, una aproximación al universo probable ([En línea], Disponible en: https://www.tendencias21.net/La-Teoria-Cuantica-una-aproximacion-al-universo-probable_a992.html

31. UNIVERSIDAD DE CORDOBA, No Dolly - Teorema De La No Clonación Cuántica {En línea}. Fecha {24 de Mayo de 2018} Disponible en: http://www.uco.es/hbarra/index.php/blog/182-no-clonacion

32. XIFRE, Patricia, Antecedentes y perspectivas de estudio en historia de la Criptografía {En línea}. Fecha {19 de Mayo de 2018}. Disponible en: http://www.cnv.gob.ar/infoadicional/rsafaq.htm

ANEXOS

ANEXO 1. INFOGRAMA MARTHA LARA

(Ver imagen Infograma_Criptografia_cuantica pdf)

ANEXO 2. FORMATO RAE

RESUMEN ANALITICO ESPECIALIZADO RAE	
1. Titulo.	LA COMPUTACION CUANTICA Y LAS IMPLICACIONES SOBRE LA CRIPTOGRAFIA MODERNA.
2. Autor.	LARA, Pérez, MARTHA Lucia
3. Edición.	N/A
4. Fecha.	9 de diciembre 2018
5. Palabras claves.	Criptografía, cuántica, protocolos, algoritmos, seguridad, información, criptosistemas, llaves, claves.
6. Descripción.	Monografía sobre el estudio de las implicaciones que la física cuántica realizará sobre la criptografía moderna. Se abordaron conceptos sobre los sistemas de cómputo tradicionales, la criptografía moderna, su historia y los mayores aportes que ha hecho a la tecnología actual. Esta monografía tiene como fin realizar un análisis del impacto de la criptografía cuántica en los procesos de las comunicaciones modernas, sirviéndose de las leyes de la física y aprovechando los estudios realizados sobre el principio de incertidumbre de Heisenberg y temas cuánticos desarrollados.
7. Fuente.	Esta monografía se basó en publicaciones especializadas sobre Física Cuántica de diferentes fuentes como investigaciones en internet, tutoriales y videos especializados.

8. Contenido.	Con el transcurrir del tiempo, la seguridad de la información ha tomado una gran importancia y de ahí que se realicen todos los procedimientos y métodos necesarios para asegurar que la transmisión de los datos a través de Internet sea totalmente seguro, para que esto se cumpla desde la antigüedad se han venido desarrollando una variedad de investigaciones enfocadas en la encriptación, desde métodos rudimentarios hasta complejos logaritmos criptográficos. Gracias a la necesidad de proteger la información, nacen varios sistemas de protección, entre ellos los criptográficos; estos sistemas de protección cuentan con algoritmos y funciones matemáticas que permiten “cifrar y proteger” la información y nos “asegura” que estas transmisiones son seguras entre el emisor y el receptor Estos cambios han obligado a que las organizaciones presten más atención a la seguridad de la información, sin dejar de lado estar actualizados con la tecnología, se debe avanzar conociendo la importancia de la seguridad informática, de esta manera surgen los diferentes sistemas de protección como los firewalls, IDS, protocolos de conexión segura y la criptografía. Esta monografía se realiza para entender como la criptografía cuántica cambio de manera drástica la Ciberseguridad.

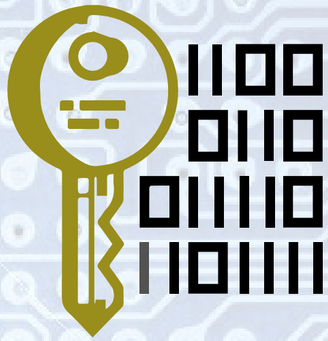
	Así mismo, tiene como fin dar un insumo a la comunidad académica y a los interesados, el material de investigación y las implementaciones que se han realizado hasta la fecha sobre la criptografía cuántica.
9. Metodología.	La metodología de este trabajo es investigativa con el fin de conocer y divulgar las implicaciones que la criptografía cuántica traerá a la tecnología actual. En ella se abordó conceptos sobre los sistemas de cómputo tradicionales, la criptografía moderna, su historia y los mayores aportes que ha hecho a la tecnología, tomando como base publicaciones especializadas sobre Física Cuántica, entrevistas y videos científicos.
10. Conclusiones.	Aplicando las fórmulas propuestas por los físicos más destacados de la historia en el mundo cuántico y aplicándolas a la criptografía cuántica se puede llegar a imaginar un futuro con una seguridad mucho más fiable en cuanto a la transmisión de datos lo que permitirá contribuir a un mundo seguro. Los experimentos realizados hacia la computación cuántica en los últimos años, nos permite realizar un panorama alentador para conocer y desarrollar los ordenadores cuánticos, en especial por las capacidades superiores que tendrán sobre la resolución de tareas complejas como lo es la factorización de números, búsqueda de moléculas, entre otros. La criptografía cuántica, se origina como una solución a una falla de seguridad en la distribución de las claves entre el emisor y el receptor. El uso de un canal cuántico utilizado por el protocolo BB84 permite hacer un monitoreo en tiempo real y permite validar si la transmisión está siendo interceptada, su seguridad parte del uso de fenómenos físicos. La criptografía cuántica no está siendo aprovechada al 100% sobre las comunicaciones por el rango geográfico que puede cubrir, pero con el tiempo se puede pensar que con la ayuda de la implementación

	de redes de comunicación llegaron a transmitir mensajes codificados a distancias superiores.
11. Autor del RAE.	Martha Lucia Lara Pérez.

CRIPTOGRAFIA CUANTICA

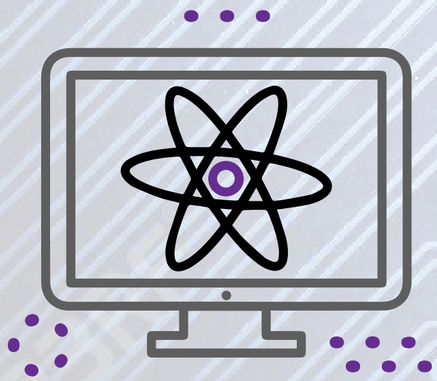
La Criptografía es una técnica que hace uso de las técnicas y métodos de las matematicas con el **principal objetivo de cifrar**, lo que permite **proteger la información** o los mensajes con la ayuda de algoritmos y claves.

En la **Actualidad** podemos ver **el uso de la criptografía** en varias aplicaciones, no solamente en el intercambio seguro de información, sino en diferentes actividades cotidianas **como la compra por internet, una llamada por celular, un retiro de cajero electrónico,** entre otros.



¿Qué es la criptografía Cuántica?

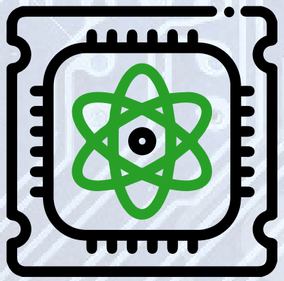
La Criptografía cuántica **utiliza los principios de la mecánica cuántica** para desarrollar un criptosistema completamente seguro, aprovechando los dos principios más importantes de la física cuántica, **el principio de la superposición y el principio de incertidumbre.**



¿Por qué la criptografía cuántica?

La principal característica de la criptografía cuántica es **el uso de partículas luminosas conocidas como fotones** y por sus propiedades cuánticas intrínsecas permite el desarrollo de un criptosistema inquebrantable, esto gracias al principio de incertidumbre que indica que el estado cuántico varia cuando el sistema es perturbado.

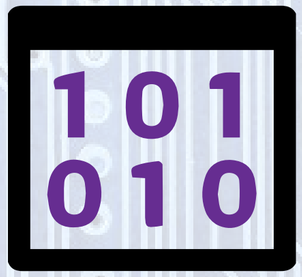
Estos criptosistemas usan los fotones para su transmisión y se puede codificar y encriptar mediante el método normal de clave secreta.



¿Cómo se transmite la información?

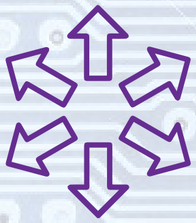
La información se transmite a través de Qubits, estas partículas elementales por el principio de la superposición permiten que su estado pueda ser 0 y 1 a la vez y que puedan transmitirse con dos polaridades vertical, horizontal y su orientación inclinado hacia la izquierda, hacia la derecha, vertical y horizontal.

El teorema de clonación garantiza que el Qubit no pueda ser clonado, lo que permite hacer 100% más segura la transmisión entre el emisor y el receptor.



Ventajas de la criptografía Cuántica

1. **Distribución de claves a nivel cuántico**, apoyado en diferentes protocolos basados en la polarización que nos permite codificar la información en tiempo, frecuencia, polarización, entre otros.



2. **Ampliación de la seguridad** introduciendo protocolos que nos permite evitar errores de clave.

3. Es **imposible descifrar una clave cuántica**, lo que permite asegurar la transmisión del mensaje ya que, si en algún momento es intervenida, cambia el estado de la clave.

4. La criptografía tradicional utiliza las matemáticas para el modelo de seguridad, **la cuántica se apoya netamente en la física**.